IAMU
International Association of Maritime Universities

THE NIPPON FOUNDATION

IAMU 2018 Research Project
(No. 20180107)

Technology for safer and greener shipping Addressing Cyber Security in Maritime Education and Training (CYMET)

By

Satakunta University of Applied Sciences

August 2019

IAMU
International Association of Maritime Universities

This report is published as part of the 2018 Research Project in the 2018 Capacity Building Project of International Association of Maritime Universities, which is fully supported by The Nippon Foundation.

Published by the International Association of Maritime Universities (IAMU) Secretariat
Meiwa Building 8F, 1-15-10 Toranomon, Minato-ku,
Tokyo 105-0001, JAPAN
TEL : 81-3-6257-1812 E-mail : info@iamu-edu.org URL : http://www.iamu-edu.org

ISBN978-4-907408-27-5

IAMU
International Association of Maritime Universities

THE NIPPON FOUNDATION

IAMU 2018 Research Project
(No. 20180107)

Technology for Safer and Greener Shipping Addressing Cyber Security in Maritime Education and Training (CYMET)

By
Satakunta University of Applied Sciences

Contractor : Juha KÄMÄRI, SAMK
Research Coordinator : Sauli Ahvenjärvi, SAMK
Research Partner : Ireneusz Czarnowski, GMU
John Mogensen, SIMAC

Contents

Final Report for the FY2018 IAMU

Research Project

Theme: Technology for safer and greener shipping

Addressing Cyber Security in Maritime Education and Training (CYMET)

Satakunta University of Applied Sciences

And

Sauli Ahvenjärvi

Authors: Sauli Ahvenjärvi, Ireneusz Czarnowski, John Mogensen

Principal Lecturer, Satakunta University of Applied Sciences, sauli.ahvenjarvi@samk.fi
Professor, Gdynia Maritime University, i.czarnowski@umg.edu.pl
Assistant Professor, Svendborg International Maritime Academy, jmo@simac.dk

Abstract: Maritime cyber security is a topical issue in terms of automated navigation, digitalization, IoT and other web-based applications. As technology has developed, information technology on board ships has become safety-critical and networked. Recent cyber attacks against shipping industry have hit the head office of the company. The shipping company's personnel is considered the weakest point from the cyber security point of view. Cyber risks may occur from personnel having access to the systems onboard, for example by introducing malware via removable media. The international reseach project CYMET, a joint project by Satakunta University of Applied Sciences (Finland), Gdynia Maritime Acedemy (Poland) and Svendborg International Maritime Academy (Denmark), initiated by International Association of Maritime Universities (IAMU), addresses the needs of cyber security training of seafarers. The current IMO standard of training of seafarers to cope with cyber threats is not on a satisfactory level. The project summarizes the needs, the current status and recommendations for maritime cyber security training and introduces a web-based tool to support the member universities of IAMU in running courses on maritime cyber security management.

Keyword: *Maritime, Education, STCW, Cyber Security, Safety*

Executive summary

The research project 'Addressing Cyber Security in Maritime Education and Training' (CYMET) was carried out by Satakunta University of Applied Sciences (SAMK), Gdynia Maritime University (GMU) and Svendborg International Maritime Academy (SIMAC) within the project system of International Association of Maritime Universities (IAMU) between May 2018 and May 2019.

Maritime cyber security is a topical issue in terms of automated navigation, digitalization, IoT and other web-based applications. As technology has developed, information technology onboard ships has become safety-critical and networked. A cyber-attack could be an intentional attempt to modify, disconnect, destruct or to unauthorizedly access or use an asset. Within the marine transportation framework cyber-attacks concern computer information systems, computer infrastructures, including Information Technology (IT) networks, or personal computer devices, i.e. any type of offensive activity aimed at IT and Operation Technology (OT) systems, computer networks, and/or personal computer devices attempting to threaten, destroy or access systems and data of a ship or a shipping company. The attacker can be a person or process that attempts to access data, functions or other restricted areas of the system, without authorization, potentially with malicious intent.

Maritime cyber-security, understood as measures taken to protect network and computer assets both on ships, terminals, ports, and all computerized equipment supporting maritime operations, is an important aspect for maintaining information exchange, without modification and loss. Seafarers are at the frontline of management in the maritime domain and they are seen the most critical barrier between success or failure when it comes to protecting the integrity of the data systems on board ships.

The objective of the CYMET project was to promote maritime safety by increasing the awareness of cyber safety issues related to ships and maritime transport, and the proper consideration of these themes in education and research activities by the IAMU member universities. The present status and existing demands in training of seafarers was to be evaluated, and recommendations provided on how cyber safety should be taken into account in maritime education and training. A platform for joint development and sharing of web-based e-learning material on maritime cyber security was to be created and pilot tested as well at the end of the project.

A literature study of the present status of cyber safety training requirements in the IMO STCW code and an assessment of the present status of education and research on cyber safety issues in IAMU member universities based on a questionnaire survey was carried out.

It can be concluded, that not only cyber security but also cyber safety is needed to be addressed in maritime education and training. It is already a mandatory requirement under the ISM code although it is not specifically mentioned. Another conclusion is that education and training should address all aspects of cyber safety issues for both Information Technology (IT) and Operation Technology (OT) systems, since the ISM code aims at managing the ship in a safe manner, handling all risk to a sufficient level.

The survey among the IAMU member universities indicates that education and training on cyber safety issues are incorporated to some extent at a number of universities and in a variety of fields of teaching covering both IT and OT systems. It also reveals that self-paced learning is not applied by the majority of the respondents in the survey. This could be because of the special application of IT and OT systems in the maritime domain and the lack of special developed training packages on cyber security and cyber safety issues for the maritime domain. This is not known, but could be explored in future research.

It seems that the biggest risks for cyber attacks are related with the human element. Managing this part of the cyber security calls for keeping up awareness of cyber threats and ability to avoid risky behavior in the whole organization. All employees of the shipping company, from top to bottom and from land organization to seafarers, should have up-to-date knowledge about cyber threats and the means of protection against them. This can be achieved only by proper training of the personnel. Not only once, but continuously, since cyber threats take constantly new forms, directions and targets.

Taking into consideration the present technical development within the shipping industry, training of new seafarers should offer appropriate knowledge about cyber threats and management of cyber security in the shipping industry context. However, the present edition of the STCW convention does not set clear requirement for seafarers' knowledge about cyber security.

As an essential topic within maritime cyber security, safe information exchange has been studied within the project. The taxonomy of information exchange was presented and the safe information exchange was discussed taking into consideration different aspects according to type, character, mode and role of the information exchange. The main conclusion from this discussion was that cyber risk management can be based on two pillars: people (human) and technology. The two pillars were characterised with respect to the safe information exchange process. Based on this analysis, important aspects about the training and qualifications of seafarers to cope with cyber risks were highlighted. It was found out that the existing training programmes for deck officer students are not sufficient in relation with the character and importance of the problem. The final conclusion is the recommendation to update the academic programs accordingly. In the future, more specific recommendation on the contents of academic curricula should be formulated and discussed.

A training package on maritime cyber security issues was created within the CYMET project for the use of IAMU member universities. It was developed jointly by the three universities. After analyzing two alternative platform technologies, the open source web-learning platform Moodle was selected. The member universities of IAMU have the access to the material at the e-learning portal of IAMU. The e-learning course on Maritime Cyber Security was briefly pilot tested. The feedback from students was mainly positive. It is recommended that IAMU considers initiation of a development project, which concentrates in development of the Maritime Cyber Security self-education material further and takes care of updating and complementing the course contents. Another approach could be establishing a special Working Group for this purpose.

CYMET project and its main results have been/will be presented in the following four papers: *'Addressing Cyber Security in Training of the Mariner of the Future – the CYMET Project'* at the DGON symposium in Berlin, Germany in September 2018, *'Safe Information Exchange on Board of the Ship'* at TransNav 2019 conference in Gdynia, Poland in June 2019,*'Addressing Cyber Security In Maritime Education And Training'*, submitted for publication in the WMU Journal of Maritime Affairs and *Joint Production of Web-learning Material by IAMU Member Universities*, submitted for publication at IAMU Conference in Tokyo, Japan in November 2019.

Sauli Ahvenjärvi
DSc (Tech), Principal Lecturer, Satakunta University of Applied Sciences
coordinator of CYMET project

FY2018 IAMU Research Project

Addressing Cyber Security in Maritime Education and Training (CYMET)

CYMET project and its main results have been/will be presented in the following four papers: *'Addressing Cyber Security in Training of the Mariner of the Future – the CYMET Project'* at the DGON symposium in Berlin, Germany in September 2018, *'Safe Information Exchange on Board of the Ship'* at TransNav 2019 conference in Gdynia, Poland in June 2019,*'Addressing Cyber Security In Maritime Education And Training'*, submitted for publication in the WMU Journal of Maritime Affairs and *Joint Production of Web-learning Material by IAMU Member Universities*, submitted for publication at IAMU Conference in Tokyo, Japan in November 2019. Chapters 1 to 4 of this report consist of the essential contents of those four papers.

1. Maritime Cyber Security Requires Immediate Attention

1.1. Introduction

Traditionally recognised safety risks in seafaring are due to piracy, dangerous cargoes, equipment failure, extreme environmental conditions and various types of human errors related to operation, maintenance and management of the ship. There is a new growing threat on top of these: cyber attacks. Some major shipping companies have recently been hit by cyber attacks, e.g. Maersk, BW Group, and Clarksons. Those incidents involved shoreside IT systems, but the increasing connectivity of vessels and their heightened reliance on software are bringing the cyber threat also to sea. Maritime cyber security has become a highly topical issue for sea transportation industry due to developing ship intelligence, autonomy, remote control, IoT and various web-based applications. As shipping technology has developed, information systems onboard ships have become safety-critical and networked. This has increased the safety risks of maritime operations due to unauthorised access or malicious attacks to critical systems.

Paying special attention to the human element is an important area in management of cyber security. Experience from the past cyber security incidents points out that the majority of cyber security incidents are related to the human element [1]. The ship's personnel is apparently a potential weak point of the safety of intelligent onboard systems.

There are several ways to utilize this weak point by the cyber attackers. In general, all human related cyber threats originate from lack of awareness and thus marine cyber security management shall be taken into serious consideration by all organisations responsible for education and training of seafarers. Also maritime universities should pay more attention to cyber security in their research activity.

1.2. Cyber security management in the maritime domain

There have been different opinions about cyber risks in the maritime domain. According to David Rider from the alliance of Company Security Officers (CSO Alliance) some commercial providers are suggesting risks of a hostile attack on ship's systems causing the vessel to be remotely controlled or causing catastrophic navigation errors etc. while on the other hand, some people say that this notion is

nonsense due to the number of fail safes and manual overrides and controls in place [2]. Other voices point out that the most likely threat is actually to the servers inside the company's head office. However, the shipping industry got a nasty wake-up in 2017 in the form of cyber attacks against three big shipping companies Maersk [3], BW Group [4] and Clarksons [5], causing substantial economical losses. Although these cyber attacks hit the headquarters of these companies, there are many interesting targets for cyber attackers also onboard modern ships: intelligent navigation and steering systems, machinery automation, remote diagnostics and maintenance services of the machinery, communication systems, cargo management systems, applications of IoT and cloud computing etc.

In 2017, I.H.S. Fairplay conducted a maritime cyber security survey, to which 284 people responded. 34 percent of them said that their company had experienced a cyber attack in the previous 12 months [6]. Of those attacks, the majority were ransomware and phishing incidents; the same sort of incidents are affecting companies everywhere, so they are not at all specific to the maritime world.

The work for improving cyber security in the shipping industry has started. Several reports, useful guidelines and codes of practice for maritime cyber security management have been published by companies, associations and governmental organisations [1], [7], [8]. IMO published its Guidelines on management of cyber security in 2017 [9].

Targeted good level of cyber security of a shipping company or a single ship can not be achieved and maintained just by updating hardware and software. The guidelines by BIMCO [7] recommend that the cyber risk management of a ship should contain at least the following tasks:

- identify the roles and responsibilities of users, key personnel, and management both ashore and on board
- identify the systems, assets, data and capabilities, which if disrupted, could pose risks to the ship's operations and safety
- implement technical measures to protect against a cyber incident and ensure continuity of operations. This may include configuration of networks, access control to networks and systems, communication and boundary defense and the use of protection and detection software
- implement activities and plans (procedural protection measures) to provide resilience
- against cyber incidents. This may include training and awareness, software maintenance, remote and local access, access privileges, use of removable media and equipment disposal
- implement activities to prepare for and respond to cyber incidents.

This list of necessary tasks shows, that proper management of cyber security is not just a matter of installing new software or hardware. The required action will touch the whole organisation and influence its entire working culture.

