TRANSNAV
http://www.transnav.eu
the International Journal
on Marine Navigation
and Safety of Sea Transportation
Volume 13
Number 1
March 2019

DOI: 10.12716/1001.13.01.17

Safe Information Exchange on Board of the Ship

S. Ahvenjärvi
Satakunta University of Applied Sciences, Rauma, Finland

I. Czarnowski
Gdynia Maritime University, Gdynia, Poland

J. Kåla
Satakunta University of Applied Sciences, Rauma, Finland

A. Kyster
Svendborg International Maritime Academy, Svendborg, Denmark

I. Meyer
Gdynia Maritime University, Gdynia, Poland

J. Mogensen
Svendborg International Maritime Academy, Svendborg, Denmark

P. Szyman
Gdynia Maritime University, Gdynia, Poland

ABSTRACT: Information exchange is an important component of life and human behavior 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 paper 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.

1 INTRODUCTION

Information is an integral part of the world and valuable for personal, social and organisational functioning [1]. 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 non-technical, 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. 1). Such discussion on the cyber operations in the maritime environment has been carried out in [2].

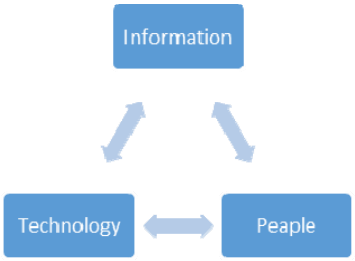


Figure 1. The three elements of cyber operations [2]

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 cyber-attacks, which are understood as modification, disconnection, destruction, theft or unauthorized access to or unauthorized use of an asset. Cyber-attacks might concern computer information systems, computer infrastructures, including IT networks, or personal computer devices [11], i.e. it can be any type of offensive activity aimed at information technology (IT) and operational technology (OT) systems, computer networks, and/or personal computer devices attempting to threaten, destroy or access ship systems and data [7]. 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 [11].

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.

The paper is organized in the following way: In Chapter 2 a taxonomy of information exchange is presented. In Chapter 3 the safe information exchange is discussed. Recommendations for maritime training with respect to the safe information exchange and in general to cyber security are presented in chapter 4. The last chapter concludes the paper with final remarks.

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.

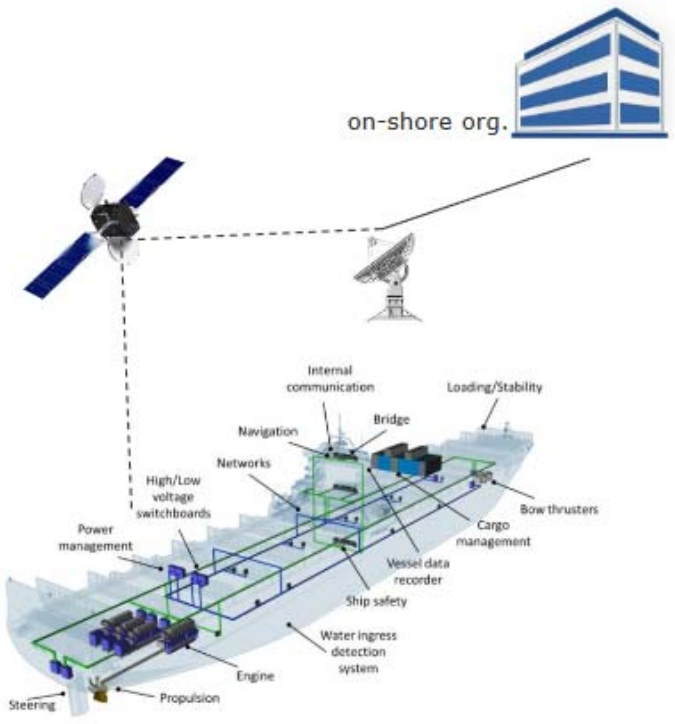
Information can be also considered with respect to its formal and unformal character. While unformal character of information is restricted to accepted rules of information exchange which are known for actors, the formal character of information is embedded in precisely defined and accepted rules and 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.

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 operational 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 [7]. 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.



Information Technology (IT)

- IT networks
- E-mail
- Administration, accounts, crew lists, ...
- Planned Maintenance
- Spares management and requisitioning
- Electronic manuals & certificates
- Permits to work
- Charter party, notice of readiness, bill of lading...

Operation Technology (OT)

- PLCs
- SCADA
- On-board measurement and control
- ECDIS, GPS
- Remote support for engines
- Data loggers
- Engine & Cargo control
- Dynamic positioning, ...

Figure 2. Information technology (IT) and operational technology (OT) on board of the ship [5]

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 1.

Table 1. Taxonomies for information exchange

	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

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 [9].

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 [14].

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. According to the IMO Resolution MSC.428(98) on Maritime Cyber Risk Management [10], 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 in different ship space an information technology (IT) and operational technology (OT).

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 operational technology (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 [10]. 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 [12], 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 [14]. 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 [12]. Thus, cyber-security is important with respect to the attacks on operational technology (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 operational technology (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 3. Best practice by DNV [12]

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.

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.

ACKNOWLEDGMENTS

This work has been carried out as part of the international project CYMET "Addressing Cyber Security in Maritime Education and Training" of the research project system for FY2018 by International Association of Maritime Universities (IAMU), funded by Nippon Foundation.

BIBLIOGRAPHY

[1] Jennifer Rowley, What is information? Information Services and Use 18(4), 1998, 243 – 254
[2] 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.pdf [Accessed February 2019]
[3] 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
[4] OMG Unified Modelling Language (OMG UML), Superstructure, V2.1.2, Available: http://www2.imm.dtu.dk/courses/02291/files/UML2.4.1_superstructure.pdf [Accessed February 2019]
[5] Alireza Shameli-Sendi, Rouzbeh Aghababaei-Barzegar, and Mohamed Cheriet, Taxonomy of Information Security Risk Assessment (ISRA), Computers & Security 57, 2016, 14-30
[6] The guidelines on cyber security onboard ships, The guidelines of BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WORLD SHIPPING COUNCIL, Version 3,
[7] Cyber security threats in maritime industry, DNV, 2019
[8] Osiris A.Valdez Bandaa, Floris Goerlandta, A STAMP-based approach for designing maritime safety management systems, Safety Science 109, 2018, 109-129
[9] 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]

[10] 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]
[11] 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]
[12] Practice of Cyber Security Management System on Cargo Ship, CCS China Classification Society, Available: http://www.ccs.org.cn/ccswzen/, [Accessed February 2019]
[13] 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]
[14] ISO/IEC 27000 family - Information security management systems, Available: https://www.iso.org/isoiec-27001-information-security.html [Accessed February 2019]