Digital Skill 2

Maritime Cybersecurity
Course description

Content

Toolbox Guide

Appendix 1 – Table of Constructive Alignment

Appendix 2 – Example lessons

- Lesson 1 – Cybersecurity Awareness
- Lesson 2 – Maritime Cybersecurity Awareness
- Lesson 3 – International legal framework and guidance on cyber and maritime cybersecurity

Appendix 3 – Module Content

Appendix 4 – Example Assessment Cases

Appendix 5 – Bibliography

Co-funded by the
Erasmus+ Programme
of the European Union

THE TOOLBOX GUIDE

Curriculum

Learning Objectives	The intended learning objective of the "*Maritime Cybersecurity Course*" is to provide maritime professionals with the knowledge and skills required to minimise ships' vulnerability, prevent main cyber risks, and respond effectively to cyber incidents and attacks. The following subject areas will be covered: 1. Cybersecurity Awareness – essential elements, actual context and scenarios, main threats, actors, techniques and tactics; 2. Maritime cybersecurity awareness – risks and threats for shipping industry and vessels instigated by onboard IT and OT systems vulnerabilities; digital transformation for the shipping industry and on board ships; 3. EU framework on Cybersecurity, IMO references and industry guidelines related to maritime cyber risk management; 4. Maritime cyber risk management process - key elements and best practices for maritime professionals; 5. Cyber-attacks in the shipping industry - analysis and case studies. The goal of this course is to provide knowledge and therefore awareness, in terms of cyber risk management in the maritime domain and understanding of operating vessels in an increasingly technological and digitalized maritime environment.
Target group	The course is intended for maritime professionals who hold responsibility positions onboard and also for ashore personnel to make them aware of the safety and security management related to cyber threats on board, in particular: **Onboard**: Master, Chief Mate, Chief Engineer, 2nd Engineer, Ship Security Officer (SSO), Ship Safety Officer, and any other position identified by the company. **Ashore**: Company Security Officer (CSO); Data protection officer (DPO); Designated Person Ashore (DPA); IT manager and any other position as identified by the company.
Entry requirement	EQF LEVEL 4/5/6 The minimum competence requirements is National Equivalent of EQF level 4,5,6 or relevant industry experience. The range of levels reflects the progression from Digital Skills 1 package and the further development of those skills in this package, whilst remaining accessible to those at EQF Level 4. Onboard experience as a deck or engine officer (STCW table A-II/1 or Table A- III/1) or at least one-year working experience as ashore-based employee.

Co-funded by the Erasmus+ Programme of the European Union

Duration	The suggested number of contact hours is of indicatively up to 24 hours, which includes indicatively 2/3 hours for assessment. It is recommended to complete the course in a period of up to 4 weeks. Also, up to 21 hours are suggested for independent learning and research.
Assessment	Assessment of the acquired learning outcomes will be carried out using: - diagnostic self-assessments; - formative assessment (e.g. socrative questioning, self-assessment, oral presentation). - Summative assessment using: ▪ multiple choice questions test and/or ▪ practical exercises (case studies, simulation, gaming).

Co-funded by the
Erasmus+ Programme
of the European Union

Course Description - *Maritime Cybersecurity Course*	
Course Outline	**1. Cybersecurity awareness (*indicatively* 4hrs)** 1.1 Basic definition - essential concept – actual contest/scenario on cyber global risk and threats 1.2 Cyber risks and threats 1.3 Cyber threats – actors and motivation 1.4 Cyber threats – common cyber tools and infiltration techniques 1.5 Cyber Kill Chain 1.6 Introduction to CIA Triad Model – key elements **2. Maritime cybersecurity awareness (*indicatively* 4hrs)** 2.1 Main topics on Cyber Risk in the maritime domain for shipping industry and onboard 2.2 Information Technology (IT) and Operational Technology (OT) onboard and typical vulnerabilities, Shipboard Networks 2.3 Digital transformation and new technologies in the shipping industry and on board ships **3. International legal framework and guidance on cyber and maritime cybersecurity (*indicatively* 2hrs)** 3.1 EU References on cybersecurity and cybersecurity guidelines on maritime sector; 3.2 IMO guidance 3.3 Maritime industry guidelines and other guidance and standards 3.4 Legal impact of cybersecurity on commercial operations of the vessel **4. Maritime cyber risk management process and best practices for maritime professionals (*indicatively* 4/5hrs)** 4.1 Analysis of Maritime Cyber Risk Management process 4.2 Cybersecurity best practices for maritime professionals **5. Main cyber-attacks and incidents in the shipping industry (*indicatively* 2 hrs)** 5.1 Overview of main cyber-attacks and incidents in the shipping industry 5.2 Description and analysis of most relevant attacks that affected the shipping industry **6. Maritime cybersecurity: training and practical activities (*indicatively* 4hrs)** 6.1 Maritime OT training scenarios 6.2 Maritime IT training scenarios *Indicatively 2 or 3 hours in total are dedicated to Assessment activities (diagnostic, formative, summative).*

Co-funded by the Erasmus+ Programme of the European Union

Learning Outcome	By the end of the course, participants will be able to: *1. Knowledge and understanding:* 1.1. Understand essential cybersecurity terms and concepts; 1.2. Identify main cyber risks and threats, threat actors and their objectives; 1.3. Recognise and assess potential cyber risks and threats on board (IT and OT systems); 1.4. Indicate and summarise the EU legal framework and guidelines, and IMO guidance on maritime cybersecurity; 1.5. Summarise the Cyber Risk Management process according to the relevant maritime-related guidelines. *2. Skills and competences:* 2.1. Interpret the integrity of data and recognise alerts; 2.2. Use digital devices onboard to ensure required security levels for digital networks, servers and applications; 2.3. Detect and prevent cyber-attacks and decide on actions to be taken (preventive and reactive measures); 2.4. Carry out cybersecurity risk management and assessment. *3. Responsibility and autonomy:* 3.1. Apply the cyber risk management framework to prevent attacks in accordance with Safety Management Systems (SMS) requirements; 3.2. Recognise incidents or cyber-attacks on board IT and OT systems and devices connected to the digital networks services; 3.3. Facilitate information sharing among key actors. 3.4. Be empowered and able to act appropriately when a cyber threat presents itself 3.5. Recognise the impact of personal behaviours that could make a cyber security breach more likely

Teaching methods	The primary teaching method is blended learning, *i.e.* a combination of online educational methods and classroom-based methods.
Teaching material	− Audio-visual material: PowerPoint presentations, videos (if any); − Printed materials: texts, papers, essays, articles and other supporting documentation; − Case studies/scenarios; − Simulation; − Recommended reading, recommended videos, supporting learning material.

Co-funded by the Erasmus+ Programme of the European Union

Assessment/exam	The participants' progress through the course should be formatively assessed using a variety of assessment methods, for instance self-checking or automated multiple-choices tests or reflective activities after each module. Summative assessment should identify participants' specialisation and their ability to respond to cybersecurity challenges in the maritime cyber domain. The process should use practical exercises (case studies; simulation), multiple-choice tests and similar assessment methods.
Evaluation	
Course Review	– Participants will be provided with an opportunity to complete a short survey to evaluate the EP delivery and content of the package. – Upon completing this evaluation, individual lecturers will also carry out module reflection according to the template that will be provided. These processes will be in accordance with the institution/company's internal processes

Digital Skills 2 – Scheme of Work

Maritime Cybersecurity Course

Appendix 1 – Table of Constructive Alignment

Lecturer/s: ..... **Session/s:** **Indicatively 24 hours**

Programme: **Digital Skills 2**	**Modules**: 1. Cybersecurity awareness; 2. Maritime Cybersecurity awareness; 3. International legal framework and guidance on Cyber and Maritime Cybersecurity; 4. Maritime Cyber Risk Management process and best practices for maritime professionals; 5. Main cyber-attacks in the shipping industry; 6. Maritime cybersecurity: training and practical activities.	No. of Weeks: *indicatively 4 weeks.*
Diagnostic self-assessment		

Co-funded by the Erasmus+ Programme of the European Union

1. **Cybersecurity awareness** *(approximately 4 hours)*				
Lesson number	**Lesson**	**Learning Outcome (numbered as per toolbox guide)**	**Teaching method(s)**	**Assessment[1] - questions for end of module quiz and final assessment**
1	1.1 Basic elements and actual contest/scenario on Cyber global risk and threats	− primarily 1.1 − partly 1.2	− Presentation using PowerPoint and videos	− Self-Assessment quiz − Case studies analysis − Socrative Questioning
1	1.2 Cyber risk and threats	− primarily 1.2		
2	1.3 Cyber threats – key actors	− primarily 1.2		
2	1.4 Cyber threats – techniques and tactics	− primarily 1.1 − partly 2.1 and 2.3		
3	1.5 Cyber kill chain	− 1.2 and 1.3		
4	1.6 Introduction to CIA Triad Model – key elements	− 1.3 and 2.4 and 3.3		

[1] Indicative Assesment methods that could be adopted. This note is referred to all 6 Modules.