1.3. The human element of cyber security

It could be possible and rather straightforward to build a firm protection against cyber attacks for a totally unmanned and autonomous system. But in the real-life, an ordinary socio-technical system has a weak point that can be utilised by cyber attackers to get to the target: the human being in contact with the targeted system. The poor human being can be almost anyone in the organisation. In some cases the origin of the cyber threat is an employee inside the organisation. According to a recent survey by the Cyber Edge Group, 1200 IT professionals from companies all over the world consider ”lack of skilled personnel” and ”low security awareness among employees” the two biggest problems in defending the organisation against cyber threats [10]. The marine cyber security survey by

I.H.S. Fairplay revealed that a great number of employees in shipping business have not received cyber awareness training of any kind. No less than 47 percent of those questioned believed that their organization's biggest cyber vulnerability was the staff [6]. The most vulnerable area of the cyber defence of a company seems to be the personnel.

There are different options for cyber attackers for utilising the human element. A cyber attack can occur via the personnel having access to the critical systems onboard, for example by the possibility to introduce malware via removable storage. Or by using own device at work and plugging it into the ship's system, thereby releasing a malware inadvertently carried in the computer or smartphone. Isolating the ship entirely from the Internet doesn't eliminate the threat. Infections can still enter the ship's network through portable devices with memory on them or through a new software installed to the system by a person in the ship's organisation. Phishing attacks are another form of cyber threats that utilize the human element. Phishing can happen for example through forged web sites or e-mails. The most sophisticated operations are planned and executed in such a way that the persons having been exploited by the attackers never become aware of having been the weak point and having made the cyber attack possible.

It has been proposed that over one third of data breaches in organisations are attributed to human error or negligence. Danish maritime cyber security company CyberKeel published in 2014 a whitepaper about maritime cyber threats. It strongly stresses the role of the human element and the importance of improving the awareness about cyber threats [11]. It seems that a good starting point for enhancing the cyber security is to pay attention to the human element, i.e. to training of the personnel.

However, the task is not simple. Cyber threats do not remain the same, but they constantly take new forms and utilize new ideas to fool the victim. The attackers keep inventing new sneaky methods to utilize the human element in accomplishing cyber attacks. The knowledge and procedures that were good for protection against cyber threats a year ago might suffer from serious shortcomings today. The company instructions, procedures and practices need to be updated continuously. The endless race with cyber attackers is a challenge also for training providers.

The goal of training is to give the seagoing personnel and the people working in the land organisation of the shipping company proper general knowledge about cyber security in the maritime domain, awareness about potential risks and how to avoid them, and the attitude for good management of cyber security of the company. The training should build sound criticalness and proper working habits to minimise the risk of a person to become a victim of a cyber attack. Successful management of the human element of the maritime cyber security calls for collaboration of all parties involved.

It is important to understand that the cyber security know-how of the personnel must be refreshed and updated on a regular basis in order to maintain a good level of protection. The company procedures and instructions on management of cyber security must be reviewed and updated regularly as well.

1.4. The CYMET project

The International Association of Maritime Universities (IAMU) is a non-profit global network of leading maritime universities providing Maritime Education and Training (MET) of seafarers for the global shipping industry. In 2007, IAMU was certified as a non-governmental organization (NGO), qualified with the International Maritime Organization (IMO), and has expanded the scope of its activities not only to higher education research institutions but also to activities with the international maritime society [12].

Within its project system, IAMU is running international research projects on selected topics. The focus areas of the research projects are defined annually. Maritime cyber security was selected as one of the focus areas, or main themes, for the research projects of 2018. The research project Addressing Cyber Security in Maritime Education and Training (CYMET) was started in May 2018.

The goal of the CYMET project is to increase the knowledge and awareness of cyber safety issues within seafaring industry and proper consideration of these themes in education and research activities of the IAMU member universities. CYMET is a joint project coordinated by Satakunta University of Applied Sciences (Finland) and accomplished in collaboration with Gdynia Maritime Academy (Poland) and Svendborg International Maritime Academy (Denmark). The project started in June 2018 and it will be completed in May 2019. The work has been arranged into seven work packages:

WP 1: Study on the present status and development of cyber security in the maritime domain.
WP 2: Study of the present status of cyber security training requirements and assessment of the present status of education on cyber security issues in IAMU member universities.
WP 3: Based on WP1 and WP2, specifying needs and producing proposals for development of the maritime education and training on cyber security subjects.
WP 4: Selection of the platform for the IAMU Maritime Cyber Security web learning package.
WP 5: Collecting material and development & testing the web learning course.
WP 6: Pilot tests and fine-tuning of the web learning course.
WP 7: Production of reports and conference articles, progress report and the final report of the project.

In the beginning of the project, a study of the current status of the maritime cyber security and training of maritime cyber security in the IAMU member universities was conducted. Needs for training of seafarers in management of cyber security were identified and proposals and recommendations for development of this training were stated. Another outcome of the CYMET project is the online training package for IAMU member universities for running courses on maritime cyber security. A training package on cyber security issues for maritime professionals was created and piloted. The learning package consist of texts, images, videos and links to relevant material in the Internet. Personal exercises provide the students with feedback of the progress of learning. This matter will be discussed in detail in the last chapter of this report. Keeping the training material up-to-date is also an important matter. Some proposals about updating the material after the CYMET project has come to the end are presented in the end of this report.

1.5. Preliminary comments in the beginning of the project

Some preliminary comments could be given about the issue already in the beginning of the project. Firstly, it is an obvious matter that the present version of the International Convention on Standards for Training, Certification and Watchkeeping for Seafarers (STCW) by IMO [13] which is the international reference for training of seafarers, does not pay specific attention to cyber security awareness of seafarers. Consequently, maritime training institutions may not have cyber security training included in their standard deck officer or engine officer curriculum. This is a remarkable shortcoming at the present situation. IAMU and the international shipping industry could take action to get STCW amended by basic cyber security management. This should be done as quickly as possible since the shipping industry is experiencing a rapid and thorough development into the era of complex integration, digital communication, IoT, cloud computing, remote control and autonomy.

It is also of vital importance that people working in maritime transportation industry have a possibility to update their knowledge on cyber security on a regular basis. There are some commercial training

providers on the market offering courses on maritime cyber security. To complement this supply the public maritime education and training institutions, including IAMU member universities, could develop refreshment courses on cyber security for the maritime industry. It should be considered at IMO if some form of refreshment training on cyber security issues should be made mandatory. The refreshment training could then be arranged by STCW certified training institutions. To ensure the quality of the training, the refreshment courses could be included in standard auditing procedures.

It should be noted hereby that management of the human factor of maritime cyber security is not completed by only training the personnel. The cyber security related practices and procedures of the company and the ships must also be reviewed and renewed, when necessary. Training without development of effective practices against cyber risks would not lead to any success. And vice versa. Building a good cyber security culture is not possible without continuous development of practices and procedures and without continuous training of the personnel. Applying working practices that take cyber security into consideration should be a routine for anyone in the organization.

1.6. Conclusions

As automation, autonomy and intelligent computer-based solutions gain ever bigger role in sea transportation systems, the shipping industry must be prepared and protected against cyber threats. It seems that the biggest risks for cyber attacks are related with the human element. Managing this part of the cyber security calls for keeping up awareness of cyber threats and ability to avoid risky behavior in the whole organization. All employees of the shipping company, from top to bottom and from land organization to seafarers, should have up-to-date knowledge about cyber threats and the means of protection against them. This can be achieved only by proper training of the personnel. Not only once, but continuously, since cyber threats take constantly new forms, directions and targets.

Taking into consideration the present technical development within the shipping industry, training of new seafarers should offer appropriate knowledge about cyber threats and management of cyber security in the shipping industry context. The present edition of the STCW convention by IMO, which forms the international minimum standard for training of seafarers, does not set specific requirement for seafarers' knowledge about cyber security.

The International Association of Maritime Universities (IAMU) selected maritime cyber security as one of the key topics for the FY 2018 research project period. IAMU initiated the research project CYMET - Addressing Cyber Security in Maritime Education and Training. The project is coordinated by Satakunta University of Applied Sciences from Finland and carried out in close collaboration with Gdynia Maritime University from Poland and Svendborg International Maritime Academy from Denmark. The work packages of the project include an analysis of the current state of maritime cyber security and an evaluation of the demands in training of seafarers, and producing a recommendation on how cyber security should be taken into account in maritime education and training. An outcome of the project is a web-based training material for IAMU member universities supporting the education on cyber security topics.

2. Safe Information Exchange on Board of the Ship

Information exchange is an important component of life and human behaviour on the personal level. It is also an important factor from the perspective of a technical and business processes. An interesting safety-critical environment for information exchange is a ship, where different kinds of information is sent and received both internally and externally. Information is exchanged internally for communication among the crew and in different technical systems onboard the ship. In many cases, safety of information exchange is especially crucial. This chapter presents a taxonomy of information, bearing in mind its exchange, and discusses the problem of safe information exchange considering different systems existing on board the ship and the relation between different actors. The issue of safe information exchange from the perspective of maritime training is also discussed.

2.1 Introduction

Information is an integral part of the world and valuable for personal, social and organisational functioning [14]. Different definitions of information can be found in literature. These definitions are formulated in different perspectives according to the nature of information. One of the definitions characterises information from the perspective of knowledge. In another one, information is also understood as a resource, a commodity or as a constitutive force in society. Information plays also important role in decision making processes. Information is also the backbone for information science and computer science. In these domains information is defined from the perspective of data, used for operations carried out by information systems, where data is processed. Different kinds of information structures are also defined for storing and processing data in the systems.

Information related to the data can uphold different kinds of operations. The use of data can be understood in different ways in present-day and modern systems. This concerns especially cyber operations, defined as the engagement of cyberspace capabilities for data processing and communication between different actors and where, according to the theory of system analysis, an actor may represent roles played by human users, external hardware, or other subjects that interact within the existing environment. Thus, cyber operations also cover the entire scope of cyberspace, both technical and nontechnical, and is merged with cyber system, where different combination of facilities, equipment, personnel, procedures and communications are integrated to provide cyber services. In literature, the problem of cyber operations is discussed in term of three elements: Information, Technology and People (see Fig. 2.1). Such discussion on the cyber operations in the maritime environment has been carried out in [15].

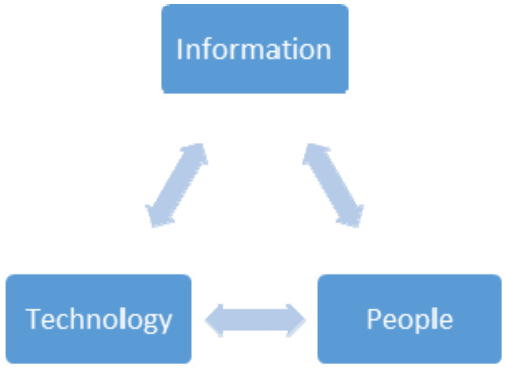

Figure 2.1 The three elements of cyber operations [15]

Maritime sector, including maritime industry, defined as “all areas and things of, on, under, relating to, adjacent to, or bordering on sea, ocean, or other navigable waterway, including all maritime-related activities, infrastructure, people, cargo, vessels and other conveyances" is an exceptional example of a domain where safety-critical exchange of information exists. Modern ships are increasingly dependent on information exchange inside and between technical systems as a result of digitalisation, networking and integration. The use of computing and communication technology on board of ships, where the data is processed to provide critical information for different digital systems (for example, ECDIS, Dynamic Positioning system, integrated navigation system etc.), is increasing from year to year.

Maritime sector is particularly exposed to cyberattacks, which are understood as modification, disconnection, destruction, theft or unauthorized access to or unauthorized use of an asset. Cyberattacks might concern computer information systems, computer infrastructures, including IT networks, or personal computer devices [24], i.e. it can be any type of offensive activity aimed at information technology (IT) and operation technology (OT) systems, computer networks, and/or personal computer devices attempting to threaten, destroy or access ship systems and data [20]. An attacker in this case is a person or a process that attempts to access data, functions or other restricted areas of the system, without authorization, potentially with malicious intent [24].

Thus, maritime cyber security, understood as measures taken to protect network and computer assets both on ships, terminals, ports, and all computerized equipment supporting maritime operations, is an important aspect for maintaining the integrity of information exchange, without modifications and losses. Thus, the need for cyber risk management is becoming critically important [3].

It is significant for different actors of maritime sector to be more aware of, and better understand, the scope of safe information exchange which, by definition, shall guarantee the correctness of cyber operations and keep it protected and resistant against different manifestations of cyber-attacks.

