Analysis of cyber-security aspects both ashore and at sea

T P Avanesova¹, L K Gruzdeva¹, R A Iuskaev¹, D Yu Gruzdev², M L Somko¹
¹Admiral Ushakov Maritime State University, Novorossiysk, Lenin Avenue 93, 353924, Russia
²Deputy Head, English Department, Military University, MoD, Moscow, Russia
E-mail avanesova1@mail.ru

Abstract. Cyberattacks on critical infrastructure facilities are becoming more complex, ranging from implementation into software codes and ending with powerful opportunities for indirect impact, for example, in the form of geodynamic threats. The maritime industry also suffers from cyberattacks. Information systems, equipment, remote control stations are available to hackers. They can obtain data about valuable cargoes and movement of ships taking them off course, making them run aground or even sinking them. This article elaborates the impact of various maritime cyber security standards. It covers multiple issues including blackmailing, extortion, taking-over ships at a distance. Messing with schedules, ship positioning and in and out traffic, and terminal operations also take place. Countermeasures must be calculated and worked out. It is recommended to have cyber-security drills and information security in maritime transport establishments.

Keywords: cyber-attacks, geodynamic threats, breaches of cybersecurity, cyber security drill, navigation and control systems, IT systems, cyber hacking, the international cyber-security regulations, public safety, neural networks.

1. Introduction

Nowadays digital technologies are affected by cyber-attacks in almost all spheres of life from banking to traffic and to global operations. The modern understanding of cybersecurity does not get positive results from standard solutions in conditions of navigation at sea. Typical cyber security management systems facilitate procedures and algorithms for managing many technological and organizational processes at large industrial enterprises, special infrastructure and service formations, oil and gas pipelines, nuclear and hydroelectric power plants, large communication systems, airports, railway junctions, etc. This is especially true for national nuclear power programs. In this regard, geodynamic threats should be taken into account to protect critical infrastructure facilities from dangers. Risks of cyber-attacks increase and countermeasures must be used. The territorial placement of server devices of critical objects, as well as communication lines and control between them are recommended to be constructed according to geodynamic risks [1]. Cartographic data on more detailed distributions of crustal movements, tectonic disturbances and anomalous gravitational field should be taken into consideration [2].

Cyber-attacks send devastating waves are carried out in areas with the largest footprint in the life of modern people. It is noted that sea trade accounting for a mighty 90% of freight turnaround of goods across the globe is a most crucial. It often comes under attacks by hackers due to the high automation and computerization of ports and shore-based facilities. Cyber-attacks were unleashed on servers of the largest maritime carriers Maersk (Denmark) and COSCO (China), blocking cargo terminal systems in 2017 and 2018. Hackers tried to disrupt the operation of the enterprise “Administration of seaports of the Azov Sea” of Russia in early 2018.

Much is being done both ashore and at sea to improve best world practices against cyber-attacks. Port authorities have gone a long way in preventing cyber-attacks by drawing up response plans, working with
federal agencies on cyber security violation. They involve coast guards, local law-enforcers, construction of new lighthouses in areas free of cybersecurity. Special measures should be taken to avoid geodynamic risks, vulnerable in terms of cyber security [3].

2. Analysis of International Publications on Cyber Security Aspects

The existence of cyber security risks can lead to security and operational impacts both in shipping companies and on ships. Risk management is critical to the safe operation of shipping. In practice, it has been focused primarily on physical security (IMO ISPS Code) and safe operations (IMO ISM Code). However, the reliance on information technology in shipping operations is increasing. In this connection the international cyber-security papers were adopted in 2013, 2014 and 2016. Spain’s Government approved the strategy of national maritime-cybersecurity in 2013. The International Maritime Bureau (IMB) issued a warning in 2014 about the growing threat of cyber-attacks against shipping industry. It indicates the situation in the maritime sector was attracting more attention of cyber-pirates. The IMO Maritime Safety Committee approved the cyber risk guide “Interim Guidelines on Maritime Cyber Risk Management” in 2016.

The IMO also proposes a cyber security framework based on five functional elements: Identify, Protect, Detect, Respond and Recover for the cyber-security risk management. They should be implemented and executed continuously for the sake of everybody’s safety. The IMO guide encompasses requirements of the member states, maritime administrations and recognized best practices of shipping. They are guidelines on Cyber security Onboard Ships by BIMCO, CLIA, ICS, INTERCARGO and INTERTANKO; ISO 27001 Information Technologies Security Management; National Institute of Standards and Technology Cybersecurity Framework (NIST CSF).