Co-funded by the Erasmus+ Programme of the European Union

2. **Maritime Cybersecurity awareness** *(approximately 4 hrs)*				
Lesson number	**Lesson**	**Learning Outcome (numbered as per toolbox guide)**	**Teaching method(s)**	**Assessment - questions for end of module quiz and final assessment**
5	2.1 Main topics on Cyber Risk in the maritime domain for shipping industry and onboard	– primarily 2.1	– Presentation using PowerPoint, Videos/images/Photos etc. about cyber risk in the maritime domain made by maritime stakeholders	– Self-Assessment quiz – Case studies analysis – Multiple choices test – Socrative Questioning – Gaming
6	2.2 Information Technology (IT) and Operational Technology (OT) systems onboard and typical vulnerabilities, Shipboard networks	– primarily 2.2 – partly 2.3 – primarily 1.3 – partly 2.2		
7	2.3 Digital transformation and new technologies in the shipping industry and onboard ships	– primarily, 1.5 – partly 2.1 and 2.2		
Formative assessment – Module 1 and 2				

Co-funded by the Erasmus+ Programme of the European Union

3. International legal framework and guidance on Cyber and Maritime Cybersecurity *(approximately 2hrs)*				
Lesson number	**Lesson**	**Learning Outcome (numbered as per toolbox guide)**	**Teaching method(s)**	**Assessment - questions for end of module quiz and final assessment**
8	3.1 EU references on cybersecurity and cybersecurity guidelines on maritime sector	− primarily 1.4 − partly 3.1	− Presentation using PowerPoint − Independent research and review of documents related to specific interest and specialisation of learners	− Assessed through self-checking questions and case studies and integrated into summative assessment − Oral presentation
8	3.2 IMO guidance	− primarily 1.4 − partly 3.1		
9	3.3 Maritime Industry guidelines and other guidance and standards 3.4 Legal impact of cybersecurity on commercial operations of the vessel	− primarily 1.5 and 1.4 − Partly 3.1 and 3.2		
Formative Assessment – Module 3				

Co-funded by the Erasmus+ Programme of the European Union

4. Maritime Cyber Risk Management process and Best Practices for maritime professionals *(approximately 4 or 5 hrs)*				
Lesson number	**Lesson**	**Learning Outcome (numbered as per toolbox guide)**	**Teaching method(s)**	**Assessment - questions for end of module quiz and final assessment**
10	4.1 Analysis of Maritime Cyber Risk Management process	− primarily 1.5 − partly 3.1	− Presentation using PowerPoint Supporting material for management and assessment (like ISO Standard)	− Self Assessment test − Case studies analysis − Multiple choices test − Socrative Questioning
11	4.2 Cybersecurity Best Practices for maritime professionals	− primarily 2.4 − partly 2.3	− Presentation using PowerPoint − Supporting document on Cyber Best Practices	
Formative Assessment – Module 4				

Co-funded by the Erasmus+ Programme of the European Union

5. Main cyber-attacks and incidents in the shipping industry *(approximately 2 or 3 hrs)*				
Lesson number	**Lesson**	**Learning Outcome (numbered as per toolbox guide)**	**Teaching method(s)**	**Assessment - questions for end of module quiz and final assessment**
12	5.1 Overview on main cyber-attacks and incidents in the shipping industry	− primarily 3.1 − partly 3.2 and 3.3	− Presentation using PowerPoint − Lectures/media articles − Press releases − Articles about the different attacks	− Tests − Simulation
13	5.2 Description and analysis of most relevant attacks that affected the shipping industry		− Discussion Group − Lectures − Socrative Questioning	
Formative Assessment – Module 5				

6. Maritime cybersecurity: training and practical activities *(approximately 4 hrs)*				
Lesson number	**Lesson**	**Learning Outcome (numbered as per toolbox guide)**	**Teaching method(s)**	**Assessment - questions for end of module quiz and final assessment**
14	6.1 OT training scenarios	− primarily 3.2 and 3.3	− Group discussion based on exercises, scenarios, presentation using PowerPoint	− Practical Exercises (e.g. Case Studies) − Simulation
	6.2 IT training scenarios			
Final assessment (approximately 1 hour and 30 minutes)				

Co-funded by the Erasmus+ Programme of the European Union

Appendix 2/1 Example Lesson

Lesson plan – Module 1: Cybersecurity Awareness

1.0 Introduction

Rapidly developing information and communication technologies have raised mass communication and its mediums to a prominent place in modern society, industry, e-governance and also maritime industry, including shipping and logistic transportation.
Cybersecurity is generally used as substitute with the terms Information Security and Computer Security. Cybersecurity that goes beyond the limits of the traditional information security to involve not only the security of information tools but also the other assets, involving the person's own confidential information.
Cybersecurity in maritime has a huge potential to affect the safety of the crew, vessel, cargo and even ports. Cybersecurity in shipping is concerned with the data protection of IT systems, on board ships hardware and sensors and data leak from unauthorized access, manipulation and disruption.
The core purpose of this lesson is to introduce participants in the world of to the most useful terms in Information Security and Computer Security discipline.
This lesson will provide the fundamentals knowledge regarding basic elements for different virus expressions, methods of malware infection and key actors with various techniques and tactics used in cyber-attack.

2.0 Learning Outcomes

The participants at end of this module will achieve the following LOs:

1.1. Understand essential cybersecurity terms and concepts;
1.2. Identify main cyber risks and threats, threat actors and their objectives;
1.3. Recognise and assess potential cyber risks and threats on board (IT and OT systems)
2.1. Interpret the data integrity and recognise alerts;
2.3. Detect and prevent cyber-attacks and decide on actions to be taken (preventive and reactive measures);
2.4. Be familiar with cybersecurity risk management and assessment;
3.3. Facilitate information sharing among key actors.

3.0 Teaching Methods

Oral presentation aiming to convey a structured set of information about the subject, followed by the most essential information on the subject with audio-visual using slides, video, digital presentations.
Also the teacher gives to the participants a demonstrations regarding how a cyber-attack can made on board ship.

Co-funded by the
Erasmus+ Programme
of the European Union

Module Content

Lessons' plan

The teacher presents a brief overview of topics, followed by a detail presentation using PowerPoint slide show, and useful video presentations.
The teacher will organize small group discussions of the importance of different topics of the lectures course content.
Participants could be prompted:

- to understand cyber threats – key actors;
- to recognize different cyber risk and threats;
- to recognize the distinction between Information Technology (IT) and Operational Technology systems (OT);
- to know virus definitions that can put in danger IT or OT;
- to know some various ways regarding techniques and tactics that can put in danger the IT and OT.

Course contents

1. Cybersecurity Awareness

1.1 Basic definition – essential concept – actual contest/scenario on cyber global risk and threats

1.1.1 Introduction
1.1.2 Definitions

1.2 Cyber risk and threats

1.2.1 Different Virus Expressions and Methods of Malware and Virus Infection and Spread;
Explain the most common like: Computer Viruses, Worms, Adware, Spyware, Ransomware, Bots, Rootkits, Trojan Horses, Bugs.
1.2.2 Types of cyber attack;
Explain the most common like: Malware, Crash-Override, Triton, Zombie zero attack, Water holing, Scanning.

Self-Assessment quiz 1.1. and 1.2

1.3 Cyber threats – key actors and motivation

Explain the most common like: A Cyber Threat Actor (CTA), Cybercriminals Motivation, Affiliation, Common Tactics, Techniques, and Procedures, Insider Threats, Cyber Spies: State-Sponsored Attackers / Nation-State actors, Cyber-spies, Hacktivists and Terrorist Organizations.
Give illustration about statistics of different top regarding cyber threat reports and include findings, major incidents and more.