The information exchange from the perspective of different actors and elements of cyber operations is discussed in this paper. The aim is to analyse the nature of information exchange in different operational situations on a ship, as well as from the perspective of different cyber systems onboard. The discussion is aimed at understanding which information is important for the safety of different operations, especially those onboard a ship and in one or other way related to the exchange of information. The goal is also to point out which kind of information and its exchange should be kept

under special supervision and should be covered by cyber risk management to treat this exchange as safe one. For this reason the taxonomy of information exchange with respect to different criteria is presented in the next chapter. However, the general aim of the discussion is to formulate conclusions and recommendations for maritime training processes. These recommendations could be considered for updating of academic curricula in relation to aspects of information security, safe information exchange and cyber security.

2.2 A taxonomy of information exchange

Information is a perennially significant asset in all organizations of different kinds and can be exchanged in different ways between different actors of the considered domain. In this chapter a taxonomy for information exchange is introduced. Based on the introduced taxonomy, different criteria and classification of information exchange in different ways is presented.

Based on the way of the information exchange, it can be classified as verbal and nonverbal. Verbal form means that the information is exchanged using spoken words in a natural form. Nonverbal exchange of information is also very natural but is carried out using established codes, marks, behaviour or flags (i.e. for example based on the International maritime signal flags). Sometimes nonverbal information exchange is customary, for example raising a flag when the ship is about to leave the port.

Information can be also considered with respect to its formal and unformal character. While unformal character of information is restricted to accepted rules of information exchange which are known for actors, the formal character of information is embedded in precisely defined and accepted rules and standards. Formal information can be formulated and exchanged as obligatory, on demand, for safety and protection of sailing ship traffic or for information for different marine services.

Based on the medium of information exchange, one can call it traditional or electronic. The traditional way of information exchange means that the information is exchanged in verbal form or using written or in other ways coded words (nonverbal).

Electronic information exchange, depending on type of the electronic equipment, can be digital or analog. It can be based on telecommunication infrastructure including radio, satellite or Internet connections, or it can be based on infrastructure dedicated to communicate between electronic units. The process of information exchange also depends on type of the medium and it can be wired or wireless.

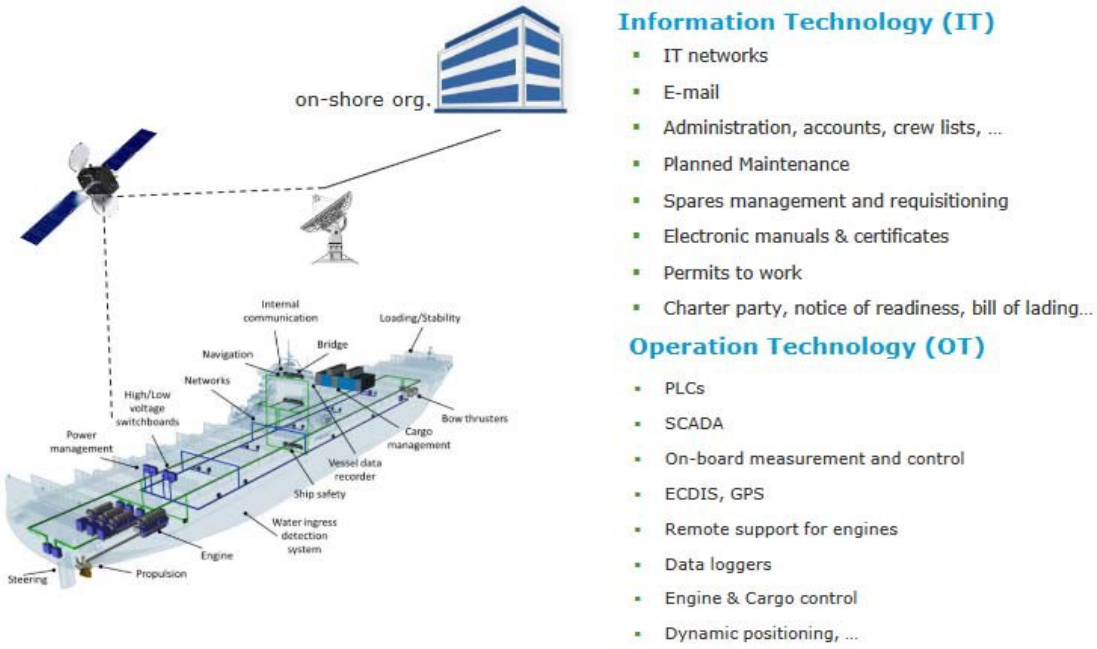

Figure 2.2. Information technology (IT) and operation technology (OT) on board of the ship [18]

Information can be forwarded directly to the recipients, which means that the information is addressed to a specified user of the system - it is also so-called direct mode. It is not a rule, that the exchange of information must take place exclusively between two actors. Information can be sent to all users of the system, without specification of the recipients and without any feedback. This type of communication is called broadcast mode. In this situation information is sent without any restrictions, in other words it is available for all users of the considered system. When information is dedicated for specific actors in the system, it means that information is at the same time prohibited for all others. The information can be exchanged between actors on board of the ship or it can be transmitted to actors on shore. In case of information exchange on board of the ship, it can be carried out between actors - persons (people) and systems. The systems can be classified as an information technology (IT) and operation technology (OT). IT systems focus on the use of data as information whilst OT systems focus on the use of data to control and monitor working parameters of different ship's units or processes. IT also covers the spectrum of technologies for information processing, including software, hardware and communication technologies. OT is hardware and software that directly monitors/controls physical devices and processes [20]. In case of such information exchange, the information is treated as input to the system. In the next phase, the information (data) is processed with respect to the assumed goals, but also based on specified procedures and rules. IT by definition can be used to process the data in many different ways. IT can process the data, which then can be used by the user personally, transferred outside of the ship via selected communication systems (via IT network or based on email), or it can be transferred to the OT as an input. The OT can then exchange information in a work-specific and natural manner.

Some of IT operations can be carried out using personal units (i.e. personal computer, mobile phone etc.) It is also possible to utilize available onboard units, which are intended for other purposes. Examples of information and operational technologies are presented in Fig. 2.2.

To sum up, information exchange can be carried out in various and diverse ways. The ways differ from each other in several dimensions. The differences can be considered with respect to the character, form, type and mode, and the kind of information being exchanged. These criteria refer to technical, technology, procedural and social aspects. The list of different criteria and examples of approaches for information exchanging under the umbrella of discussed taxonomies is shown in Table 2.1.

	Type/mode	Form	Character	Kind
Technical	broadcast direct wired wireless			within system
Technology	digital analog radio satellite internet			
Procedural and social		verbal nonverbal	formal unformal dedicated	obligatory on demand personal for safety

Table 2.1. Taxonomies for information exchange

2.3 Safe information exchange

As mentioned above, information is a perennially significant business asset in all organizations, therefore, it must be protected as any other valuable asset. This protection is the objective of an information security program.

The problem of safe information exchange concerns the process where two or more actors exchange information. The information can have different form or type, and the exchange can be carried out using different technical equipment and communication interfaces.

The aim of safe information exchange is to transmit information from one point to another using the established communication medium without loss any part of the information, with confidentiality, as well as with maintaining safety of the organization. Safe information exchange should be considered with respect to the safety management system. In general, safety management system integrates policy, objectives, plans, procedures, organisation, responsibilities and other measures with aim to manage safety elements of the organisation. Safety management system is crucial for organisations that deal with significant safety risks, for example within maritime industry [22].

Safe information exchange has also a relation with secure information exchange. However, in this case we should consider the problem with respect to the protection of information. ISO/IEC 27000 family of standards, being the formulated regulations with respect to the Information Security Management Systems, promotes confidentiality, integrity and availability of information as the

fundamental aspects of information security management. In this context confidentiality means that that only authorized persons can access the information, integrity means that the methods of processing information are accurate and complete, and availability means that only authorized users have access to it at any time [27].

Bearing in mind, that the use of electronic signals is typical for modern information exchange, and that the digital mode and cyber technologies are crucial and essential to the operation and management of numerous ship systems (i.e. integrated bridge systems, machinery management and power control systems, communication systems etc.) cyber risk management has become an important issue within the maritime industry. For instance, the IEC standard 61162-460 of digital interfaces for maritime navigation and radiocommunication equipment has been developed to address the need for higher safety and security standards due to increased exposure to external threats. According to the IMO Resolution MSC.428(98) on Maritime Cyber Risk Management [23], cyber risks should be appropriately addressed in the safety management systems of shipping companies. This IMO's resolution declares that cyber risk management onboard ships is mandatory as of 1 January 2021. The resolution confirms that existing risk management practices should be used to address the operational risks arising from the increased dependence on different operations based on digital processing, as well as using IT and OT in different ship spaces.

Thus, safe information exchange has a close relation with both cyber security and cyber safety. Cyber security is concerned with the protection of IT, OT, information and data from unauthorised access, manipulation and disruption. Cyber safety covers the risks of the loss of availability or integrity of safety critical data and OT. The fact is, that recent years have shown rapid growth in cyber-attacks on OT. It means, that effective cyber risk management should consider safety and security impacts resulting from the exposure or exploitation of vulnerabilities in different IT systems as well as in different procedures which concern using IT, procedures carrying out of the OT and guidance on the use of different devices by the crew and persons on board the ship [23]. In other words, the issues concerning cyber security and cyber safety need to be addressed by looking at systems, software, procedures and human factors.

From the practical point of view, cyber risk management, with respect to different real examples of information exchange between different actors, pays an attention on two pillars: people (human) and technology.

Up to 90% of all cyber security incidents can be attributed to human behaviour. Phishing and social engineering, unintentional downloads of malware, etc. are common issues, where human factor and unwise behaviour exist. On the other hand however, most members of ship crew are insufficiently prepared for handling cyber-attacks which results with behaviour that fails to reduce the damage.

In case of the human pillar two basic vulnerabilities have been pointed out [25], i.e. lack of awareness of cyber security and no ability to operate the devices like computers and their software. For example, the process of exchanging information onboard of the ship needs special attention paid to very basic activities with using of external devices. External hard drives such as USB sticks, camera memory cards and smart phones are very often used for storage. However they can spread malware and viruses in safety-critical systems. In such cases these devices offer for malicious malware a bridge across safety barriers to enter systems that are otherwise protected by network firewalls. Such irresponsible use of the external devices can infect other systems, including operational and strategic onboard systems. Once the malicious software has infected one computer, be it a personal or a company computer, it could spread itself to other units in the network, quickly paralyzing the system and making it impossible to perform important common tasks.

Software infections stemming from malicious malware or ransomware can be spread by unsuspecting and insufficiently trained users. This spreading is easy when the unsecured Internet access or insufficiently protected use of portable storage are in hands of the mentioned users [27]. Users are also inclined, by their curiosity, to use software of unknown origin, having some hidden functions and gaps that allow penetration of external systems to the users' devices. Loss of confidential information that can further be used to gain unauthorized access to personal or ship operational systems can be the result of such penetration. An easy process of sending or receiving emails can be also a source for spreading of malware and viruses. Infected computer can subsequently be a source of infection for other devices and computers onboard.

Another example of a potential cyber threat is connecting a personal wireless router or computer to an isolated network reserved for ship's operational equipment. In case the connected computer has been infected, the malicious software can spread itself to the operational software and consequently allow external systems to penetrate ship's devices. Such external software or its users can literally sit outside the ship and access critical onboard systems through wireless networks. For example, the navigation system could be manipulated by electronic GPS spoofing devices sending incorrect GPS signals resulting in deviation of the indicated ship's position from the actual one [25]. Thus, cyber-security is important with respect to the attacks on OT.

Finally, safe information exchange shall be considered also in reference to the human pillar. Attention should be paid to procedures and, in many cases, inclination to not follow the procedures and rules. For example, Fig. 3 presents eleven postulates by DNV to avoid cyber mishaps onboard the ship. They are strongly related to the process of information exchange, i.e. from procedural point of view, how the ship systems should be protected when information exchange is carried out.

Technology pillar of the cyber risk management concerned safe information exchange and is mainly related to the proper preparation of services and devices - adequately and according to procedures of cyber security. The technology pillar is very important and is beyond the influence on the human factor (users). However, it is really close to the users of different hardware and software. This pillar concerns a large number of aspects, for example:

- proper configuration of software and network,
- monitoring of ship's IT network,
- use of virus defence and firewall,
- system upgrades and timely virus database updates,
- use of cryptographic protocols,
- making information (data) backups,
- monitoring of ship's systems and detection and monitoring of fraudulent behaviour,
- management of the access to resources policy (password control, remote access control, users account management),
- remote management of user's software (removing or blocking unnecessary software functions & plug-ins).