Despite these international instructions cyber-attacks still exist. The Port of Barcelona and the Port of San Diego were attacked in the digital domain late in September 2018. It is understandable that the transport industry will come under attack in the future. Although the immediate results of those two attacks were not serious, the authorities decided not to pay much attention to avoid similar situations in the future [4].

Cyber-attacks are undoubtedly matters of public security, as well as safety of companies using these ports on a daily basis. Therefore, every ship must have an International Ship Security Certificate in compliance with the requirements of SOLAS Chapter XI-2 and Part A of the ISPS Code. They provide for measures to prevent incidents that happen intentionally [5].

3. Computer Training and Simulator Results of Navigators

The mariners’ education in cybersecurity is very essential. Computer training and simulators, obviously, provide the most valuable and affordable solutions. Successful strategies worked out to cut security risks, as well as cyber-attacks and proper methods for avoiding risks are cheaper and harmless with the right tools and software. “Seagull” is the best available today Computer Based Training (CBT) programme. It works both in the regimes of training and testing. A training session can be interrupted at any time and resumed later on. However, the assessment can only be performed once [6]. Assorted users’ data and results can be called on the screen (Figure 1).
It should be noted that scores of completed tests on the topic of “Security Awareness” (Nos. 0115, 0155, 0277, 0307) vary from 80 to 100% according to the cadet’s results given above. The results of the experimental group # 154(2) of Navigation Faculty of Novorossiysk Admiral Ushakov Maritime State University are represented in the table 1.

Table 1. Results of group 154 on training and testing

| Deck cadets testing | Assessment % |
|---------------------|--------------|
|                     | 1 | 2 | 3 |
| 1.                  | 70 | 85 | - | 97 |
| 2.                  | 67 | 89 | 95 | 100 |
| 3.                  | 60 | 84 | 90 | 95 |
| 4.                  | 50 | 85 | - | 100 |
| 5.                  | 45 | 90 | - | 100 |
| 6.                  | 67 | 78 | 83 | 87 |
| 7.                  | 48 | 70 | - | 90 |
| 8.                  | 51 | 75 | - | 86 |
| 9.                  | 58 | 75 | 80 | 87 |
| 10.                 | 63 | 70 | - | 81 |
| 11.                 | 40 | 65 | 83 | 87 |

The data of the second testing attempt show the difference in 22.45%. As six cadets refused from the third testing attempt, the results have the difference in 7.48%. The final results are of 91.81%. So, that it is necessary to note that a successful strategy reduces security risks as well as cyber-attacks. Proper methods for avoiding risks of them will be much positive in case of training seafarers to withstand them during the
Cyber Security Drills by means of new computer technologies for the purpose of occupational security safety.

4. Discussion of Critical IT Systems

Statistics reveals the attitude of people in the shipping industry to cybersecurity. More than 450 security officers, employed by companies, 100 ship security officers and 25 heads of IT departments, and chief information officers (CIOs) took part in his questionnaire on cybersecurity threats and measures to avoid them. The results break down as follows: about 67% of responders indicate that cyber is not a serious threat. 53% of responders report that they provide IT security policies onboard their vessels. 91% of responders do not have the training to deal with cyber threats [7]. It is arguable that more than a half of CIOs are for investing in systems, rather than crew competence and expertise.

The e-learning has been increasingly added to numerous navigation and traffic control tools. It makes seafaring safer and at the same time expands the shipping industry opportunities in cyber security. Digital technologies expose the ships to new risks, resulting in cooperation of ship and shore systems for the protection from terrorism. It should be an inherent part of e-navigation. However, it opens up fresher challenges of cyber-security enabling terrorists to take over a ship remotely [8].

Marine navigation and ship’s control systems are increasingly dependent on multiple information and mission-critical industrial control systems given below (Fig. 2): 1) Navigation: ECDIS, AIS, radars; command and control; 2) Engineering: propulsion, fire-fighting, lights, pumps, alarms; cargo placement and ship stability; Communication: satellites, VHF/SW/MW radios; 3) Routine operations: refueling, accounting and others.

In particular, the navigation and ship control systems normally run on commercial operating systems like Windows and Linux. Navigation networks contain significant critical IT systems. Besides, there are industrial-grade control systems like PLC and Scada for monitoring and managing critical situations.

All aspects of navigation and ship management at sea are influenced by cyber-attacks. As a result, vessels can go off course, collide, run aground and even sink. Under the circumstances, the mariners are required to understand and appreciate the dangers associated with cyber hacking. Any scenario will lead to the loss of a vessel, cost human lives, influence on the environment negatively causing global financial and economic problems [9].