Self-Assessment quiz.

1.4 Cyber threats – common cyber tools and infiltration techniques

Targeted attacks may be more sophisticated and use tools and techniques specifically created for targeting a company or ship. Examples of tools and techniques, which

may be used in these circumstances, include: Social engineering, Brute force, Denial of service (DoS), Distributed Denial of Service (DDoS) attacks, Man in the Middle (MitM) attack, Spear phishing attacks, SQL injection attack, Drive-by attack, Cross-site scripting (XSS) attack, Spyware/adware attack, Trojans attack.
Explain the stages of a cyber-attack: Survey/reconnaissance , Breach, Pivot.

Self-Assessment quiz.

1.5 Cyber Kill Chain

Illustrate the structure of a successful cyber-attack: definition of the steps used by cyber attackers in today's cyber-based attacks; understand how to identify and stop attackers at each of the respective steps.

1.6 Introduction to CIA Triad Model – key elements (Confidentiality, Integrity and Availability)

The lesson illustrates the function of the CIA triad security model that companies should follow in order to protect information stored in on-premises computer systems or in the cloud. In particular:

a. keep information secret (Confidentiality);
b. maintain the expected, accurate state of that information (Integrity);
c. ensure that the information and services are up and running (Availability).

Self-Assessment quiz 1.5 and 1.6.

4.0 Teaching Materials

The methods of this lesson are lectures, group work, PowerPoint, documents, video and other e-learning supporting materials.

PowerPoints

The PowerPoint will be explained by voice (if feasible) and text in an e-learning module. Lectures presentation and movies examples

Websites[2]:

- https://www.kaspersky.com/resource-center/threats/computer-viruses-and-malware-facts-and-faqs
- https://www.infosys.com/services/cyber-security/documents/transport-logistics-industry.pdf
- https://en.wikipedia.org/wiki/Duqu
- ENISA, Cyber Risk Management for Ports, ISBN 978-92-9204-403-9 - DOI 10.2824/671060, December 2020 (https://www.enisa.europa.eu/publications/guidelines-cyber-risk-management-for-ports)
- EU ENISA: Cyber Security Aspects in the Maritime Sector (December 19, 2011) https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-

[2] A repository of websites could be made available to offer a wider range of web references.

- EU ENISA: Port Cybersecurity – Good practices for cybersecurity in the maritime sector (November 26, 2019) - https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector
- EU ENISA: Cyber Risk Management for Ports (December 17, 2020), ISBN 978-92-9204-403-9 - DOI 10.2824/671060, December 2020 - https://www.enisa.europa.eu/publications/guidelines-cyber-risk-management-for-ports
- ABS, MANAGING CYBER RISKS AND THE ROLE OF THE P&I CLUB: AN OVERVIEW, October 2020
- https://www.american-club.com/files/files/managing_cyber_risks.pdf
- Tam, K , Cyber-Risk Assessment for Autonomous Ships, http://hdl.handle.net/10026.1/11245 R. Ramirez, N. Choucri: Improving Interdisciplinary Communication With Standardized Cyber Security Terminology, IEEE Access , vol.4, 2016 https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7437356
- https://www.globalknowledge.com/us-en/topics/cybersecurity/glossary-of-terms/#gref
- https://www.cybintsolutions.com/20-cyber-security-terms-that-you-should-know/
- https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html
- https://www.kaspersky.com/resource-center/threats/computer-viruses-and-malware-facts-and-faqs
- https://zvelo.com/network-security-malicious-threats-and-common-computer-definitions/

Other helpful reads and links related to Computer Viruses and Malware:

- Free Cloud Anti-Virus Software
- Free Ransomware Protection & Decryption Tools
- How to choose the anti-virus software that's best for you
- Malware classifications
- The Rise of Mobile Malware
- What's the Difference Computer Virus and a Worm?
- Top 7 Mobile Security Threats
- Top 7 Cyber Security Threats to Watch Out For
- Types of Spyware
- A Brief History of Computer Viruses & What the Future Holds
- Top 10 Most Notorious Hackers
- https://www.cisecurity.org/spotlight/cybersecurity-spotlight-cyber-threat-actors/
- https://www.turn-keytechnologies.com/blog/article/identifying-the-four-main-threat-actor-types/
- https://www.mdpi.com/2076-3417/10/12/4334/htm
- https://carnegieendowment.org/2019/09/30/cyber-risk-scenarios-financial-system-and-systemic-risk-assessment-pub-79911
- https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020

Video links

- https://www.youtube.com/watch?v=7yHsiTmUnPk

Co-funded by the Erasmus+ Programme of the European Union

- https://www.youtube.com/watch?v=X08wgodFgXw
- https://www.youtube.com/watch?v=g0yXmQx89x4
- https://www.youtube.com/watch?v=wcaiKgQU6VE
- https://www.youtube.com/watch?v=_jKylhJtPmI
- https://www.youtube.com/watch?v=ciNHn38EyRc
- https://www.youtube.com/watch?v=gD4-5toqiuk
- https://www.youtube.com/watch?v=70ukzSEx8p0
- https://www.youtube.com/watch?v=DfEiMj7wAi4
- https://www.youtube.com/watch?v=n8mbzU0X2nQ&feature=emb_logo
- https://www.youtube.com/watch?v=Dk-ZqQ-bfy4
- https://www.youtube.com/watch?v=2naiQd-U_kM
- https://www.youtube.com/watch?v=MNn2M3BD8eA
- https://www.youtube.com/watch?v=P0F3OxcDFQg
- https://www.youtube.com/watch?v=tmU3Qwkzerw
- https://www.youtube.com/watch?v=Ra0dGPYScLQ
- https://www.youtube.com/watch?v=qBVThFwdYTc

5.0 Socrative Questioning

Tips for using Socratic Questioning:

- plan significant questions that provide meaning and direction to the dialogue;
- use wait time: Allow at least thirty seconds for participants to respond;
- follow up on participants' responses;
- ask probing questions;
- periodically summarize in writing key points that have been discussed;
- draw as many participants as possible into the discussion;
- let participants discover knowledge on their own through the probing questions the teacher poses.

Socratic Question Type	Example
Clarification questions	What do you mean by cyber virus? Can give some examples of common cyber virus? Could hacker affect OT systems on board ship? What do you think is the main reason for hacker to make a cyber-attack? Could you give us an example of cyber treats actor?
Questions about an initial question or issue	Why is this question important? Is this question easy or difficult to answer? Why do you think that?
Assumption questions	Why would someone make this assumption? What is _____ assuming here? What could we assume instead? You seem to be assuming _____.
Reason and evidence questions	What would be an example? Why do you think this is true? What other information do we need?

Co-funded by the
Erasmus+ Programme
of the European Union

	Could you explain your reason to us?
Origin or source questions	Is this your idea or did you hear if from someplace else? Have you always felt this way? Has your opinion been influenced by something or someone?
Implication and consequence questions	What effect would that have? Could that really happen or probably happen? What is an alternative? What are you implying by that? If that happened, what else would happen as a result? Why?

6.0 Self-Assessment quiz for topic

- Identify the most common cyber virus.
- Describe the cyber risk and threats on maritime environment.
- Give examples of types of cyber-attack using malware.
- Gives some examples of cyber tools and techniques specifically created for targeting a company or ship by a cyber-attack.