To sum up, the safe information exchange depends on technology aspects, e.g. requirements imposed on this pillar. Assuming that the minimum technology requirements are met, safe information exchange depends largely on proper human behaviour. Nevertheless, the protective activities must go beyond the traditional focus on IT and a human behaviour. These activities must be undertaken keeping in mind the biggest risks of attacks on ship's OT. One of the activities, although not technical, deals with professional skills and qualifications of the personnel, thus extending the issue to the training domain.

Figure 2.3. Best practice by DNV [25]

2.4 Maritime training on safe information exchange

Safe information exchange is crucial for the management of cyber security. As it has been shown, even very simple operations can have influence on security and safety of shipping. Information exchange irrespective of the form, character, kind and mode can be a safety risk for the ship, people, environment and goods, if the users of different technical equipment and software are not aware of cyber risks and do not use the equipment in a safe manner.

Thus, there is a need to introduce regular training on cyber security awareness and safe operation of technical systems. In general, the ship's crew should understand potential vulnerabilities in computer based systems and have knowledge about appropriate technical and procedural protection measures. Operational and technical personnel should understand that they are responsible for the safety of critical systems onboard the ship. Cyber awareness training is not at the moment a mandatory requirement. However, training is a protection and control measure that forms the basis of cyber risk management. Cyber threats are more often related to operational procedures and crew training, than to the IT hardware and OT systems.

Successful preventing, spotting and fighting against cyber-attacks asks for cyber security skills and ability to evaluate potential cyber risks. It is necessary to implement proper cyber risk awareness on all levels of seafaring professions. Such cyber risk awareness shall be built by education and training.

Training on management of maritime cyber security is extremely important and should be carried out on all maritime education levels. That is of great importance especially on the bachelor level and higher levels of marine navigation and marine engineering. These graduates will potentially become captains or chief engineers of ships, and proper action and attitude related to cyber security is expected from them. They will also carry the highest responsibility of cyber risk management onboard the ship.

As a part of this work, randomly selected study programs in the field of navigation were analysed. Ten different bachelor degree programs on navigation in ten European maritime universities were analysed. The analysis was carried out to find out the contents in the curricula about cyber security on board of the ship and, in general, within shipping industry.

None of the study programs included courses in maritime cyber security. Two of them included courses on the basics of computer science with some elements of cyber security.

The result of the analysis was poor and unsatisfactory considering the extremely important issue of cyber security and the need for proper cyber risk management onboard ships. So, it is vital to immediately start updating the academic curricula in relation to the information security aspects, safe information exchange, cyber security and cyber risk management. The updating should be mandatory for all academic programs, especially within the education of merchant marine officers.

2.5 Conclusions

In this paper the issue of safe information exchange has been discussed. Firstly, we presented the taxonomy of information exchange. Then, the safe information exchange was discussed taking into consideration different aspects according to type, character, mode and role of the information exchange. The main conclusion from this discussion was that cyber risk management can be based on two pillars: people (human) and technology. The two pillars were then characterised with respect to the safe information exchange process. The final part of the paper was focused on aspects about the training and qualifications of seafarers to cope with cyber risks. It was found out that the existing training programmes for deck officer students are not sufficient in relation with the character and importance of the problem. The final conclusion is the recommendation to update the academic programs accordingly. In the future, specific recommendation on the contents of academic curricula will be formulated and discussed.

3. Addressing Cyber Security In Maritime Education And Training

This chapter presents the results of literature study of the present status of cyber safety training requirements in IMO STCW code and an assessment of the present status of education and research on cyber safety issues in IAMU member universities based on a questionnaire survey.

3.1. Introduction

Cyber safety is a highly topical and growing issue for sea transportation systems in terms of automation and autonomy, digitalization, IoT and other web-based applications. Maritime sector is also particularly exposed to cyber-attack, which is understood as modification, disconnection, destruction, theft or unauthorized access to or unauthorized use of an asset [28]. Cyber-attacks concern computer information systems, computer infrastructures, including IT networks, or personal computer devices [29], i.e. any type of offensive activity aimed at IT and OT systems, computer networks, and/or personal computer devices attempting to threaten, destroy or access ship systems and data [30]. An attacker in this case is a person or process that attempts to access data, functions or other restricted areas of the system, without authorization, potentially with malicious intent [29].

Thus, a maritime cyber-security, understood as measures taken to protect network and computer assets both on ships, terminals, ports, and all computerized equipment supporting maritime operations, is an important aspect for maintaining information exchange, without modification and loss. Thus, the need for cyber-risk management is becoming critically important [31].

Seafarers are at the frontline of management in the maritime domain and they are often the only barrier between success or failure when it comes to protecting the integrity of the data systems on board ships. Marine cyber safety should therefore be taken more into account in training, education and research and development initiatives of maritime universities.

The CYMET project aims at promoting maritime safety by increasing the awareness of cyber safety issues related to ships and maritime transport, and the proper consideration of these themes in education and research activities of the IAMU member universities. The project evaluate demands in training of seafarers, and provide a recommendation on how cyber safety should be taken into account in maritime education and training.

This paper presents the results of literature study of the present status of cyber safety training requirements in the IMO STCW code and an assessment of the present status of education and research on cyber safety issues in IAMU member universities based on a questionnaire survey.

3.2. Definitions and important terms

The issues related to cyber risks is essentially issues related to the exchange of information between different sources of information. There are basically three actors in information exchange; receivers, transmitters and transceivers. The last is a combined transmitter and receiver. In most modern operation technology (OT) and information technology (IT) systems only transceivers are operating. Examples of transceivers are humans, computers, mobile phones, programmable logic controllers (PLC's) or printers, where as examples of transmitters can be pressure transducer or temperature sensor.

Whenever information is transmitted, there is a risk that it does not reach the intended receiver in complete and unaltered form. This issues is termed transmission risk. When the information is exchanged via electronic communication channels of any kind, that has some form of connection to the internet, the issue is termed cyber-threat or cyber-risk. There can be threats against the information at the transmitter and at the receiver. A threat is any event that can alter either the information itself or the receiver of the information or both. Handling the lines of communication themselves and keeping them free from intentionally harmful human involvement is termed as communication security. Again, when the communication lines involve any kind of access to the internet, it is termed cyber-security or IT security and is essentially secure information exchange. Secure information exchange is dealing in the triad of confidentiality, integrity and availability of information as the fundamental aspects. In this context confidentiality means that only authorized persons can access the information, integrity means that the methods of processing information are accurate and complete, and availability means that only authorized users have access to it at any time [32].

The information itself can however also be faulty and IT security is not dealing with this issue. When faulty information is introduced into the secure communication system in can be treated in a completely secure manner but it is still un-safe information. The IT security management systems should address intentionally attempts from harmful sources that tries to introduce un-safe information into the communication system, but un-safe information is very easy to introduce into the communication system by way of mistake from the transmitter or faulty transmissions and this is very difficult to manage with traditional means of communication security. Exchanging complete and unaltered information that is correct and safe to use is termed safe information exchange [28]. Keeping a communication system, either an OT or IT, safe to use is then termed cyber safety management or, since it is addressing cyber-risk in order to maintain safety, cyber-risk management. Cyber safety management aims at keeping the uses, both humans and other transceivers, unharmed by the information exchange and at the same time incorporating the three aspects of cyber-security; confidentiality, integrity and availability of information. Cyber safe systems should be either protected from ever receiving un-safe information or include fault-tolerant information processing in order to eliminate potentially harmful events to occur based on the processing of un-safe information. All ship systems, like any other life-supporting system, should be build cyber safe and the risks of threats leading to harmful events should at all times be addressed by a cyber-risk management system.

3.3. The present status of cyber safety training requirements in the IMO STCW code

The International Maritime Organisation, IMO, is the United Nations specialized agency with responsibility for the safety and security of shipping and the prevention of marine and atmospheric pollution by ships. Among the agreed conventions is the code for standards of training, certification and watchkeeping for seafarers, STCW code. The STCW code contains all requirements for education of seafarers in all aspects. It is however the minimum requirements, that the seafaring nations has agreed upon and as such, the individual training program governed under a flag state can vary to some extent, but all training programs worldwide honors the STCW code.

3.3.1 Security training according to ISPS and STCW section A-VI/5 and A-VI/6

The STCW section A-VI/5 and A-VI/6 incorporates the training for seafarers in order for them to be able to fulfil their duties in accordance with the International Ship and Port Facility Security (ISPS) Code. This code which is an amendment to the Safety Of Lives At Sea, SOLAS, aims at addressing all aspects of security, but fails to address threats related to communication systems and neither OT or IT systems is mentioned anywhere. Still this training is mandatory for all seafarers as various levels,

ranging from the Ship Security Awareness certificate issued based on Section A-VI/6-1, over Designated Security Duties certificate issued based on Section A-VI/6-2 to Ship Security Officer issued based on Section A-VI/5. For port and company there are similar requirements for training. It is rather peculiar, that the threats against the IT and OT systems through lines of communication is not addressed in these sections. The ISPS code was agreed on after the shocking events of 9/11[33]. It is as though the founders of the ISPS code were not aware of the potential threats through the open communication channels of the OT and IT systems in the maritime domain and especially on board ships. The ship security training provides generic skills in aspects of risk, threats, security and safety and in assessment of procedures set in place to manage security and safety. This training could be extended to specifically include cyber-risks.

3.3.2 Relationship between ISM and STCW

In the STCW code, Section A-I/4, point 2, the ISM code is effectively set in force for the entire STCW code as the framework for the procedures, that seafarers should be trained to comply with. The International Safety Management (ISM) code, which also is an amendment to SOLAS, is dealing with all aspects of safe ship operation. This does also include management of cyber-risks, even though they are not mentioned specific at present, and as such all seafarers should be trained on appropriate level to carry out ship board procedures set in force for protecting the ship against cyber-risks and thereby ensuring that the ship is cyber safe at all times. In the ISM code the responsibilities of setting up the procedures to ensure cyber safety is laid down on the company that operates the ship [34]. Bearing this in mind, cyber safety should be incorporated in all education and training, that involves exchange of information with the use of any IT or OT system regardless of the system purpose. The ISM code is frequently discussed under the Maritime Safety Committee (MSC) of the IMO and in the 98th session held in June 2017, the MSC adopted a resolution on how to assess the proper implementation of cyber-risk management in the ISM [35]. This resolution, [36], calls on all administrations of the flag states to ensure that cyber risks are appropriately addressed in safety management systems under the ISM code no later than the first annual verification of the company's Document of Compliance after 1 January 2021. Training and education in aspects of cyber-risk management should therefore be well implemented already in all relevant aspects of STCW training and education regardless of flag state or training provider.

3.3.3. Training according to STCW section A-III/6, A-II/2 and A-III/2

In the STCW code, Section A-III/6, the minimum criteria for electro-technical officers is stated. This section deal with all parts of system assessment, operations, maintenance and repairs of electric, electronic, automatic, control systems, alarm systems, monitoring systems, communication systems, IT systems, computers, computer networks and navigation equipment. It does not specifically say anything about maintaining cyber safety, but since this is a part of the ISM code and therefore implicit something that all the stated requirements in the STCW code must comply with, the persons have a certificate of competence as electro-technical officer should be fully qualified for maintaining cyber safe conditions on board the ship they are serving at, provided that the operating company has provided the ship with suitable procedures and equipment. Similar for the training of management level in navigation in section A-II/2 and management level in engineering in section A-III/2. When it is described, that the holder of the certificate is capable of managing the equipment and keeping it in operational condition in accordance with established procedures, then it should implicit be understood, that it also implies keeping the ship cyber safe, since all procedures must be described in the ships ISM manual and cyber safety is part of ISM.

3.4. Results of the questionnaire survey among IAMU member universities

The first round of the survey was send out using the site SurveyMonkey.com, [37], to all IAMU members by way of the official list of contact mail addresses obtained from the IAMU Secretariat. The second and third round was sent out by the email address jmo@simac.dk containing a link to the survey at SurveyMonkey.com. In total 32 responded from 18 different IAMU member universities. The breakdown of respondents in member groups is listed in table 3.1.

Europe and Africa (37 members – 11 respondents, 30%)

Arab Academy for Science, Technology and Maritime Transport, Egypt

Admiral Ushakov State Maritime University, Russia

Chalmers University of Technology, Sweden

Faculty of Maritime Studies University of Rijeka, Croatia

Gdynia Maritime University, Poland

HSB | City University of Applied Sciences, Bremen

Nikola Vaptsarov Naval Academy, Bulgaria

Satakunta University of Applied Sciences, Finland

Svendborg International Maritime Academy, Denmark

TalTech Estonian Maritime Academy, Estonia

University of Southeast Norway, Norway

Asia, Pacific and Oceania (18 members – 5 respondents, 28%)

John B.Lacson Foundation Maritime University, Philippines

Kobe University, Japan

Maritime academy of Asia and the Pacific, Philippines

Maritime State University named after Admiral G.I. Nevelskoy, Russia

Myanmar Maritime University, Myanmar

Americas (9 members – 2 respondents, 22%)

Texas A & M University, USA

Universidad Tecnológica del Perú, Perú

Table 3.1: List of participants, listed according to IAMU member groups, [38].

