https://doi.org/10.53656/ped2023-6s.05

Maritime Cybersecurity
Морска киберсигурност

MARITIME CYBERSECURITY EDUCATION AND TRAINING AT NIKOLA VAPTSAROV NAVAL ACADEMY

Dr. Borislav Nikolov
Nikola Vaptsarov Naval Academy (Bulgaria)

Abstract. As of the beginning of 2021, a set of new requirements has been introduced by the International Maritime Organization (IMO), necessitating established rules and measures about the cybersecurity of the ship's systems. That is to ensure a certain level of cybersecurity onboard, as well as re-occurring training of onboard staff, is required, to maintain cybersecurity measures. That leads to a new vector of postgraduate certification and namely – ships' system cybersecurity and cybersecurity management. Its purpose is to provide the necessary knowledge and skills, related to fulfilling the requirements of the IMO. This paper examines some aspects of education and training of the ship's crew regarding cybersecurity.

Keywords: maritime cybersecurity; education; training; Moodle courses

Introduction

One of the recognized definitions of cybersecurity states it is "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets"[1]. It is important to recognize that cyber security encompasses not only the technology but people and process aspects. The behavior of individual system users, implementation of poor processes, and failure to follow standard operating procedures can all weaken a system and create cyber-security vulnerabilities (Boyes 2014).

As of the beginning of 2021, a set of new requirements has been introduced by the International Maritime Organization (IMO), necessitating established rules and measures. That is to ensure a certain level of cybersecurity onboard; a re-occurring training of onboard staff is also required to maintain cybersecurity measures (Karim 2022). That leads to a new vector of postgraduate certification and namely – ships' system cybersecurity and cybersecurity management (Akpan et al. 2022).

Cybersecurity is the responsibility of not only the IT department but all employees. Because of that, the first and the most important procedure step is the training and awareness of all of the both onboard and shore-side personnel.

The awareness procedures must cover at least the risks related to internet usage, emails, the usage of own devices in a corporate network, antivirus programs, removable devices, and other risks related to specific ships onboard and ashore activities.

The training must be focused on technical cybersecurity measures and must be conducted in a realistic environment. Usually, on board a ship, there are no such conditions. Therefore, the training must be conducted ashore before the crew members responsible for the implementation of the technical cybersecurity measures start their contract.

1. Bachelor’s and Master's degree in Cybersecurity Education at the Nikola Vaptsarov Naval Academy

Nikola Vaptsarov Naval Academy (NVNA) is the oldest technical education institution in the Republic of Bulgaria. In its more than 140 years of history, NVNA has received international recognition in the field of education, training, preparation, and postgraduate qualification of staff for the maritime industry. Currently, the two major branches in the academy are “Navigation” and “Marine Engineering”. In recent years, NVNA is engaging in establishing the education of IT specialists. Cybersecurity specialists are also among the graduates of NVNA over the last 5 years. The “Cybersecurity” profile is producing graduates with both Bachelor's and Master's degrees.

The Bachelor’s degree education is focused on developing engineering skills and knowledge. The Master's degree education at the same time provides better knowledge on the management side of cybersecurity. Thus, it could be said that the Bachelor’s degree education is designed to cover the requirements to occupy the engineer position and a Master’s degree is designed to cover the requirements for management-level positions (Kim 2021).

The Bachelor’s degree programs at NVNA cover a lot of specialized modules such as:

- Computer hardware and architectures
- System administration – Windows and Linux administration, Virtualization
- Network Administration
- Programming languages
- Database administration and security
- Penetration testing
- Digital forensic and cybersecurity risk management
- Ethical Hacking and cyber incident response
- Reverse engineering

All of the aforementioned courses are mandatory for every cybersecurity specialist. In terms of maritime cybersecurity, what is missing are the courses related to ship's OT systems. This problem could be easily resolved by adding additional elective courses to the major curriculum. At the same time, the included major curriculum courses are general to cybersecurity as well. This allows the graduates to succeed in the labor market in a large area of industries.