Appendix 2/2 Example Lesson

Lesson plan – Module 2: Maritime Cybersecurity Awareness

1.0 Introduction

The maritime industry is changing. Automated processes are running navigation and propulsion systems, cargo handling, and container tracking systems. While there are many business advantages to introducing digital processes into your operational networks, you are also vulnerable to new cyber risks that come in their wake.
Technology on ships plays a significant role to help manoeuvring through those conditions and it enables communication in situations of emergency and distress. Unfortunately, any type of technology has the potential to be used for malicious purposes. Cybersecurity awareness and culture is new on the agenda of the maritime community, but it must be taken seriously to avoid catastrophic consequences.
Today, maritime companies are increasingly adopting new technologies as legacy systems reach end of life (EOL) and their support costs become prohibitively expensive. With vessel sizes increasing and crew sizes decreasing, maritime company owners and operators are using new technologies to connect OT systems locally and remotely via satellite communications (SATCOM) and the internet to enable remote monitoring and navigational support. Industrial Internet of Things (IIoT) solutions that transfer data from sensors on equipment over satellite or the internet for analysis are growing in popularity as well.
The ability to remotely monitor OT systems improves productivity and reduces labor costs by allowing companies to consolidate the management of OT assets shoreside.
An active IIoT system onboard a vessel coupled with a fuel optimization application can collect data, send it ashore, and use it to plot the most fuel-efficient route.
Despite growing cybersecurity risks, many maritime organizations lack even rudimentary safeguards. OT equipment remains vulnerable to staff and vendor personnel who plug Transient Cyber Assets into onboard systems.
Cybersecurity has a huge potential to affect the safety of the crew, vessel, cargo and even ports. Cybersecurity is concerned with the protection of IT systems, on board hardware and sensors and data leak from unauthorised access, manipulation and disruption. Cybersecurity policies and plans cover different types of risks like information integrity, system and hardware availability on board and in the office of the shipping company.
Digitalization and communication technologies will create new services to support transport chains, and supply chains will become more integrated for all modes of transport. In the maritime transport sector, vast amounts of data are available that will support new opportunities to improve ship operations, safety and logistics.
Digitization will drive automation, lead to the development of smart ships and positively impact safety and environmental performance. New cloud technologies will significantly affect how ships and their components are designed, manufactured and operated. The Internet of Things promises to be one of the most disruptive technological revolutions since its inception.

2.0 Learning Outcomes

The participants at end of this module will achieve the following LOs:

1.3. Recognise and assess potential cyber risks and threats on board (IT and OT systems);

Co-funded by the
Erasmus+ Programme
of the European Union

1.5. Summarise the Cyber Risk Management process according to the relevant maritime-related guidelines.
2.1. Interpret the data integrity and recognise alerts;
2.2. Use digital devices onboard to ensure required security levels for digital networks, servers and applications;
2.3. Detect and prevent cyber-attacks and decide on actions to be taken (preventive and reactive measures);

3.0 Teaching Methods

Oral presentation aiming to convey a structured set of information about the subject, followed by the most essential information on the subject with audio-visual using slides, video, digital presentations.
Also the teacher gives to the participants a demonstrations regarding how a cyber-attack can made on board ship.

Module Content

Lesson plan

The teacher presents a brief overview of topics, followed by a detail presentation using PowerPoint slide show, and useful video presentations.
The teacher will organize small group discussions of the importance of different topics of the lectures course content.

Participants could be prompted:

- to know and recognize the IT and OT ship equipment;
- to understand critical vulnerabilities in common OT systems and Industrial Control Systems (ICS) on board ship;
- to recognize different cyber risk related to the heavy reliance on navigation and communication systems such as the Electronic Chart Display Information System (ECDIS), the Automated Identification System (AIS), and Very Small Aperture Terminals (VSATs);
- to understand the aim of CPS in engine room and the role of IoT and their cyber risk;
- to know some various future technologies applied in maritime industry.

Course contents

2. Maritime Cybersecurity awareness

2.1 Main topics on Cyber Risks in the maritime domain for shipping industry and onboard

2.1.1 Cyber Risk and threats onboard ship in the cyber space
Participants will be familiar with the principal OT systems interconnected on a ship includes systems like: Vessel Integrated Navigation System (VINS), Global Positioning System (GPS), Satellite Communications, Automatic Identification System (AIS) and Radar systems and electronic charts, Main engine with propulsion system, Cargo management systems.

Co-funded by the Erasmus+ Programme of the European Union

Self-Assessment quiz

2.2 Information Technology (IT) and Operational Technology (OT) systems on-board – vulnerabilities and threats – shipboard networks

The participants will be aware of the differences between IT and OT systems on board ships and also to understand responsibilities of IT and OT to maintain and manage the corporate and ICS/SCADA networks. The participants will recognize part of connection between OT systems on ship and also to identify their risks under cyber-attack threats. The participants will find the vulnerabilities of connections between OT systems like navigation with propulsion and cargo.

Self-Assessment quiz

2.3 Digital transformation and new technologies in shipping industry and on board ships

2.3.1 *Future technologies in shipbuilding*

Considering that the speed of innovation is accelerating, especially with the emergence of new digital industrial technologies known as Industry 4.0, which rely on transformational cyber physical systems (CPS) technologies, participants will find useful information regarding future technologies that can affect the transformation in the shipping industry and maritime transport.

Based on technologies that include cloud computing, blockchain, Internet of Things (IoT) and sophisticated sensors, data collection and analytics, advanced robotics, machine learning and artificial intelligence.

Participants will be familiar with future technologies in shipbuilding, like: Digitalization Area, Autonomous Vessel, Commercial Shipping and Management Operations, Internet of Vessels and Digital Platforms and Trade Finance and Logistics.

2.3.2 *Smart ship solution*

Participants will find short description information's regarding the Smart Sensor onboard ship.

2.3.3 *Some considerations regarding Cyber-Physical Systems*

Taking into account most relevant OT systems contain various Cyber-Physical Systems (CPS) and they have become important enablers for modern ship, the participants will familiarized with this concept and also with CPSs' security. They also will understand some of the common attacks that impact on the above-mentioned priorities of the CPS, like: Eavesdropping, Compromised Key attack, Man-in-the-Middle attack, Denial-of-Service attack.

2.3.4 *Some considerations regarding IoT vulnerabilities*

Participants will learn about the future OT systems on board ship and CPS that will be part of IoT, have in mind that the majority of IoT devices operate autonomously in unattended environments.

In this subchapter will provide an exhaustive review addressing such vulnerabilities and their various dimensions for IoT, like: Deficient Physical Security, Insufficient Energy, Inadequate Authentication, Improper Encryption, Unnecessarily Open Ports, Insufficient Access Control, Improper Patch Management Capabilities, Weak Programming Practices and Insufficient Audit Mechanism.

Participants will be found also the map for IoT vulnerabilities and Security Impact and finally the summary of remediation strategies.

Self-Assessment quiz.

Co-funded by the Erasmus+ Programme of the European Union

4.0 Teaching Materials

The methods of this lesson are lectures, group work, PowerPoint, documents, video and other e-learning supporting materials.

Books:

- Maritime Cybersecurity: A Guide for Leaders and Managers (Gary C. Kessler, Steven D. Shepard, 2020).

PowerPoint

The PowerPoint will be explained by voice and text in an e-learning module.
Lectures presentation and movies examples.

Websites:

- http://www.navarino.co.uk/wp-content/uploads/2018/04/Crew_Connectivity_2018_Survey_Report.pdf
- https://pearl.plymouth.ac.uk/handle/10026.1/11245
- https://www.ics-shipping.org/wp-content/uploads/2020/08/guidelines-on-cyber-security-onboard-ships-min.pdf
- Information Security Audit and Control Association, "The Merging of Cyber-security and Operational Technology", pages 1–8, 2016
- https://cybersail.org/wp-content/uploads/2017/02/IHS-BIMCO-Survey-Findings.pdf
- http://www.shippipedia.com/ship-automation-control-system/
- Skema , "Interactive Knowledge Platform For Transport And Logistics, Navigation systems including developments in e-navigation", 2019, http://www.eskema.eu/defaultinfo.aspx?topicid=47&index=4
- Maria Papadaki, Kimberly Tam, Kevin D. Jones, "Threats and Impacts in Maritime Cyber Security", https://www.researchgate.net/publication/304263412_Threats_and_Impacts_in_Maritime_Cyber_Security
- https://marine-digital.com/article_technologies_in_shipbuilding?utm_source=site_mds&utm_medium=post&utm_campaign=article_Transformational_technologies
- https://marine-digital.com/article_sensors?utm_source=site_mds&utm_medium=post&utm_campaign=article_robotics_in_maritime_industry

Videos links:

- https://www.youtube.com/watch?v=BLLu-sm9x8w
- https://www.youtube.com/watch?v=P0F3OxcDFQg
- https://www.youtube.com/watch?v=2naiQd-U_kM
- https://www.youtube.com/watch?v=sz57s7dlmSk
- https://www.youtube.com/watch?v=WhSo4DLhjz4

Co-funded by the Erasmus+ Programme of the European Union

- https://www.youtube.com/watch?v=WGi-_7HP3Hg
- https://www.youtube.com/watch?v=MNn2M3BD8eA
- https://www.youtube.com/watch?v=bqrKAoVJsi4

5.0 Socrative Questioning

Tips for Using Socratic Questioning:

- plan significant questions that provide meaning and direction to the dialogue;
- use wait time: Allow at least thirty seconds for participants to respond;
- follow up on participants' responses.