It would not be completely out of place to dwell on countermeasures. Fast efforts are taken to protect ships and port facilities to make them cyber-proof. The “Poseidon” is a unique system of marine protection.
of ports, shipyards, drilling platforms against cyber-attacks worked out by Russian Engineering Technologies. It remains unmatched in the world. The project is a database of cyber security for marine infrastructure. It is also considered as an algorithm of automated neural/artificial intellectual threat detection [10].

The Poseidon proved to have everything to cut operating costs. It is in the interest of some maritime companies, both in Russia and abroad. The designer has the alpha version deployed in the laboratory for testing. Provisions have been made for its compatibility with domestic and foreign hardware solutions by means of software developed in Russia.

5. Recommendations
It is obvious that countermeasures begin from the lowest level up to the pinnacle of any establishment. Any sophisticated systems and networks used in shipping industry should be flexible, and possible to be applied anywhere. Thus, all employees should be prepared for countermeasures to be trained during security and cyber security drills. It is essential to prevent cyber-attacks to degrade their negative impact.

The following recommendations and procedures should be taken into account:
- to install and activate antivirus software, firewalls and e-mail spam filters on all devices used in the company;
- to update company systems frequently;
- to use approved software only;
- to think twice before clicking;
- to report and respond to malware attack on the workstation;
- to make sure third parties follow company instructions;
- to use different long and smart passwords for work and personal accounts;
- to protect passwords;
- to use protected networks;
- to use secure and dedicated station for file sharing;
- to be extra cautious while going online to share data;
- to scan external drives for viruses before entering them.

Special training should be required to keep the IT department busy with larger and more sophisticated systems. The activity of specialists must be in compliance with the imminent threat. Thus, system malfunctions, human or computer errors, procedure breaches have to be reported immediately to superiors.

As individual systems grow more complex, extra measures will have to be taken to educate personnel to let them deal with more advanced procedures [11, 12].

6. Conclusion
Everybody should learn how to live and deal with cyber threats while using all modern technologies. Nowadays, cybersecurity has to become an integral part of routine operations. Moreover, it has to become everybody’s job to a certain extent. Risks are too high to approach this issue seriously as well as to be trained properly. Cyber security drills require investments and sophisticated computer systems. Training is expensive, but it should not be ignored for positive results. Requirements and regulations are to be focused on the threats of cybersecurity in different spheres of life including hydrography, geodynamics, economics and linguistics.

References
[1] Malachova H, Bednar K 2017 Providing Security in Objects of Critical Infrastructure // Vision 2020: Sustainable economic development, innovation management, and global growth VOLS I-IX pp. 3178-3188.
[2] Minaev V A, Dvoryankin S V, Faddeev A O, Nevdakh T M, Akhmetshin T R, Fadeev A A 2019 Cybersecurity and global geodynamic risks Cybersecurity issues 3 (31).
[3] Fitton, Oliver and Prince, Daniel and Germond, Basil and Lacy, Mark 2021 The future of maritime cyber security Lancaster University Lancaster.
[4] Bunyamin G, Gizem K, Pelin B 2021 Cyber security risk assessment for seaports: A case study of a container port Cyber&Security Journal Volume 103.
[5] International Code for the Security of Ships and of Port Facilities 2002 Annex1 pp 131.
[6] Kieren Nićolas Lovell, Dan Heering 2019 Exercise Neptune: maritime cybersecurity training using the navigational simulators 5th Interdisciplinary Cyber Research conference pp. 34-37.
[7] Alert! Compendium. Improving the awareness of the human element in the maritime industry Issue 1 to 40 of the International Maritime Human Element Bulletin 2003-2016 Nautical Institute project Lloyd’s Register Foundation pp. 310-312.
[8] Beaumont P 2018 Cybersecurity Risks and Automated Maritime Container Terminals in the Age of 4IR [Fourth Industrial Revolution] Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution pp.497-516.
[9] Cho C, Chung W, Kuo S 2016 Cyberphysical security and dependability analysis of digital control systems in nuclear power plants IEEE Trans. Syst. Man Cybern.: Syst. 46 (3) pp. 356-369.
[10] Poseidon 2 2020 User Manual pp.1-79.
[11] J. Mar L & Com. 1 2019 Cyber Security in the Maritime Sector Journal of Maritime Law and Commerce Vol. 50 (1).
[12] Otto Lisa et. al. 2020 Global Challenges in Maritime Security An Introduction Cham, Springer, pp. 243.