The Master's degree curriculum includes courses related to management, suchas:

– Cybersecurity management
– Cybersecurity legislation framework
– Project management
– Personnel management

This is also a general cybersecurity-related major. To cover the requirements of the maritime industry, it should be complemented by elective additional courses related to the ship's security system, the ship's security plans, and the cybersecurity design of the ship's IT and OT systems.

2. Cybersecurity awareness and training courses for seafarers

As of the beginning of 2021, a set of new requirements has been introduced by the International Maritime Organization (IMO)[2,3], necessitating established rules and measures. That is to ensure a certain level of cybersecurity onboard, as well as re-occurring training of onboard staff, is required, to maintain cybersecurity measures. That leads to a new vector of postgraduate certification and namely – ships' system cybersecurity and cybersecurity management. A decision was made to commence preparation for designing training documentation for postgraduate qualification by mid-2021. Its purpose is to provide the necessary knowledge and skills, related to fulfilling the requirements of the IMO.

In response to cybersecurity challenges in the maritime industry, NVNA decided to establish several post-graduate courses for seafarers to cover different levels of the ship's crew competencies and responsibilities.

In mid-2022, the state of the courses reached a point, where the framework was in place, the main subject of the three sub-courses had been determined, and a logical connection between them had been established. The next point in line was to expand on the lessons themselves, address practical skills, and provide all the necessary material for enhancing said skills. We conceived that NVNA possesses the necessary technical resources for the tasks, based on the available ship simulation complexes, as well as the desired level of expertise in the field of cybersecurity. All those can be successfully combined to assure the training of seafarers in cybersecurity.

As a result at the end of 2022, three postgraduate cybersecurity courses for seafarers were developed with all the required study materials.

The objective of these courses is to encompass all levels and competence of executive and management staff of ship companies. The courses are planned and developed with a certain level of overlapping of content within the three sub-courses. The objective is to provide the course participants with an adequate amount of knowledge and skills for their current employment position, as well as to ease the transition between levels of responsibility. Any of the three sub-courses can be completed individually, without having to go through any of the previous or upper levels.

The titles of the developed and currently provided cybersecurity courses at the NVNA are as follow:

– “MARITIME CYBERSECURITY ESSENTIALS – CYBER HYGIENE AT SEA”

– “MARITIME ADVANCE CYBERSECURITY – CYBERSECURITY AT SEA”

– “MARITIME CYBERSECURITY MANAGEMENT”

The “MARITIME CYBERSECURITY ESSENTIALS – CYBER HYGIENE AT SEA” course is intended for the lowest level of executive onboard staff and employees of shore enterprises, related to the measures of cybersecurity of onboard ship and ashore systems. Additionally, this course is expected to be suitable for any member of the ship staff, providing fundamental knowledge and skills for the completion of day-to-day tasks with an increased level of cybersecurity.

This course contains the following educational modules which cover all fields of cybersecurity related to the maritime industry:

– Cyber threats and vulnerabilities in the maritime industry

– Protection of personal devices

– Critical data protection

– Safely browsing the network

– Cybersecurity for mobile devices.

The duration of this course is 32 classes (academic hours). Each of the educational modules in question contains between 2 to 4 separate topics with corresponding lectures and seminars. This course contains 13 lectures and 10 seminars.

The “MARITIME ADVANCE CYBERSECURITY – CYBERSECURITY AT SEA” course is aimed at people with technical knowledge and competence, who have been tasked with administering onboard IT and OT systems. Unlike the previous level of the cybersecurity course, this one is expected to be of service to administrators and cybersecurity officers aboard. Personnel involved with planning onboard cybersecurity systems, as well as communication systems between sea and shore, can find this level of the course helpful.

This course contains the following educational modules:

– Cybersecurity of the ship’s IT and OT systems

– Cyber-attacks at sea and their mitigation.