Ask probing questions:

- periodically summarize in writing key points that have been discussed;
- draw as many participants as possible into the discussion;
- let participants discover knowledge on their own through the probing questions the teacher poses.

Socratic Question Type	Example
Clarification questions	What do you mean by OT system on board ship? Can give some examples of OT system on board ship? How we affect OT systems on board ship? Could you give us an example of future technologies in maritime industry?
Questions about an initial question or issue	Why is this question important? Is this question easy or difficult to answer? Why do you think that?
Assumption questions	Why would someone make this assumption? What is _____ assuming here? What could we assume instead? You seem to be assuming _____.
Reason and evidence questions	What would be an example? Why do you think this is true? What other information do we need? Could you explain your reason to us?
Origin or source questions	Is this your idea or did you hear if from someplace else? Have you always felt this way? Has your opinion been influenced by something or someone?
Implication and consequence questions	What effect would that have? Could that really happen or probably happen? What is an alternative? What are you implying by that? If that happened, what else would happen as a result? Why?

Co-funded by the Erasmus+ Programme of the European Union

6.0 Self-Assessment quiz for topic

- Describe the IT and OT ship equipment.
- Identify critical vulnerabilities in common OT systems and Industrial Control Systems (ICS) on board ship.
- Describe the cyber risk and threats related to the heavy reliance on navigation and communication systems.
- Identify CPS in engine room and the role of IoT and their cyber risk.
- Describe the IoT vulnerabilities and their impact on core security objectives.
- Describe the future technologies can be applied in maritime industry.

Co-funded by the
Erasmus+ Programme
of the European Union

Appendix 2/3 – Example lesson

Lesson plan – Module 3: International legal framework and guidance on cyber and maritime cybersecurity

1.0 Introduction

This lesson will provide an introduction to the main IMO and EU legal issues, guidance and standards surrounding cyber risk management and highlight their implementation through corporate policies and procedures. Participants will be provided, on managerial level, the context of the IMO and EU framework and by this understand industry actions on guidance and recommendations and their implementation within company's policies and procedures. Importantly for managerial level, this lesson will also provide an insight into implications of cybersecurity for commercial responsibilities and operation of the vessel.

2.0 Learning Outcomes

The participants at end of this module will achieve the following LOs:

1.4. Indicate and summarise the EU legal framework and guidelines, and IMO guidance on maritime cybersecurity;
1.5. Summarise the Cyber Risk Management process according to the relevant maritime-related guidelines
3.1. Apply the cyber risk management framework to prevent attacks in accordance with Safety Management Systems (SMS) requirements;
3.2. Recognise incidents or cyber-attacks on board IT and OT systems and devices connected to the digital networks services;

3.0 Teaching Methods

E-Learning which will include PowerPoint, video's, independent research, suggested reading, question and answers.

Module Content

3.1 Overview of EU legal framework and guidelines related to cybersecurity and in maritime sector

- EU's cybersecurity strategy (EU Cybersecurity Strategy)
- EU's Cybersecurity act (Reg. UE 2019/881 on 16 April 2019)
- Electronic Identification Authentication and Signature (EIAS) (Reg. UE n°910/2014 on 23 July 2014)
- General Data Protection Regulation GDPR (EU 2016/679 on 27 on April 2016)
- Network and Information Systems - NIS Directive (EU 2016/1148 on 16 July 2016)

Co-funded by the Erasmus+ Programme of the European Union

- European Network and Information Security Agency (ENISA) & guidelines published on maritime sector
- other EU references and guidelines as Transport Cybersecurity Toolkit edition December 2020 (Toolkit)

3.2 Overview of IMO codes and guidance related Maritime safety and security and on Cybersecurity

- ISM and ISPS Codes
- IMO Resolution MSC.428(98) and MSC_FAL.1/Circ.3
- Legal role for Member Governments' and Flag Administrations' requirements, as well as relevant international and industry standards and best practices (please see par. 4.1 IMO MSC FAL 1/circ.3)

Please refer also to docs listed on Teaching material 4.0

3.3 Overview of Industry guidelines related Maritime Cybersecurity

- The Guidelines on Cyber Security onboard Ships[3]
- International Association of Classification Societies (IACS) and Classification Societies
- DNV-GL (guidelines)
- NIST Framework (website)
- ISO/IEC 27001 standard on Information technology (website)

Please refer also to docs listed on Teaching material 4.0 added docs

3.4 Legal impact of cybersecurity on commercial operations of the vessel:

- Contracts, third parties, P&I cover, seaworthiness, concept of prudent shipowner; crew competence and negligence, safe port.

Lesson plan

This lesson will be one e-learning lesson which sets out perspectives from EU, IMO and Maritime Industry in the order mentioned in the modules content followed with; Insight will be given into implications of cybersecurity for commercial responsibilities and operation of the vessel.

This lesson provides the basis for instruments into cybersecurity frameworks and guidelines on which other lessons can connect.

The E-learning will incorporate some questions and answers. The E-learning can be stopped to research a question or the read related documents in order to find the answer. To engage

[3] As indicated in last version 4 – Produced and supported by: BIMCO, Chamber of Shipping of America, Digital Containership Association, International Association of Dry Cargo Shipowners (INTERCARGO), InterManager, International Association of Independent Tanker Owners (INTERTANKO), International Chamber of Shipping (ICS), International Union of Marine Insurance (IUMI), Oil Companies International Marine Forum (OCIMF), Superyacht Builders Association (Sybass) and World Shipping Council (WSC).

in E-learning participants will be provided with short case studies or articles. This approach allows learners research area's more relevant to their point of interest.

The E-learning make it possible to review whenever needed in other lessons on chapter four, five and six.

4.0 Teaching Materials

E-learning presentation text (where feasible in voice), including video and articles.

Reports

- IBM Security X-Force Threat Intelligence Index 2021
- Accenture State of Cybersecurity Report 2020
- Allianz Safety and Shipping Review 2020
- Allianz Risk Barometer 2020: Cyber top peril for companies globally for the first time
- Safety at Sea and BIMCO Cyber security White Paper, 2020, HIS Markit
- Managing Cyber Risks and the Role of the P&I Club: An Overview, 2020, ABS Group
- Japan P&I Club (2020) P&I Loss Prevention Bulletin: Cyber risk and cyber security countermeasures.

Books

- Cyber Security Workbook for On Board Ship Use 2021 Edition.

References

Will be incorporated into the e-learning for EU legal framework on data protection, cybersecurity and guidelines on maritime sector:

- General Data Protection Regulation (GDPR): REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC;
- EU NIS Directive: DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union;
- EU Cybersecurity Act: REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013;
- The EU's Cybersecurity Strategy for the Digital Decade: JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on December 16, 2020;
- European Commission (Directorate-General for Mobility and Transport - DG MOVE) 'Cybersecurity Toolkit' (December 16, 2020);
- ENISA: Cyber Security Aspects in the Maritime Sector (December 19, 2011);
- ENISA: Port Cybersecurity – Good practices for cybersecurity in the maritime sector (November 26, 2019);

- ENISA: Guidelines – Cyber Risk Management for Ports (December 17, 2020);
- Reg. UE n°910/2014 del 7/23/2014 «EIDAS» - Electronic Identification Authentication and Signature.

Will be incorporated into the E-learning for IMO guidance on Maritime Cyber risk Management:

- SOLAS Convention (1974);
- The International Safety Management (ISM) Code (1998) (IX chapter of SOLAS);
- The International Ship and Port Facility (ISPS) Code (2004) (XI-2 chapter of SOLAS);
- IMO Resolution MSC.428(98), adopted 16 June 2017 - Maritime Cyber Risk Management in Safety Management Systems;
- IMO MSC-FAL.1-Circ.3, of 5 July 2017, Guidelines on Maritime Cyber Risk Management (Secretariat);
- IMO MSC 101/4/4, of 26 March 2019, Measure to enhance Maritime Security – Cyber risk management in Safety Management System.