The overall IAMU member respondent percentage is 28%. This low number combined with the low number of total respondents leads to the fact, that the conducted survey can only at best yield some indications of the present state of education and training in cyber safety related issues among IAMU member universities.

3.4.1 Results of the questionnaire survey - Field of Teaching.

In figure 3.1 is the results of the first question listed. The respondents had the opportunity to give more than one answer. The list is divided in two groups; those who include issues on cyber safety in

teaching (marked with blue) and those who do not (marked with orange). The results reveals that only two IAMU member universities do not include any teaching in cyber safety issues. In total 5 respondents do not include issues on cyber safety in their teaching. The respondents that do include issues on cyber safety are covering a broad range of Fields of Teaching. This is in good coherence with the ISM code and the STCW code as seen in section 3, where issues of cyber safety should be addressed in education and training in relation to the technology that can be affected. Only one respondent teaches the subject cyber security as a dedicated Field of Teaching, but this can also be related to the build of the questionnaire, where this was not a predesigned answer option. The respondent put it in under the option "Other". All of the respondents who teaches IT does include issues on cyber safety, whereas the rest of the Fields of Teaching can be collected under OT and here the results are more scattered. For Technical navigation and Maritime Technology it is almost half of the respondents who do not include any issues on cyber safety.

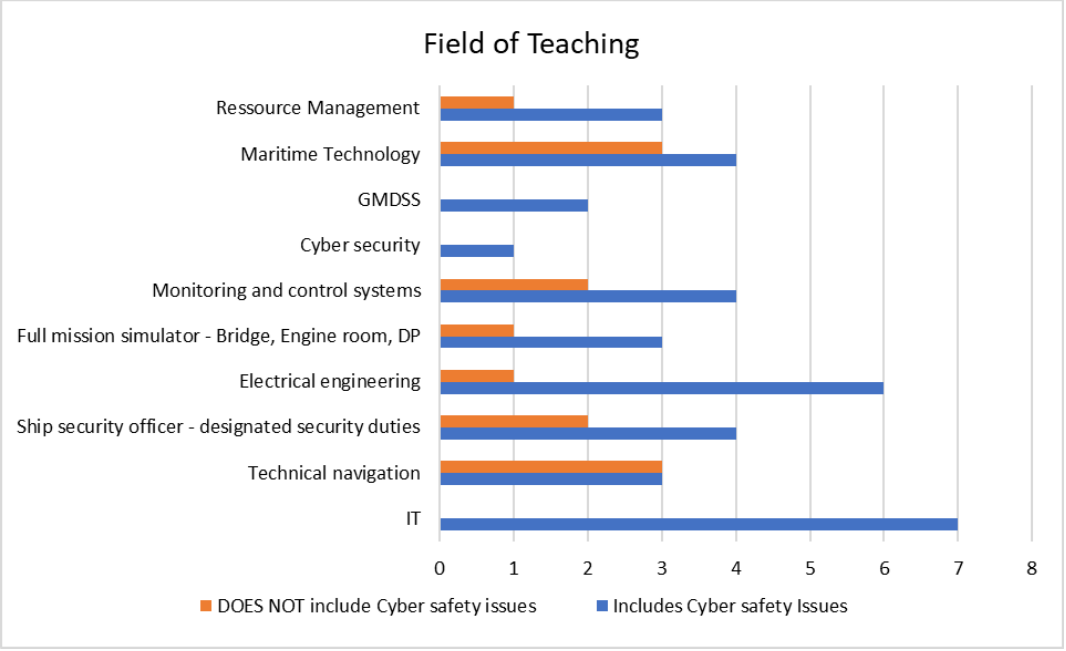

Figure 3.1: Listing of respondents answers to Field of Teaching grouped in respondents that do not include cyber safety issues in teaching and respondents who do.

3.4.2. Results of the questionnaire survey - Topics included in Teaching.

The topics included in the teaching on cyber safety issues are listed in figure 3.2. Almost everybody includes teaching on risks. Here again the respondents had the option of providing multiple answers. Those who do not include risks, do only include empirical/ historical accounts of events, which is also a way of raising awareness. The actual assessment of vulnerabilities is an extra topic provided as answer under "Other", by the same respondent who teaches cyber security as a Field of Teaching. The answers provided shows that teaching among IAMU member universities is focusing on risks and awareness and how to take protective measures. Combining it with the answers on Field of Teaching, this is mainly addressed towards IT systems and to some extent also for OT systems.

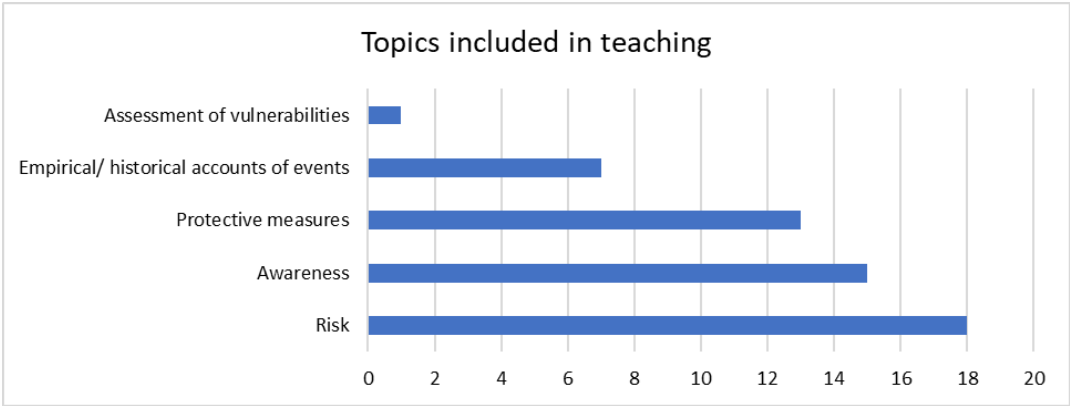

Figure 3.2: Listing of respondents answers to Topics included in Teaching on cyber safety issues.

3.4.3. Results of the questionnaire survey - Teaching Material/ Method applied.

The topics on cyber safety is brought forward to the students by applying the Teaching Material/ Method listed in figure 3.3. Almost all respondents are using lecturing as a means of teaching and of those the majority do so by help of PowerPoint presentations. A large part also include group work and exercises. Only slightly less than half includes self-paced learning of some form. Those respondents, who do not use lecturing are only using self-paced learning to cover the topics. The one respondent who goes to seminar work provided this answer under "Other" and it is the same person who teaches cyber security as a Field of Teaching. Interestingly that respondent do not use self-paced learning, even though this is one of the most common ways of providing awareness training on cyber security for IT systems.

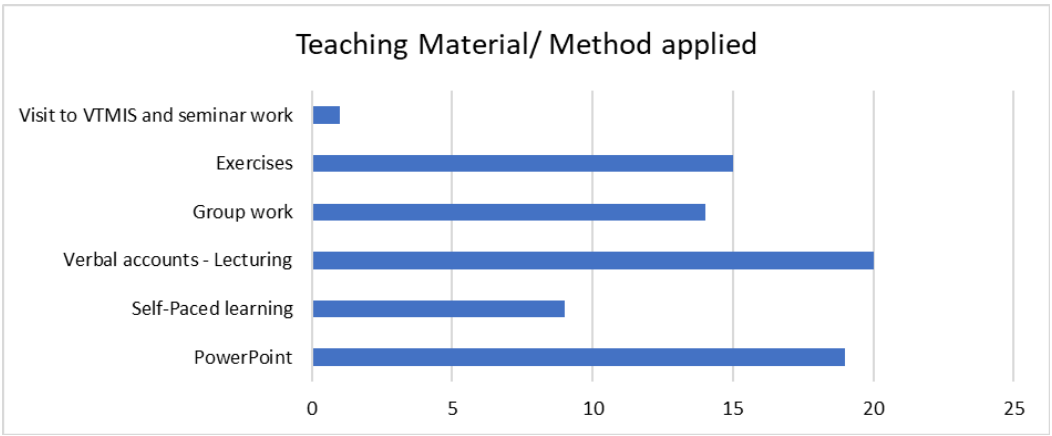

Figure 3.3: Listing of respondents answers to Teaching Material/ Methods applied in Teaching on cyber safety issues.

3.5. Conclusion

Based on the study it can be concluded, that not only cyber security but also cyber safety is needed to be addressed in maritime education and training. It is already a mandatory requirement under the ISM code although it is not specifically mentioned. It can also be concluded that education and training should address all aspects of cyber safety issues for both IT and OT systems, since the ISM code aims at managing the ship in a safe manner, handling all risk to a sufficient level. The survey among the IAMU member universities indicates that education and training on cyber safety issues are incorporated to some extent at a number of universities and in a variety of Fields of Teaching covering both IT and OT systems. It also reveals that self-paced learning is not applied by the majority of the respondents in the survey. This could be because of the special application of IT and OT systems in the maritime domain and the lack of special developed training packages on cyber security and cyber safety issues for the maritime domain. This is not known, but could be explored in future research.

4. E-learning Material for training of Maritime Cyber Security

4.1. Introduction

In all areas of higher education the use of the internet and web-based learning have gained much attention, for several reasons. Firstly, the internet is a source of useful material for educational purposes. Secondly, affordable and versatile software tools are available for development and running web-based courses. Thirdly, conducting lectures online for a larger number of students is cost-effective. Fourthly, web-based courses can be followed online by students anywhere in the world.

The convention on Standards of Training, Certification and Watchkeeping (STCW) by IMO forms a useful basis for collaboration between maritime education providers. Since STCW forms the minimum standard for training of seafarers, the essential contents of training material should consist of similar elements all over the world. Naturally, this does not fully apply in reality due to linguistic and cultural differences, variation in the educational system between countries and different pedagogical methods applied. However, there may be unexploited potential in producing training material in collaboration between MET institutions.

The objective of the CYMET project is to increase the knowledge and awareness of cyber safety issues within the seafaring industry and to enhance proper consideration of these issues in education and research activities of the IAMU member universities. One of the concrete outcomes of the CYMET project is a package of web-learning material on maritime cyber security management, developed by the partners SAMK, GMU and SIMAC and made available for all IAMU member universities.

Even though it might be challenging to compose a uniform and unified set of training material produced by several teachers from different universities, this kind of collaboration can be very beneficial and rewarding. Wider collaboration between the member universities in production of web-learning material should be considered in IAMU. It could be used to enhance the quality of education and training of seafarers globally. The Basic Agreement of IAMU states: *The members shall cooperate with each other in a range of scientific and academic studies, developments, and practical applications associated with Maritime Education and Training and endeavour to achieve measurable and worthwhile outcomes for Maritime Education and Training through IAMU activities*.

4.2. Some pedagogical aspects of web-based learning

Efficient web-based-training, especially when it is based on self-education, must be based on different pedagogy and didactics than traditional face-to-face classroom lecturing. The World-Wide-Web became popular in the early 1990's. The new possibilities offered by the internet for training and education were discovered soon by education professionals. Exploiting of these new possibilities started in different variations of e-learning and web-based learning. Today we have already over 20 year's experience of utilizing internet on all levels of education.

One can't say that the results of web-based training are worse or better than the results of traditional face-to-face classroom training. There are many other things affecting the learning process than just the applied technology. Figure 4.1 shows that even though we can place the technology to the centre of the educating process, there are such factors as pedagogy, implementation and even institution playing an important role in this process.