The duration of this course is 16 classes (academic hours). Each of the educational modules in question contains between 3 and 4 separate topics with corresponding lectures and seminars.

The "MARITIME CYBERSECURITY MANAGEMENT" course is aimed at staff, who are responsible for creating cybersecurity procedures and their application in ship companies. This course partly overlaps with the previous one, which will allow different-level staff to easily re-qualify.

This course contains the following educational modules:

– Cyber-attacks at sea and their mitigation

– Management of cybersecurity at sea

The duration of this course is 16 classes (academic hours). Each of the educational modules in question contains 4 separate topics with corresponding lectures and seminars.

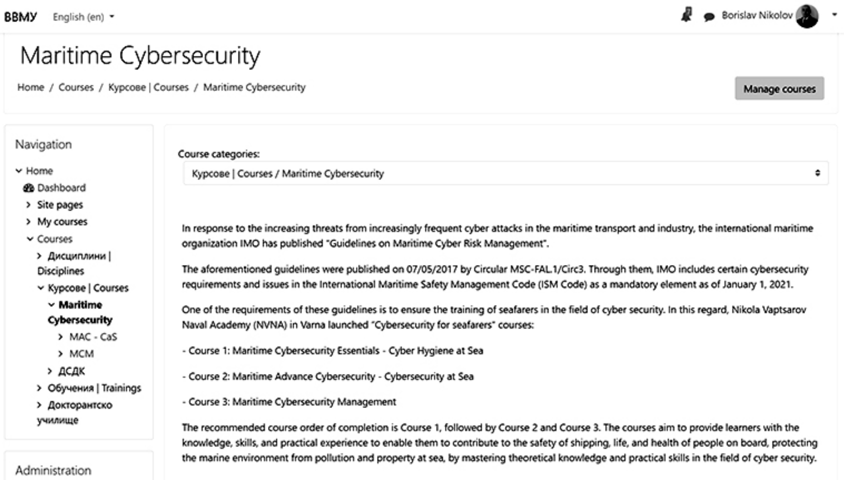
The course "MARITIME ADVANCE CYBERSECURITY – CYBERSECURITY AT SEA" has 7 lectures and 4 seminars developed. That same course, as well as the "MARITIME CYBERSECURITY MANAGEMENT" course, are of modular type, with 2 modules per course, as one of the modules is common for both of the courses. That allows the participants to complete each of these courses in a shorter time, depending on their prior knowledge. The second module of the course "MARITIME CYBERSECURITY MANAGEMENT" has 4 lectures and 2 seminars prepared.

The three courses have 24 separate lectures and 16 seminars altogether. All study resources are available in English, as that is the primary language in the maritime industry, and that helps in advertising said course to a broader range of potential foreign applicants. English is the primary language during participation in any of the three courses.

Applied seminars are conducted in a prearranged virtual computer environment which is developed and hosted in the Security Operations and Training Center of NVNA.

Each of the aforementioned three courses is considered completed after an exam, in the form of a test, through the locally hosted learning management system (LMS) in NVNA available online after authentification with appropriate credentials[6]. The system in question is based on the MOODLE platform. For each of the courses, a separate, corresponding exam has been created in the MOODLE system. The students/trainees have adequate access to the system, which includes all necessary study materials, lectures, presentations, and practical assignments. The final exam is formed from a question bank, from each chapter of the course (Dechev 2006).

The content of each of the offered courses is aligned with the recommendations of the leading international organizations in the field of seafarer training including cybersecurity at sea such as BIMCO[4] and DNV[7].



Maritime Cybersecurity

Home / Courses / Курсове | Courses / Maritime Cybersecurity

Course categories: Курсове | Courses / Maritime Cybersecurity

In response to the increasing threats from increasingly frequent cyber attacks in the maritime transport and industry, the international maritime organization IMO has published "Guidelines on Maritime Cyber Risk Management".