Will be incorporated into the E-learning for Maritime Industry guidelines and standard and other references:

- The Guidelines on Cyber Security onboard Ships - Version 4, on December 12, 2020, Produced and supported by BIMCO, ICS etc.;
- ISO/IEC 27001 standard on Information technology – Security techniques – Information security management systems – Requirements. Published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC);
- NIST Framework: the US National Institute of Standards and Technology (NIST) edit «Framework for Improving Critical Infrastructure Cybersecurity» called «Cybersecurity Framework» (2018);
- BIMCO Cyber Security Clause (2019);
- ICS Circular: Clause Model published by the Lloyds Market Association for Cyber Risks, (2019);
- IACS (International Association of Classification Societies) Single Standalone Recommendation on Cyber Resilience (April 2020);
- DCSA (Digital Container Shipping Association) Implementation Guide for Cyber Security on Vessels» (v. 1.0 - March 2020);
- Best Practices for Cyber Security On-board Ship (FR) (v. 1.0 - October 2016);
- IET Standard (UK) - Code of Practice: Cyber Security for Ports and Port Systems (v.2 – January 2020);
- IET Standard (UK) - Code of Practice: Cyber Security for Ship (v.1 – September 2017).

Websites

On EU:

- (EU Strategy) https://ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade

- (EU Mobility and Transport) https://ec.europa.eu/transport/sites/transport/files/cybersecurity-toolkit_en.pdf
- (EU cybersecurity) https://ec.europa.eu/transport/themes/security/cybersecurity_en
- (EU GDPR Regulation) https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=IT
- (EU NIS Directive) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148
- (EU Cybersecurity Act) https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881&from=IT
- (EU ENISA) https://www.enisa.europa.eu/
- (EU ENISA) https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1
- (EU ENISA) https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector
- (EU ENISA) https://www.enisa.europa.eu/publications/guidelines-cyber-risk-management-for-ports

On IMO:

- (IMO) https://www.imo.org/en
- (IMO on Cybersecurity) https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx
- (IMO on ISM Code) https://www.imo.org/en/OurWork/HumanElement/Pages/ISMCode.aspx
- (IMO on ISPS Code) https://www.imo.org/en/OurWork/Security/Pages/SOLAS-XI-2%20ISPS%20Code.aspx
- (IMO Resolution MSC.428(98) https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf
- (IMO MSC-FAL.1/Circ.3) https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf

Others websites

- https://www.bimco.org/
- https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships
- https://www.bimco.org/contracts-and-clauses/bimco-clauses/current/cyber-security-clause-2019
- https://www.iso.org/home.html
- https://www.iso.org/isoiec-27001-information-security.html
- https://www.nist.gov/
- https://www.nist.gov/cyberframework
- https://www.ics-shipping.org/

Co-funded by the Erasmus+ Programme of the European Union

- https://www.icc-ccs.org/
- https://www.ssi.gouv.fr/
- https://www.gov.uk/government/publications/ship-security-cyber-security-code-of-practice
- https://www.gov.uk/government/publications/ports-and-port-systems-cyber-security-code-of-practice
- https://dcsa.org/
- https://dcsa.org/standards/cyber-security-guide/
- https://www.iacs.org.uk/
- https://www.dnv.com/
- https://www.dnvgl.it/assurance/cyber-security/index.html
- https://www.rina.org/en
- https://www.accenture.com/_acnmedia/PDF-116/Accenture-Cybersecurity-Report-2020.pdf
- https://www.allianz.com/content/dam/onemarketing/azcom/Allianz_com/press/document/Allianz-Risk-Barometer-2020-press-release_EN.pdf

5.0 Socrative Questioning

Will be incorporated into the E-learning.

6.0 Self-Assessment quiz for topic

Will be incorporated into the E-learning.

Appendix 3

Module Content[4]

Modules	Lessons	Module Content* *Not exhaustive list, please refer also to example lesson in Appendix 2/1*
1. Cybersecurity awareness	**1.1.** Basic elements and actual contest/scenario on Cyber global risk and threats	– Basic definition and terms in use in the Cyber Domain (What is Cyber, Cyberspace, Cybersecurity, Cybercrime). – The actual global scenario on Cyber Threats.
	1.2. Cyber risk and threats	– Common cyber tools as malware: ransomware, ransomware double-extortion, Trojan, Spyware, Worms – Different types of threats: external and internal attacks, accidents, tampering, etc.
	1.3. Cyber threats – key actors	– Prevalent threat actors and motivations. Hackers, activist, Criminal Organization, Non-State and State actors, terrorism phenomena in cyber threats, cheats and racketeer.
	1.4. Cyber threats – techniques and tactics	– Common Cyber infiltration: techniques and tactics: phishing, spear-phishing, water-holing, social-engineering, undermining supply-chain, brute-force, bot and bot-net, hoaxing, whaling, smishing, pop-up windows, baiting.
	1.5. Cyber kill chain	– The cyber kill chain illustrates the structure of a successful cyber-attack. It defines the steps used by cyber attackers in today's cyber-based attacks. The theory is that by understanding each of these stages, defenders can better identify and stop attackers at each of the respective stages.

[4] This Module Content illustrates the indicative content of the lessons that can be adaptable to the specific learning needs.

	1.6. Introduction to CIA Triad Model – key elements	– The CIA triad represents the functions of the information systems. It is a security model that companies should follow in order to protect information stored in on-premises computer systems or in the cloud. It helps to: ▪ keep information secret (Confidentiality); ▪ maintain the expected, accurate state of that information (Integrity); ▪ ensure that the information and services are up and running (Availability).

Co-funded by the
Erasmus+ Programme
of the European Union

Modules	Lessons	Module Content* *Not exhaustive list, please refer also to example lesson in Appendix 2/2*
2. Maritime Cybersecurity awareness	**2.1** Main topics on Cyber Risk in the maritime domain for shipping industry and onboard	– The Maritime Cybersecurity threat landscape. – Recurring Maritime Cyber Threat and trends. – Understand the differences between cyber risk in the maritime sectors. – New scenarios in the Maritime domain. – The specificity of cyber risks in the maritime sector compared to other areas.
	2.2 Information Technology (IT) and Operational Technology (OT) systems onboard – vulnerabilities and threats – Shipboard Networks	– Focus on Informational Technology (IT) and Operational Technology (OT) Systems onboard. – Cyber term refers into maritime domain of interconnected networks of IT and OT ship system. – Critical cyber aspect on IT and OT maritime systems and identify vulnerability.
	2.3 Digital transformation and new technologies in shipping industry and onboard ships	– New digital technologies in Shipping Industry and onboard merchant vessels. – Evolving Cyber-Attack Surfaces. – Increasing automation ad regulations and vulnerability.

Co-funded by the Erasmus+ Programme of the European Union

Modules	Lessons	Module Content* *Not exhaustive list, please refer also to example lesson in Appendix 2/3*
3. International legal framework and guidance on Cyber and Maritime Cybersecurity	**3.1.** EU references on cybersecurity and guidelines on maritime sector	– New EU's Cybersecurity Strategy (ref.). – GDPR Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. – Network and Information systems (NIS) – Directive (EU) 2016/1148 on 16 July 2016, concerning measures for a high common level of security of network and information systems across the Union and new NIS 2.0. – ENISA and Maritime Cybersecurity Guidelines published: *Analysis of Cybersecurity aspects in the Maritime Sector* (November 2011). – Port Cybersecurity – Good practices for cybersecurity in the maritime sector (November 2019) and Cyber Risk Management for Ports – Guidelines for cybersecurity in the maritime sector (December 2020). – Other EU references and guidelines (e.g., Transport Cybersecurity Toolkit edition December 2020). – Reg. UE n°910/2014 on 23 July 2014 «EIDAS» - Electronic Identification Authentication and Signature. – Reg. UE 2019/881 on 17 April 4/17/2009: Cybersecurity Act.
	3.2. IMO guidance	– ISM and ISPS Codes. – IMO Resolution MSC.428(98) adopted 16 June 2017 Maritime Cyber Risk Management in Safety Management Systems. – IMO MSC FAL.1/Circ.3 Pubbl. 5 July 2017 "Guidelines on Maritime

		Cyber Risk Management in Safety Management Systems". - Certification requirements. - Other IMO relevant document (e.g., IMO MSC 101/4/4 Pubbl. 26 March 2019. - Measure to enhance Maritime Security - Cyber risk management in Safety Management Systems (SMS).
	3.3. Maritime Industry guidelines and other guidance and standards **3.4.** Legal impact of Cybersecurity on commercial operations of the vessels	Industry guidance and standard: - Guidelines on cybersecurity board Ships issued by Shipping Industry (BIMCO, CLIA, ICS, etc.); - ISO/IEC 27001 standard on Information technology; - NIST Framework. Other's international reference, guidelines and standards, as follows e.g.: - DCSA Cybersecurity guide; - DNV-GL recommendation practice on cybersecurity; - Other's guideline and recommend documents; - Contracts, third parties, P&I cover, seaworthiness, concept of prudent shipowner; crew competence and negligence, safe port.