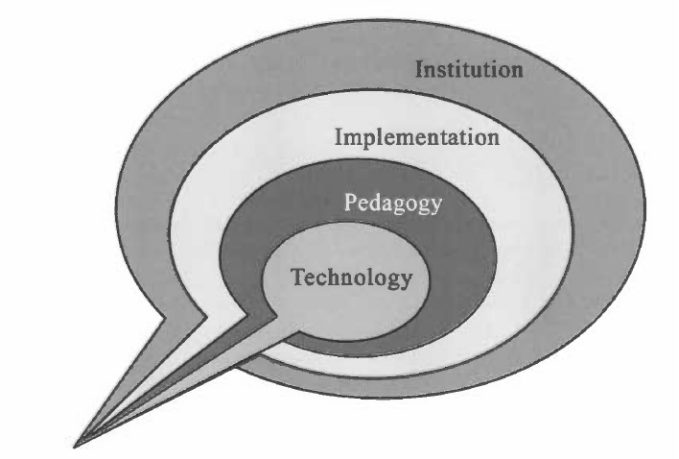

Figure 4.1 The four components of flexible learning in higher education [39]

Learning is a complicated process affected by a large amount of factors starting with motivation of the student - and the teacher- , experience and the learning style of the student, learning environment, readiness to utilize the technology, language skills, timing, structure of the material, visual outlook of the training material, stress, fears, other emotional factors and so on. There are hundreds of books and thousands of scientific articles written about training and pedagogical theories. Although deeper analysis of these matters is beyond the scope of this report, there are some aspects worth mentioning, that should be taken into account in development of web-based and self-learning courses. These are some – not all – features of a good web-learning course:

- In the beginning of the course, it is important to wake up the motivation to learn and the curiosity of the student towards the subject in concern. This can be done for instance by presenting a video of an eye-opening case from real life. It is said that "wondering is a key to learning".
- The self-learning course should be organized so, that the student can study it in smaller pieces. The material should be divided into lessons or chapters. It should be organized in a logical order guiding the student to build his/her knowledge effectively.
- Each lesson or chapter of the self-learning course should end with control questions or exercises which provide the student with feedback about his/her progress.
- The typical amount of student's working hours should be in balance with the amount of credit points earned from passing the course.
- The English language of the material should not be too difficult to understand. It must be kept in mind that the students of the self-learning course come from different parts of the world and that many of them do not speak English as their native language. All difficult terms and phrases should be explained for instance by using pop-up type help texts.
- A good web-learning course is exciting. If there are enough resources available, the attractiveness and effectiveness of the self-learning course can be enhanced by using simulations and challenging interactive functions, like in video games, into it.

The internet contains an enormous amount of ready-made videos, lectures, presentations, articles, photos, graphics etc. that could be useful for the self-learning course. However, the teacher has to keep in mind that the international and national copyright laws shall not be violated.

Web-based learning fits quite well in the subject of maritime cyber security management, for the following reasons:

- the focus is in building of knowledge, not in training of practical skills,
- the theme is global: the goal and the contents of the training are the same all over the world,
- the subject has a natural direct connection with the applied web-based learning technology,
- there is a huge amount of useful and up-to-date material about this topic in the Internet.

Additional benefits from using web-based self-learning as the training method in CYMET project are:

- publishing and updating the training material in electronic/digital format in stead of printed format is more cost-effective,
- web-based course is scalable, i.e. the amount of students attending the course is not limited (at least theoretically),
- it is possible to share a web-based course quickly and with no extra cost to all IAMU member universities..

4.3. Selection of the web-learning platform

Before the web-learning material could be developed and made available to IAMU member universities, the software tool for producing, sharing and using the material in teaching had to be selected. The platform to be chosen should meet at least the following criteria:

- the material should be available to IAMU member universities,
- the platform should be commonly used,
- it should be easy to use and simple to maintain,
- it should contain key functions and features of an advanced web-learning platform.

An important aspect is also the price of using the platform. If possible, it should not be too expensive, preferably free.

There are number of web-learning platforms, services and systems available on the market. Based on a brief preliminary study about the supply the project group decided to have a closer look at two alternatives: **Moodle** and **Itslearning**.

4.3.1 Moodle

Moodle is said to be the most popular web-learning environment worldwide among institutions of higher education. Moodle is a free open source code software system, originally developed by Martin Dougiamas. The first version was released in 2002. According to Wikipedia, the Moodle Project is led and coordinated nowadays by an Australian company Moodle HQ and it is financially supported by a network of Moodle Partner service companies worldwide. According to Moodle.org -home pages, Moodle has at the moment (May 2019) over 150 million users in 227 countries.

Moodle is widely being used also by the member universities of IAMU. Figure 4.2 shows a typical lay-out of a Moodle web page (a snapshot from https://www.moodlebites.com), although a Moodle course can also look very different.

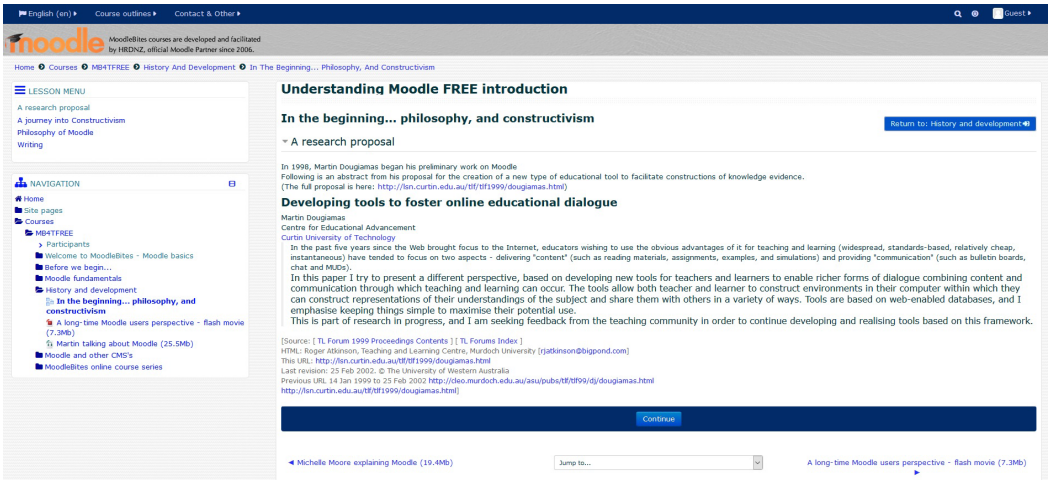

Figure 4.2. A sample page of Moodle (https://www.moodlebites.com)

IAMU has established an e-learning portal on its web pages. It is also based on Moodle. It was realized that if the member universities want to use the courses at the IAMU e-learning portal, they would need to install the Moodle course to their own server. IAMU does not apparently have resources for taking care of thousands of student enrollments from maritime universities worldwide and for online maintenance of the system, which would be required to provide the users with a proper and reliable service. On the other hand, this kind of service hardly belongs to the core activities of IAMU.

4.3.2 Itslearning

As an alternative to Moodle, the cloud based learning platform Itslearning was studied by the CYMET project group. Itslearning is a commercial service, maintained and distributed by the company Itslearning AS, Norway. Itslearning was developed in Bergen, Norway, in 1999 and according to Wikipedia it is said to have over four million active users worldwide.

Itslearning is a comprehensive learning management system offering tools for curriculum management, objective-based course plans and assessments in one online location. The platform gives easy-to-use tools for creating online courses, for collaboration and sharing materials, and it automates routine tasks within the education processes of the institution.

From IAMU's point of view, there would be some advantages of using a cloud based system like Itslearning:

- the courses are available worldwide without the need to download and install material to the university's own IT system,
- enrollment of students from different universities is managed by the system,
- development and maintenance of the course material in collaboration of several teachers is easy.

On the other hand, since the service is not free, the costs of using Itslearning may reduce the willingness of using the service. However, pricing today (May 2019) is rather moderate and it is based

on the number of students. Moreover, it includes full maintenance of the system, which reduces indirect costs on the IT management side.

After studying these two alternatives, Moodle at the IAMU e-learning platform was chosen unanimously by the project group for producing and publishing the web-learning material on maritime cyber security. The main reasons to this decision were:

- Moodle is more widely used and it is already familiar to the member universities of IAMU,
- Moodle is free,
- the e-learning portal on the web site of IAMU is based on Moodle.

Especially the last argument was seen important. The CYMET project group did not see any reason for creating another e-learning environment for the members of IAMU. Although Moodle has some weaknesses compared to Itslearning regarding the management of student enrollments and the need to download and install the course material to the IT system of each university, it clearly fulfills the requirements for a functioning web-learning platform.

The web-learning course and additional material for maritime cyber security training developed during the CYMET project can be found at http://iamu-edu.org/moodle/. A username/password issued by the maintenance of IAMU e-learning platform is required for accessing the material.

It would be a strategic decision by IAMU to establish or buy a cloud based service for development and maintenance of jointly developed e-learning courses in stead of the present IAMU e-learning platform.

4.4. Joint production of the training material

A web-based training package on cyber security issues for maritime professionals was created jointly by the partners of the CYMET project. The material consists of texts, images and links to relevant material in the Internet. Personal exercises were included to provide the students with feedback of the progress of their learning. It was agreed by the producers of the material that each member will produce the material for one whole chapter and then the chapters are put together to form the whole course. In other words, there was no group work was done during the production. However, the producers had the possibility to study and comment the others' texts.

One could say that this is not the best way of working together from the point of uniformity of the result. But due to limited resources of CYMET project this was the only practical way to get the work done. However, it would be better in the future to have a named editor, or a group of editors, having the responsibility of checking the material and editing it into a standardised format. Also updating the course material in the future must be considered. The editor could assure the correctness of the contents, the correctness of the English language and the uniformity of applied expressions and terminology.

Another important area of consideration is copyright regulation. There might be differences in Copyright rules and practices from country to country. The material must be produced in such a way that it will not violate any international copyright legislation.

4.5. The IAMU Maritime Cyber Security web-learning course

The learning package was designed for 100% self-education and it was organized into seven lessons:

1. Introduction
2. Understanding cyber threats
3. Awareness across the organization
4. Elements of cyber security management
5. Good practices
6. Rules, standards and guidelines
7. Examples from the real life

The material consists of plain text with links to videos and articles in the internet and multiple choice questions in the end of each lesson to give the student some feedback about learning of the contents of the lesson. Due to the amount of available resources, it was decided by the project team, that no animations or videos would be developed within this project.

The target group of this web-learning package includes all persons within the maritime industry, who should be aware about cyber threats and who should know the basic principles and guidelines about management of maritime cyber security. So this course could be the first course about maritime cyber security and it could be complemented with more advanced courses providing the students with deeper knowledge and skills about practices of cyber security management. However, some good practices are introduced in the 5th lesson of this training package.

The training material developed by CYMET project contains also additional special chapters, which were not included into the basic course. They can be used in the advanced courses mentioned above. The additional topics included in the material package are:

1. Network integrity
2. GPS jamming and spoofing
3. Safe information exchange

The front page of the web-learning package is shown in Figure 1. The material is organized into seven lessons or modules. The last module contains the feedback questions used in connection with the pilot testing of the course.

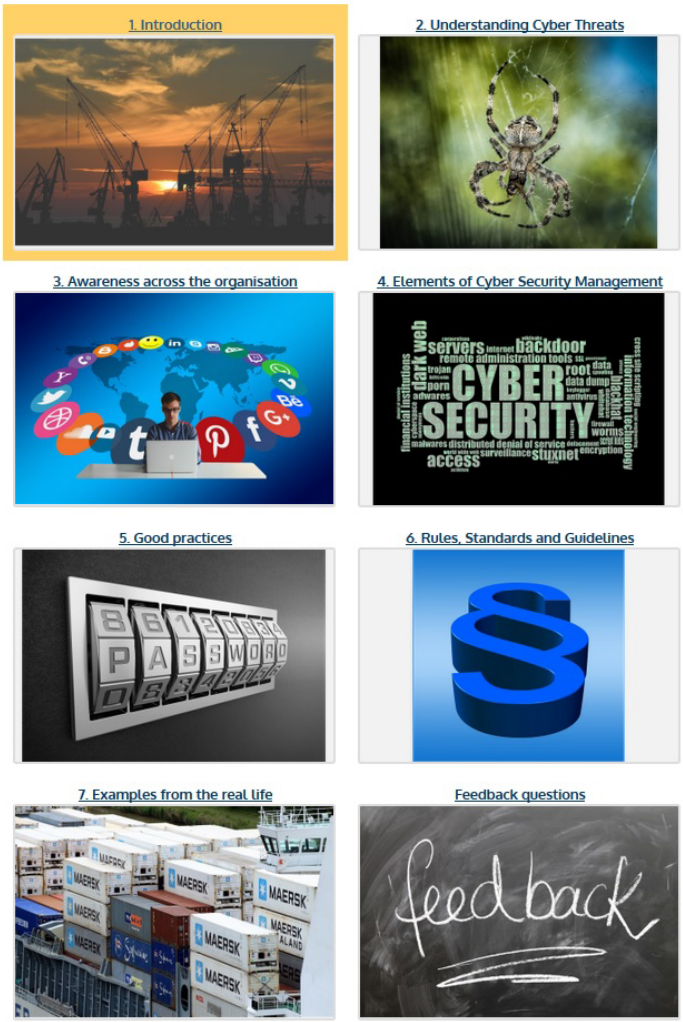

Figure 4.2. The modules of the web-learning course.