The aforementioned guidelines were published on 07/05/2017 by Circular MSC-FAL.1/Circ3. Through them, IMO includes certain cybersecurity requirements and issues in the International Maritime Safety Management Code (ISM Code) as a mandatory element as of January 1, 2021.

One of the requirements of these guidelines is to ensure the training of seafarers in the field of cyber security. In this regard, Nikola Vaptsarov Naval Academy (NVNA) in Varna launched "Cybersecurity for seafarers" courses:

- Course 1: Maritime Cybersecurity Essentials - Cyber Hygiene at Sea

- Course 2: Maritime Advance Cybersecurity - Cybersecurity at Sea

- Course 3: Maritime Cybersecurity Management

The recommended course order of completion is Course 1, followed by Course 2 and Course 3. The courses aim to provide learners with the knowledge, skills, and practical experience to enable them to contribute to the safety of shipping, life, and health of people on board, protecting the marine environment from pollution and property at sea, by mastering theoretical knowledge and practical skills in the field of cyber security.

Figure 1. Maritime cybersecurity electronic courses in NVNA's LMS[6]

3. Cybersecurity Training Facilities

Cybersecurity practices and exercises should be provided in an environment that is similar to the real as much as possible[5] (Andreev et al. 2018). The best way for this is the usage of a virtual training environment. In this way real systems could be represented by virtual machines and any cyber issue could be examined without risk of damage to the real systems. This is even more relevant to the maritime industry because of the characteristics of the ship's IT and OT systems.

The required hardware and software to build a virtual training environment that represents the ship's IT and OT systems are available at NVNA. The required

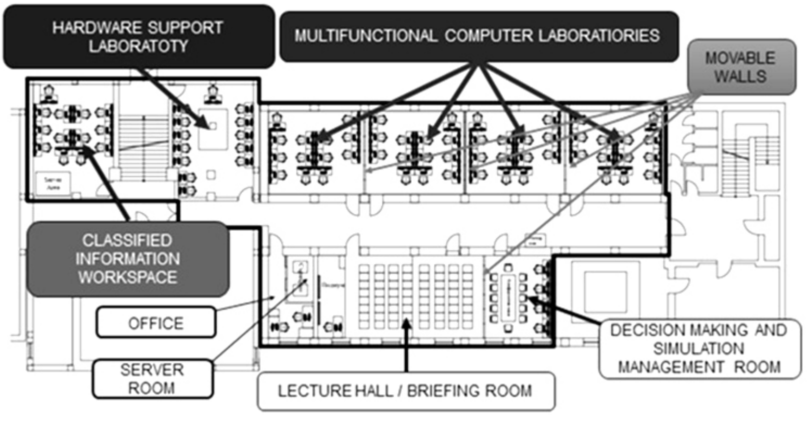

HARDWARE SUPPORT LABORATOTY
MULTIFUNCTIONAL COMPUTER LABORATIORIES
MOVABLE WALLS
CLASSIFIED INFORMATION WORKSPACE
OFFICE
SERVER ROOM
LECTURE HALL / BRIEFING ROOM
DECISION MAKING AND SIMULATION MANAGEMENT ROOM

Figure 2. Security Operation and Training Center at NVNA

hardware is situated at the Security Operations and Training Center (SOTC) of the academy.

In addition to the available computer workplaces at SOTC, a cluster of servers and storage with installed virtualization software is available for use. On this cluster of servers, a cyber range software developed as a result of an internal project in NVNA is deployed. The cyber range software provides a virtualized training environment in which different ships' IT and OT systems can be simulated. After the end of the training, the virtualized training environment can be easily reloaded for the next exercise.

The equipment of the SOTC is used to provide training and education for Bachelor's and Master's degree students and maritime cybersecurity training for seafarers as well (Raimondi et al. 2022).

Conclusions and summary

This article presents the current state of maritime cybersecurity training and education provided at Nikola Vaptsarov Naval Academy. The provided short cybersecurity courses are developed to cover the responsibilities of all staff members and personnel onboard the ship.