Co-funded by the Erasmus+ Programme of the European Union

Modules	Lessons	Module Content
4. Maritime Cyber Risk Management process, key elements and Best Practices for maritime professionals	**4.1.** Analysis of Maritime Cyber Risk Management process: - assessing the likelihood; - impact assessment (CIA triad model and critical system on maritime sector); - risk assessment (four phases and third party); - protection measures (protection in deep, technical and procedural measures); - detection protection measures; - contingency plans; - response and recover procedures occurred by cyber security incidents onboard.	Maritime Cyber Risk Management process based on analysis of essential guidelines on Cyber Security onboard ships produced by Maritime Industry (primarily guideline produced and supported by BIMCO, ICS). The lessons of this module must guide the course participants to analyse and understand the essential aspects and steps for the Cyber Risk Management onboard ships and in general in the management of maritime shipments. In particular by touching the following points: – assessing the likelihood; – impact assessment (CIA triad model and ship's critical system); – risk assessment (four phases and third party); – protection measures (protection in deep, technical and procedural measures); – detection protection measures; – contingency plans; – response and recover procedures occurred by cyber security incidents.
	4.2. Cybersecurity Best practices for maritime professionals.	– Practical tools and ways to mitigate and avoid, when it is possible, incidents, threats and cyber risks dedicated to maritime professionals.

Co-funded by the Erasmus+ Programme of the European Union

Modules	Lessons	Module Content
5. Main cyber-attacks in the shipping industry	**5.1** Overview on main cyber–attacks in the shipping industry.	– Description of main cyber events/attacks suffered in the shipping industry in recent years. – Underline the evolution of cyber-attack methods during time.
	5.2 Analysis and Case Studies.	– Analysis on previous events and discussion on specific "Case Studies".

Modules	Lessons	Module Content
6. Maritime cybersecurity: training and practical activities.	**6.1** OT training scenarios. **6.2** IT training scenarios.	– Simulation of OT training scenarios on onboard system (ECDIS, SCADA etc.). – Simulation of IT training scenarios on computer systems onboard and ashore in Maritime Company: malicious e-mail received onboard and ashore computer; and cyber-attack to main system/server ashore (typical ransomware attack).

Appendix 4 – Example Assessment Case 1

OT Case – GNSS/ECDIS interference

Case construction (Teacher)

The case can be authentic, fictional or a mix. The example case must be based on real-life or on a realistic fictitious scenario. The case should be related to the shipping business, including a merchant ship, on a Company or both of them, with an initial description of the initial circumstances.
The problems encountered and the different phases of the case, that concern the governance and technical ship level, will be described. Participants will have to analyse and/or solve the problems since their origin, including thorough discussion and interaction with the teacher.
This activity should be based on using the knowledge, skills and competences described in the learning outcomes. Therefore, it is important that the problems described demonstrate that the course's learning outcomes have been achieved; see Appendix 1 (Constructive Alignment Table).
The task may be assigned to individual participants or a group of them. In the latter case, each group may be responsible for various aspects or share the same task.
It is very important to make sure that participants are fully aware of the learning outcomes they have to achieve. This can also be done by including learning outcomes in the case description.
In addition to the description and the problems presented (accident or IT attack or OT problems/incident), the case may also contain appendices holding relevant data and/or important information to the case's description and development.
The relevant data can be in the form of a scenario in graphic form (picture), but also others document (Word or Excel) as well as reference information of particular interest through links to specific websites can be added.
The goal is to demonstrate how cybersecurity problems must be understood, evaluated, and addressed with awareness. An exemplary case, this will allow participants to understand how to apply the course contents to their daily needs, is reported below.

The following text is an example of the exam case that will be proposed to the participants.

Introduction

This case will be used during the course (in **Module 6**: ***Maritime Cybersecurity: training and practical activities***) and will be used to put into practice and apply the knowledge and skills acquired in the previous modules and related lessons of the entire course.
The training scenario is therefore postponed to the end of the five theoretical modules of the course. Therefore, participants will have the possibility and the opportunity to respond to all or most situations (incidents or cyber-attacks) proposed.
It is not possible completing the simulation or addressing all the challenges before the end of the course. To reach such a goal, it will be essential having followed all the lessons of the previous modules and have developed all the required skills.

Case report

A written report to reply to the exam case can be produced and handed to the teacher at the end of the simulation (according to the lesson plan). The written report should contain all relevant answers to the problems submitted and to the challenges identified in the case. It is advisable to repeat

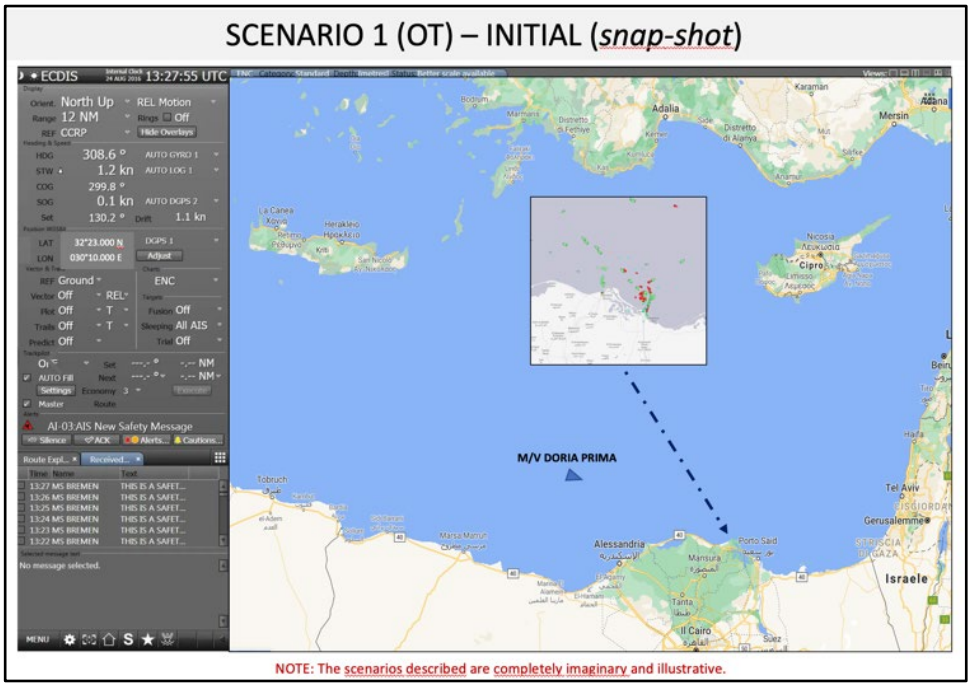
Co-funded by the
Erasmus+ Programme
of the European Union

several times the case phases considered more difficult by participants. The report describes the main issues identified by participants and how they have tried to solve them. Finally, they will demonstrate the learning outcomes of the course.

Case Description

Scenario

- You are Master of the vessel MV DORIA PRIMA on a fully loaded voyage, departing from Genova Terminal (Italy) and heading to Khalid Port, Sharjah (UAE).
- The vessel is bound for a port in India, and within a few hours, it will arrive in the proximity of Port Said for transit through the Suez Canal. We are at dusk. The vessel is navigating using ECDIS.
- The vessels position is 32°23'00'N, 030°10'00''E, East Mediterranean Sea, close to the Egyptian coast (see snap-shot).