There is a sample text from Module 2 “Understanding cyber threats” in Appendix A. This text is followed by links to additional material in the internet, i.e. videos, news articles, research papers etc. on the subject in concern. The student is asked to read through the text, to watch the videos and to study other additional material behind the links. After studying the material the student should answer a few questions about the studied topic. The questions are not for assessment purposes, but for providing the student with feedback about his/her progress.

4.6. Pilot tests of the web-learning course

The web-learning course on maritime cyber security has been pilot tested by students of the participating universities in Finland, Denmark and Poland. The Students have been asked to study the material on the Moodle course and after completing the course to give feedback by answering the following questions:

1. How long did it take to complete the course?
2. Did you find the contents of the course interesting?
3. How was the development of your knowledge about maritime cyber security?
4. Was the course suitable for self education?
5. How was the difficulty of the course?
6. Did you have problems in understanding the English language?
7. Is the coverage of the course OK, or perhaps too narrow or too wide?
8. Were the instructions for using the self learning course sufficient?
9. Were the instructions for using the self learning course clear enough?
10. Do you want to give any other feedback about the course (open question)?

The response to the feedback questions indicates that this web-learning course was found useful, interesting and suitable for self-learning. Some of the students felt that the topics were somewhat too general, i.e. they would prefer more examples from the shipping industry and about ship equipment, even though the real life examples of cyber-attacks were taken from the shipping world. Some of the students had difficulties in understanding the English language, which is quite understandable, since none of the students were native English speakers. The amount of feedback is not big enough to draw stronger conclusions, but the impression is that the developed web-learning course does not require any significant corrections or modifications so far.

Another important source of feedback would be teachers of IAMU member universities. However, during the CYMET project it was not possible to collect this feedback.

4.7 Conclusions

Joint production of web-learning material is a promising idea, since maritime universities and other MET institutions around the world have a shared need to develop and run courses on same topics about seafaring and marine technology. However, it has been seen in practice that teachers do not necessarily like to use material (texts, PowerPoint presentations, exams etc.) made by someone else. They prefer to use material created by themselves. Lecturing is a very personal matter. It can be compared to coaching or performing arts. An experienced lecturer may not want to follow the logic of another lecturer's presentation, because he/she may prefer another approach to the subject in concern or he/she wants to put emphasis and priority on matters differently than the colleague who made the presentation. The reason for omitting the ready-made material could also be the English language. Or there might be technical problems.

Despite of these challenges, the international maritime education community could benefit from collaboration in the area of training material development. By utilizing the best available expertise within its member universities, IAMU could promote the quality of MET globally. There is room for joint development of training material on selected topics. Management of maritime cyber security is one of those topics. Maritime cyber security is a highly critical area for the shipping industry and there is an acute need for training of seafarers to be aware of and to cope with cyber threats. This area is new and it is developing rapidly. That's why the use of best possible expertise for training on this area is important.

Jointly developed web-learning material should be as easy to use as possible. The best solution from the teacher's point of view would be to create a high-quality self-education course and to make it available through a cloud service. However, it does not fall in the area of core activities of IAMU to maintain such services. The solution could be to outsource the cloud service for IAMU web-learning

courses. In that case all IAMU member universities would have to become customers of this service provider.

Another solution would be to use IAMU web pages as a storage of material that could be downloaded and installed to the member university's own computer network. This approach was selected in CYMET-project. The web-learning course has to be downloaded from the IAMU e-learning platform (Moodle) and installed on the member university's own Moodle server.

The web-learning course was pilot-tested at GMU, SIMAC and SAMK. The feedback from students has been positive.

An important matter for the future is the maintenance of the developed course. The contents of the web-learning course on maritime cyber security should be updated on a regular basis. A proper mechanism for continuous updating of the course material is necessary.

5. Final conclusions and recommendations

This research project 'Addressing Cyber Security in Maritime Education and Training' (CYMET) was carried out by Satakunta University of Applied Sciences (SAMK), Gdynia Maritime University (GMU) and Svendborg International Maritime Academy (SIMAC) between May 2018 and May 2019.

Both cyber safety and cyber security are growing issues for sea transportation systems in terms of automation and autonomy, digitalization, IoT and other web-based applications. As technology has developed, information technology onboard ships has become safety-critical and networked. A cyber-attack could be an intentional attempt to modify, disconnect, destruct or to unauthorizedly access or use an asset. Within the marine transportation framework cyber-attacks concern computer information systems, computer infrastructures, including Information Technology (IT) networks, or personal computer devices, i.e. any type of offensive activity aimed at IT and Operation Technology (OT) systems, computer networks, and/or personal computer devices attempting to threaten, destroy or access systems and data of a ship or a shipping company. The attacker can be a person or process that attempts to access data, functions or other restricted areas of the system, without authorization, potentially with malicious intent.

Taking into consideration the present technical development within the shipping industry, training of new seafarers should offer appropriate knowledge about cyber threats and management of cyber security in the shipping industry context. At the moment, this is not the case. The present edition of the STCW convention by IMO, which forms the international minimum standard for training of seafarers, does not set clear requirement for seafarers' knowledge about cyber security.

It can be concluded, that not only cyber security but also cyber safety is needed to be addressed in maritime education and training. It is already a mandatory requirement under the ISM code although it is not specifically mentioned. Education and training should address all aspects of cyber safety issues for both IT and OT systems, since the ISM code aims at managing the ship in a safe manner, handling all risk to a sufficient level. The survey among the IAMU member universities indicates that education and training on cyber safety issues are incorporated to some extent at a number of universities and in a variety of Fields of Teaching covering both IT and OT systems. It also reveals that self-paced learning is not applied by the majority of the respondents in the survey. This could be because of the special application of IT and OT systems in the maritime domain and the lack of special developed training packages on cyber security and cyber safety issues for the maritime domain. This is not known, but could be explored in future research.

The biggest risks for cyber-attacks are related with the human element. Seafarers are seen the most critical barrier between success or failure when it comes to protecting the integrity of the data systems on board ships. Thus marine cyber safety should be taken into account in training, education and research and development initiatives of maritime universities.

Managing the human part of the cyber security calls for keeping up awareness of cyber threats and ability to avoid risky behavior in the whole organization. All employees of the shipping company, from top to bottom and from land organization to seafarers, should have up-to-date knowledge about cyber threats and the means of protection against them. This can be achieved only by proper training of the personnel. Not only once, but continuously, since cyber threats take constantly new forms, directions and targets.

As an essential topic within maritime cyber security, safe information exchange was studied within this project. The taxonomy of information exchange was presented and the safe information exchange

was discussed taking into consideration different aspects according to type, character, mode and role of the information exchange. The main conclusion from this discussion was that cyber risk management can be based on two pillars: people (human) and technology. The two pillars were characterised with respect to the safe information exchange process. It was found out that the existing training programmes for deck officer students are not sufficient in relation with the character and importance of the problem. The conclusion is the recommendation to update the academic programs accordingly. In the future, more specific recommendation on the contents of academic curricula should be formulated and discussed.

A training package on cyber security issues for maritime professionals was created during the CYMET project for the use of IAMU member universities. It was developed jointly by the three organizations of this project. Joint production of web-learning material can be beneficial for the parties involved. The positive experience of collaboration in production of training material should encourage maritime universities to share their expertise in this way for the benefit of the quality of education and training of seafarers globally.

IAMU is encouraged to consider a strategic decision about promoting production of high quality e-learning material in collaboration between its member universities. The recent work of IAMU in creating the Body of Knowledge (BoK) for Global Maritime Professional (GMP) could, for example, be continued in the form of production of high quality training material (texts, videos, webinars etc.) on selected topics in the GMP BoK. Maritime cyber security management suits well to joint production of training material and courses, since the problem of cyber threats is acute and global, and all maritime universities may not have necessary resources and expertise for developing good quality training courses on maritime cyber security. The experience from CYMET project shows that this form of collaboration is possible and beneficial.

However, there are a few technical issues to be solved. The most important task is to make the use of training material as easy as possible from teachers' point of view. Downloading course material from the IAMU e-learning portal and importing it to the Moodle of the university is a rather clumsy procedure. The use of the developed web-learning courses should be made easier. Eliminating the need to download and import courses by utilizing cloud services could be a solution for the future.

Another important point to be solved is to keep the course material up-to-date. Cyber threats are changing continuously. As they get new forms the contents of the training material should be updated accordingly. Therefore it is recommended that IAMU considers initiation of a development project, which concentrates in development of the Maritime Cyber Security self-education material further, looks for a solution to the above mentioned downloading/importing problem and takes care of updating and complementing the Cyber Security course contents. Another approach would be to establish a special Working Group for this purpose.

6. Acknowledgments

The authors would like to thank International Association of Maritime Universities (IAMU) and the Nippon Foundation in Japan for financing the CYMET project. Special thanks to following persons for their valuable contribution to this work: Jimmy Kåla (*Satakunta University of Applied Sciences),* Andreas Kyster (*Svendborg International Maritime Academy),* Ireneusz Meyer (*Gdynia Maritime University),* Pawel Szyman (*Gdynia Maritime University)* and Johan Bolmsten *(World Maritime University).*

References:

[1] DNV-GL (2016): Cyber Security Resilience Management for Ships and Mobile Offshore Units in Operation, available at: http://www.dnvgl.com, p. 8.

[2] Rider, D. (2018): Cyber Security at Sea: The Real Threats, The Maritime Executive, at: https://www.maritime-executive.com/blog/cyber-security-at-sea-the-real-threats#gs.0cFMf3g

[3] Chirgwin, R. (2018): IT 'heroes' saved Maersk from NotPetya with ten-day reinstallation bliz, available at: https://www.theregister.co.uk/2018/01/25/after_notpetya_maersk_replaced_everything/

[4] Bergman, J. (2017): Singapore LNG giant confirms cyber attack, LNG World Shipping, available at: https://www.lngworldshipping.com/news/view,singapore-lng-giant-confirms-cyber-attack_49563.htm

[5] Schuler, M. (2018): Clarkson Plc Reveals Details of 2017 Cyber Security Incident, available at: https://gcaptain.com/clarkson-plc-reveals-details-of-2017-cyber-security-incident/

[6] I.H.S. Fairplay Magazine staff (2018): Maritime cyber security survey 2017, available at: https://fairplay.ihs.com/safety-regulation/article/4292441/maritime-cyber-security-survey-2017

[7] BIMCO (2017): The Guidelines on Cyber Security Onboard Ships, version 2.0, available at: https://www.bimco.org

[8] IET (2017): IET Cyber Security Code of Practice for Ships, available at: https://www.gov.uk

[9] IMO (2017): IMO Guidelines on Maritime Cyber Risk Management, available at: http://www.imo.org

[10] CyberEdge Group (2018): 2018 Cyberthreat Defense Report, p. 17, available at: https://www.cptech.com/resources/2018-cyberthreat-defense-report/

[11] CyberKeel (2014): Maritime Cyber-Risks, 2014, p. 2, available at: https://maritimecyprus.files.wordpress.com/2015/06/maritime-cyber-risks.pdf

[12] IAMU (2018): Information about the International Association of Maritime Universities, at IAMU home page at: http://iamu-edu.org/?page_id=22

[13] IMO (2017): STCW inc. 2010 Manila Amendments, 2017 Edition, London UK

[14] Jennifer Rowley, What is information? Information Services and Use 18(4), 1998, 243 – 254

[15] Olivier Fitton, Daniel Prince, Basil Germond, Mark Lacy, The future of maritime cyber security. Lancaster University 2015. Available: http://eprints.lancs.ac.uk/72696/1/ Cyber_Operations_in_the_Maritime_Environment_v2.0.pd f [Accessed February 2019]

[16] Boris Svilicic, Junzo Kamahara, Matthew Rooks, Yoshiji Yano, Maritime Cyber Risk Management: An Experimental Ship Assessment. The Journal of Navigation, 1-13, 2019, doi:10.1017/S0373463318001157

[17] OMG Unified Modelling Language (OMG UML), Superstructure, V2.1.2, Available: http://www2.imm.dtu.dk/courses/02291/files/UML2.4.1_su perstructure.pdf [Accessed February 2019]

[18] Alireza Shameli-Sendi, Rouzbeh Aghababaei-Barzegar, and Mohamed Cheriet, Taxonomy of Information Security Risk Assessment (ISRA), Computers & Security 57, 2016, 14-30

[19] The guidelines on cyber security onboard ships, The guidelines of BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WORLD SHIPPING COUNCIL, Version 3,

[20] Cyber security threats in maritime industry, DNV, 2019

[21] Osiris A.Valdez Bandaa, Floris Goerlandta, A STAMPbased approach for designing maritime safety management systems, Safety Science 109, 2018, 109-129