The curricula for the Bachelor's and the Master's cybersecurity programs at Nikola Vaptsarov Naval Academy should be modified to include courses related to the ship's IT and OT systems – principles, best practices, and concepts for building a well-protected and secure enterprise infrastructure on board the ship.

The maritime simulators in NVNA should be integrated as soon as possible with the SOTC. In this way, more realistic cybersecurity training for seafarers could be achieved. In addition, this will open a new potential for research in the field of cybersecurity in the marine industry.

NOTES

1. INTERNATIONAL TELECOMMUNICATIONS UNION, 2008. Series X: Data Networks, Open System Communications and Security, Telecommunications security: Overview of cybersecurity. ITU-T X.1205
2. MSC-FAL.1-Circ.3 – Guidelines on Maritime Cyber Risk Management. International Maritime Organization. Available from: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf. [Last accessed 23 Apr 2023].
3. MSC 98/23/Add.1 Annex 10 – Resolution MSC.428(98) Maritime Cyber Risk Management in Safety Systems. International Maritime Organization. Available from: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf. [Last accessed 23 Apr 2023].
4. BIMCO. The Guidelines on Cyber Security Onboard Ships, Version 4. Web site. BIMCO Publications. Available from: https://www.bimco.org/about-us-and-

our-members/publications/the-guidelines-on-cyber-security-onboard-ships. [Last accessed 01 May 2023]

5. RAYTHEON INTELLIGENCE AND SPACE (RIS). Persistent Cyber Training Environment. Web site. Available from: https://www.raytheonintelligenceandspace.com/capabilities/products/persistent-cyber-training-environment. [Last accessed 01 May 2023]
6. NVNA. Maritime Cybersecurity. Web site. Nikola Vaptsarov Naval Academy. Available from: https://dlc.naval-acad.bg/course/index.php?categoryid=24.
7. DNV. Web site. Available from: https://www.dnv.com/.

REFERENCES

AKPAN, F. et al, 2022. Cybersecurity Challenges in the Maritime Sector. *Network*, no. 2, pp. 123 – 138. Available from: https://doi.org/10.3390/network2010009.

ANDREEV, E.; DYANKOVA, E. & TSONEV, Y., 2018. Prilozhenie na igrovizaciya za povishavane na kachestvoto na prakticheskite zanyatiya. *Sedma natsionalna konferenciya po elektronno obuchenie vyv visshite uchilishta.* ISBN 978-954-07-4509-1.

BOYES, H., 2014. Maritime Cyber Security – Securing the Digital Seaways. *Engineering & Technology Reference*. Available from: https://doi.org/10.1049/etr.2014.0009.

DECHEV, Y., 2006. Analiz na metodite za control na znaniyata i prilozhenieto im v elektronno obichenie na morski kadri. *Vtora nacionalna konferencia po elektronno obuchenie vyv vissheto obrazovanie,* pp. 117 – 120. ISBN-10-954-07-2413-9.

KARIM, M., 2022. Maritime cybersecurity and the IMO legal instruments: Sluggish response to an escalating threat? *Marine Policy*. 143. 105138. Available from: https://doi.org/10.1016/j.marpol.2022.105138.

KIM, J., 2021. A Study on the Development of Information Protection Education Contents in the Maritime Using Metaverse. *Journal of the Korea Institute of Information Security and Cryptology*, vol. 31, no. 10. Available from: https://doi.org/10.13089/JKIISC.2021.31.5.1.

RAIMONDI, M. et al, 2022. Training the Maritime Security Operations Centre Teams. Available from: https://doi.org/10.1109/CSR54599.2022.9850324.

✉ **Dr. Borislav Nikolov**
ORCID iD: 0000-0002-6055-8538
Web of Science Researcher ID: AAZ-6105-2021
Nikola Vaptsarov Naval Academy
Varna, Bulgaria
E-mail: nikolov@naval-acad.bg