[22] IMO: Maritime Cyber Risk Management in Safety Management Systems , Resolution MSC.428(98), Annex 10, page 1, Available:

http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/Resolution%20MSC.428(98).pdf [Accessed February 2019]
[23] Information technology — Security techniques — Information security management systems — Overview and vocabulary, International Standard, ISO/IEC 2700, First edition, 2009, Available: standards.iso.org [Accessed February 2019]
[24] Cyber security awareness in the maritime industry, A joint production by DNV GL and GARD, Available: http://www.gard.no/Content/25634225/Cyber%20Security_ Presentation%20(ID%201418279).pdf [Accessed February 2019]
[25] Practice of Cyber Security Management System on Cargo Ship, CCS China Classification Society, Available: http://www.ccs.org.cn/ccswzen/, [Accessed February 2019]
[26] Creating value from data in shipping. Practical guide, DNV-GL, Available: https://www.dnvgl.com/maritime/Creating-Value-from-Data-in-Shipping/index.html [Accessed February 2019]
[27] ISO/IEC 27000 family - Information security management systems, Available: https://www.iso.org/isoiec-27001information-security.html [Accessed February 2019]
[28] Sauli Ahvenjärvi, Ireneusz Czarnowski, Andreas Kyster, Ireneusz Meyer, John Mogensen, Paweł Szyman, Safe Information Exchange on Board of the Ship, TransNav, vol. ?, page ??, 2019 (submitted and accepted but not yet published)
[29] Cyber security awareness in the maritime industry, A joint production by DNV GL and GARD, Available: http://www.gard.no/Content/25634225/Cyber%20Security_Presentation%20(ID%201418279).pdf [Accessed February 2019]
[30] Cyber security threats in maritime industry, DNV, 2019
[31] Boris Svilicic, Junzo Kamahara, Matthew Rooks, Yoshiji Yano, Maritime Cyber Risk Management: An Experimental Ship Assessment. The Journal of Navigation, 1-13, 2019, doi: 10.1017/S0373463318001157
[32] ISO/IEC 27000 family - Information security management systems, Available:https://www.iso.org/isoiec-27001-information-security.html [Accessed February 2019]
[33] FAQ on ISPS and maritime security, Available:http://www.imo.org/blast/mainframe.asp?topic_id=897#threats [Accessed Marts 2019]
[34] ISM Code and Guidelines on Implementation of the ISM Code, Available:http://www.imo.org/en/OurWork/HumanElement/SafetyManagement/Pages/ISMCode.aspx [Accessed April 2019]
[35] Maritime Safety Committee (MSC), 98th session, 7-16 June 2017 Available:http://www.imo.org/en/MediaCentre/MeetingSummaries/MSC/Pages/MSC-98th-session.aspx [Accessed April 2019]
[36] Resolution MSC.428(98): Maritime Cyber Risk Management in Safety Management Systems Available: http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/Resolution%20MSC.428(98).pdf [Accessed April 2019]
[37] SurveyMonkey Available: https://da.surveymonkey.com/ [Accessed April 2019]
[38] IAMU Homepage Available: http://iamu-edu.org/?page_id=2985 [Accessed April 2019]
[39] Collins, B. & Moonen J. 2001: Flexible learning in a digital world – experiences and expectations. Routledge New York.

Appendix

APPENDIX A

Sample text from the Maritime Cyber Security Moodle course (Module 2):

Chapter 2 - Understanding the Cyber Threats

When hearing the word cyber attack, we often tend to think about a piece of software somehow infiltrating our computer, severely compromising its operation. While this can be the case, the big picture is a bit more complicated than that.

First of all, cyber attacks can be categorized as either untargeted, or targeted. Untargeted attacks are designed to cause damage to as many organizations as possible. Targeted attacks on the other hand, are aimed at a specific target organization. Untargeted attacks are usually quite basic in design, that use relatively simple tools in order to breach a company's IT systems. Some of the most common methods for this are:

- Social engineering. This method consists of the potential cyber attackers trying to convince individuals working for the targeted organization to break their security procedures, in order to make the breaching easier. A common way for attackers of doing this is through social media channels, although that's not always the case.
- Phishing. Sending out a big number of emails to potential targets, with content that aims to convince individuals to give away sensitive information. This is often done by claiming the email comes from the individuals own employer, and requesting the individual to click on a link in the mail that takes them to a staged website, where they are for example asked to give away their passwords and credentials. Other tricks that are often used to enhance the effectiveness of these emails is to claim that the matter is urgent, and that ignoring, or even postponing the requested action might lead to severe damage for the individual's employer. Whenever an email sender motivates their requests with authority, and/or urgency, and/or threats, the receiver should act with caution and criticism, verifying the request with the claimed sender or relative authorities, before proceeding.
- Water holing. Consists of either altering an existing website, or creating an entirely new one, designed to look like the original, in an attempt to take advantage of site visitors. For example, an employee trying to log in to an "employees' area" on what they believe to be the organization's website, might end up unknowingly giving away their username and password.
- Ransomware. A piece of software that infiltrates the targets' computers and encrypts data, until the creator/distributor of the software decrypts the data. Usually the decryption isn't done before a ransom fee has been paid to the creator/distributor, if even then.
- Scanning. A method that randomly targets attacks against vast portions of the internet.

Targeted attacks are often more complex and thought through than untargeted attacks. Since they are purpose built to attack a specific company, or even a specific ship in the scope and space of the shipping industry, they might be using custom made techniques and tools to fulfil their purpose. Examples of these are:

- Spear-phishing. A more sophisticated version of phishing, where the receivers get personalized emails. It's common for these emails to contain malicious software either directly, or behind links that automatically download it when clicked upon.
- Deploying botnets. Botnets are a group of internet-connected computers/devices commanded to simultaneously attack a website and thereby overload the site, compromising its functions. Even worse, the attack can target a DNS, or "Domain Name Server", taking down dozens of websites at once. This is

known as a DDoS, or “Distributed Denial of Service” attack, not to be confused with a DoS, or “Denial of Service” attack. A DoS attack is caused by a single attacker targeting a single website and making it temporarily useless, sometimes for up to several days, making it lose revenue and consumer trust. The rise of the IoT has provided DDoS attackers with a very large number of often very poorly protected devices that can be hijacked and used to deliver a DDoS. There are even so called “botnet for hire” services, from where attackers can rent a botnet to launch the attack from. It is also common to send the targeted website a “DDoS ransom note”, asking them to pay a ransom fee in exchange of not getting attacked. The DDoS threat is real: according to iotbusinessnews.com, the 2016 “Dyn DNS” attack made Twitter, Netflix and other online giants unusable. They also say big websites could lose up to 40 000 US dollars/hour during an unmitigated DDoS attack.

- Subverting the supply chain. This method consists of delivering the attack to the target organization by compromising either software or hardware, that are going to be delivered to the target organization.

Threat Actors

Cyber attacks can be launched by many different kinds of interest groups, each with their own specific goals. The motives and people behind the attacks and their interests are usually as follows:

- Cyber misuse. This form of attack is usually conducted by rather unsophisticated hackers, or even by dissatisfied employees of the organization itself. Sometimes classified data is accessed for research purposes only, and while it may be that no direct damage is done, it’s still illegal in most instances, if done without the data owner’s permission. Some hackers are pure opportunists, individuals that want to show off their hacking skills. They would for example hack a system, and then post the passwords and credentials of that system on public forums or social media, just for the sake of gaining recognition.
- Activist groups. The groups might be seeking publicity, in order to convince the public to support their case of for example resisting the shipping of specific cargoes in specific areas. Targets include ships, ship owners/operators, cargo receivers, or some other actor in the supply chain of the cargo. This is sometimes called “hacktivism”.
- Espionage. Unauthorized access of the target’s computer systems, in order to extract classified information. This may for example be done by hackers either for state purposes, or to seek financial gain either for themselves or a competitor to the target (if paid by the competitor to do it), the later sometimes referred to as “industrial espionage”.
- Organized crime. Examples include hackers working together with pirates in order to facilitate a physical attack on a ship. If the hackers can break into a shipping company’s or cargo handler’s logistics management system, they can possibly find out which ship is going to be loaded with what cargo, and passing through what area at a given point in time. This makes it easier for them to commit theft of valuable cargo, or kidnapping in order to receive ransom payments. Another example is to alter the cargo data, in order to facilitate smuggling of illegal cargo.
- Terrorism. Includes for example “remotely hijacking” a ship by compromising its navigation and propulsion/steering systems, forcing the ship to switch from a “business as usual operational mode” to something closer to a “survival mode”. This method plants fear in the public, and is most effective when done to a ship that’s either in close proximity to a passenger ship, seaside hotel etc., or even directly to a passenger ship.
- Warfare. A nation state in an armed conflict with another one, might try to perform some sort of espionage or direct disruption of ship OT, with the purpose of disrupting the operations of the enemy state’s ships on a general level, in order to halt their transports of weapons, fuel, and food.

Desired attack outcomes for the attacker that haven’t been described earlier are for example destruction of cargo, ships, and shipping facilities. Influencing where in the world the ship is willing to do business by for example altering relevant data. Distracting the ship’s crew by for example altering the readout of a sensor, as a smokescreen in order to facilitate a data extraction operation.

Attack Symptoms - Data Compromise

As there are different methods of delivering an attack, there are different ways in which the attacks can cause trouble. Here are three examples of common data compromise:

- Loss of confidentiality. This means that sensitive data has been obtained and understood by the attacker, in such a way that it is possible to exploit the target.
- Loss of integrity. In this situation the target cannot be sure that any data hasn't been, at least partially, altered by the attacker, which will probably lead to at least some level of complications of everyday business.
- Loss of availability. A case where the data is being made unavailable to the target, causing disruptions to doing business.

These three (Confidentiality, Integrity, Availability), form the basis for the so-called CIA model, which is a common method used as a part of cyber risk assessment. For example, if a no backup USB drive containing encrypted data but no data decryption software, is lost/stolen, there is no loss of confidentiality, due to the data being encrypted, but a loss of availability, since the data is unavailable to the user. When using the CIA method, the one of the three that yields the highest risk, should determine the overall risk for that specific procedure or technical entity.

Stages of a Cyber Attack

A cyber attack is done in multiple stages. It can usually be described as a 4-stage process:

1. Survey/Reconnaissance. The time spent on this stage can vary greatly, depending on the strength of the motivation of the attacker, the strength of the organization's defences, and the time available (in case the attacker's motivation for the attack is to stop a specific thing from happening, like for example making a ship unable to navigate and thereby stopping it from carrying a dangerous cargo into a specific geographical region before it reaches it). A popular way of gathering information preceding a cyber attack is the so-called OSINT method. OSINT stands for "Open Source Intelligence", and means gathering bits and pieces of information from social media, news, the organization's website, interviews with the senior management etc., that are not classified, and that are not sensitive one by one, but when combined they can allow a potential attacker to build a good road map for an attack.
2. Delivery. The attacker commences the attack.
3. Breach. The method chosen for the attack and the severity of the exploited vulnerability will decide the extent of the breach. It's important to keep in mind that not all attacks make systems crash. Some attacks are not even designed to make systems crash, but rather to infiltrate the system, and extract data in a stealthy way, making them harder to spot. This way, the attackers can extract data over a long period of time, which might be effective in case of for example national espionage. Examples include interrupting or disrupting the operation of the ECDIS or "Electronic Chart Display", gaining access to data that is sensitive from a point of view of commerce and safety, like crew/passenger lists or cargo manifests, or even gain full control of a machinery management system. An ECDIS is a computer-based navigation system, that combines information from GPS, radar and AIS among others, and projects this combined information onto a screen with an electronic navigational chart. GPS stands for Global Positioning System, and AIS for Automatic Identification System. The GPS shows the ship's position on the sea, and the AIS makes it possible to track other ships' movements, in case they are giving out AIS data. The radar also provides information on the position of other objects in relation to the ship, but in a more direct, accurate, and reliable way than the AIS, because the radar's function is based on direct bouncing of radio waves, rather than transmitting and receiving data packages.

4. Affect. What affect a breach will have for the organization is determined by the motivations and goals set out by the attacker. Once inside the system, the hacker might be able to not only monitor, destroy, or extract data, but also expand the attack onwards, or perform necessary actions in order to be able to return to the system at a later stage. An example of destruction of data would be to destroy important pre-arrival data from the ship's cargo handling database, in order to postpone and severely complicate a ship's upcoming port operations, causing financial loss to the organization.

International Association of Maritime Universities

Meiwa Building 8F, 1-15-10 Toranomon, Minato-ku, Tokyo 105-0001, Japan

Tel : 81-3-6257-1812 E-mail : info@iamu-edu.org URL : http://www.iamu-edu.org

ISBN No. 978-4-907408-27-5