The weather and the sea conditions are good but worsening is expected soon; storms and the very rough sea is expected from the South-East.
Furthermore, from what is known, the traffic present in Port Said's area is quite intense.
The Company has recently released a circular, published by a well-known private Intelligence Analysis Company, about the possible presence of electronic interference to the satellite navigation capabilities in some areas of the Eastern and Central Mediterranean Sea.

Co-funded by the
Erasmus+ Programme
of the European Union

Details about M/V DORIA PRIMA

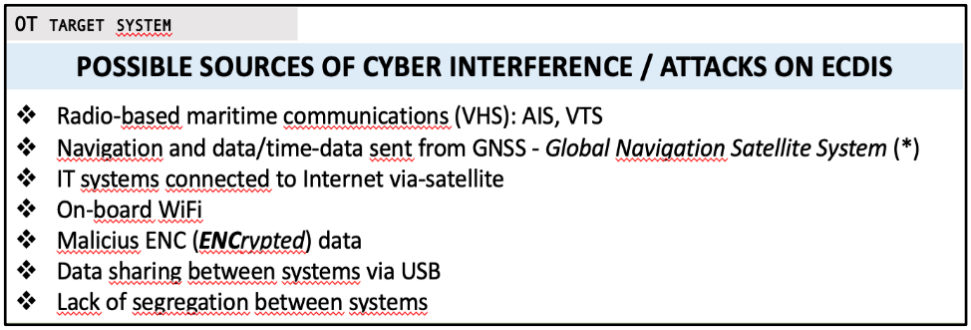
MV DORIA PRIMA is an RO-RO Cargo vessel (IMO: 91705734567), flying the Italian flag, owned by the OSC (Oceanic Shipping Company). Details (*notional*) can be found on https://www.marinetraffic.com/.

Loading the scenario

Due to ongoing technical problems, probably linked to difficulties in digital satellite connection, the MV DORIA PRIMA Master is having problems to contact the Company headquarter using all communication channels (SATCOM, VOIP, e-mail). Also, interferences on the VHF channels are recorded, preventing communications with other ships in the area and with the destination port's maritime authorities. Even via the INMARSAT telephone, communications are strangely disturbed and almost intelligible. The radar screen is disturbed. The AIS system is active.
After checking the ship's route, the 1st Mate informs the Master that he doubts the exact position.

Development of the scenario

1. You are the ship's Master. What actions are you going to implement after being aware that your ship has suffered/is suffering problems with the ECDIS electronic navigation system following the checks carried out? (The answer will have to be 10/15 lines max.)



2. Following the checks performed, given the information, it is likely that the problem is due to interference on the GNSS satellite system:
   What technical and operational actions should be taken?
   What are the further actions that you and Company can take?

3. In which order would you put the various actions to be implemented?
   What would you do later than the resolution of the problem?

Discussion topics – Socrative Questioning

A. Does the crew have to be informed? If so, at what level and on what?
B. What type or technique of interference/cyber-attack has the ship suffered?
C. According to the probable technique/type identified, can shipping operations continue?
D. Which actions would you take on board?

Co-funded by the
Erasmus+ Programme
of the European Union

E. What immediate actions can or should the Company perform after being informed about circumstances?
F. Would you find it useful to inform/compare your situation with other ships in the proximity?
G. Is it necessary to draw up a report on the incident? If so, to whom should it be sent in the first instance?
H. What measures for containment/reduction of interference/attack must be ordered by the Master of the ship immediately?
I. What containment/reduction measures of the interference/attack suffered by the ship must be arranged by the Company?
J. Should the Company take other actions? For example:
    - revision/update the Cyber Risk Management procedure on DoC and SMS;
    - informative note to the Masters of the Company's ships navigating the area where the cyber event occurred or to the entire fleet.

Co-funded by the
Erasmus+ Programme
of the European Union

Example Assessment Case 2

IT Case - Create backup and use PGP encryption

The participants will be provided with laptop, external USB (and access to online cloud service). The exercise consists in:

- creating a backup of participant's data (or dataset provided by teacher) to external USB media (and to online cloud storage);
- restoring data from the backup;
- writing short report on the actions above and send it with PGP encrypted e-mail to teachers e-mail address.

Example Assessment Case 3

OT Case - ECDIS infected with ransomware

Set bup ECDIS station with charts and sensors connected (real equipment or emulated) and infect it with ransomware (https://github.com/ytisf/theZoo/tree/master/malwares/Binaries).
The participant should:

- understand, what happened with the system;
- know, what are the following actions (from killcard);
- know, where to get the system configuration backup files, operating system DVD, etc.;
- reinstall the operating system, ECDIS software and get the charts back.

Example Assessment Case 4

IT Case – USB media is infected with malware

The participants receive 3/4 USB medias, where one is infected with malware. The participants should:

- detect, which media is infected;
- detect, what kind of malware is on the media;
- clean the media, if possible.

Example Assessment Case 5

Governance - follow the procedures onboard the ship during the simulated cyber incident

This exercise can be carried out together with the crew and company's representatives (ISM, CISO). The aim is to employ company cyber policy in case of a cyber incident onboard the ship. This is a practical exercise that can bring out drawbacks and flaws in the policies and allows to rewrite them, that they would be more closer to reality.

Co-funded by the
Erasmus+ Programme
of the European Union

Appendix 5 – Bibliography *

**Please refer also to references listed in the example lessons (Appendices 2/1, 2/2 and 2/3)*

Books and documents:

- *Cybersecurity Workbook for On Board Ship Use*, 2021 Edition (Witherbys, BIMCO and ICS)
- *The Guidelines on Cybersecurity onboard Ships* - Version 4, December 2020 (Maritime Industry BIMCO, ICS etc.)
- *Guidelines on Cyber Risk Management for Ports*, December 2020 (ENISA)
- *Cybersecurity Toolkit*, December 2020 (European Commission)
- *Framework for Improving Critical Infrastructure Cybersecurity - Cybersecurity Framework*, ed. 2018 (NIST - National Institute of Standards and Technology)
- *New standard insurance clause for information security*, 2019 (BIMCO).
- *Analysis of Cybersecurity aspects in the Maritime Sector*, 2011 (ENISA)
- *The EU's cybersecurity strategy for the digital decade*, 2021
- *Best Practices for Cybersecurity On-board Ship*, ver. 1.0, October 2016 (published by France Ministry of Economy, Environment and Sea, under license from Agence Nationale de la Sécurité des Systèmes d'Information – ANSSI)
- *Code of Practice: Cybersecurity for Ships*, 2017 (IET Standard – The Institution of Engineering and Technology)
- *Future of the Sea: Cybersecurity*, 2017 (UK Government Office for Science)
- *Maritime Cybersecurity. A Guide for Leaders and Managers*, 2020 (G. C. Kessler, S. D. Shepard))
- *A Master's Guide to Cyber Security*, 2015 (UK Chamber of Shipping)
- *Cyber risks and Seaworthiness*, Seaways, 2017 (Clark, J. and Parson, L.)
- *Managing Cyber Risks and the Role of the P&I Club: An Overview*, 2020 (ABS Group)
- P*&I Loss Prevention Bulletin: Cyber risk and cyber security countermeasures*, 2020 (Japan P&I Club)
- *Vulnerability Management Case Study*, 2018 (Cyprus Shipping Chamber)
- ISO/IEC 27001 and the *Guidelines on Cybersecurity on Board Ships*
- ICS Circular: Clause Model published by the Lloyds Market Association for Cyber Risks, 2019
- IMO Resolution MSC.428(98), adopted 16 June 2017 - Maritime Cyber Risk Management in Safety Management Systems
- IMO MSC-FAL.1-Circ.3, of 5 July 2017, Guidelines on Maritime Cyber Risk Management (Secretariat)
- IMO MSC 101/4/4, of 26 March 2019, MEASURES TO ENHANCE MARITIME SECURITY - Cyber Risk Management in Safety Management Systems (SMS)
- JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL - The EU's Cybersecurity Strategy for the Digital Decade, Brussels 12 December 2020
- REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Co-funded by the Erasmus+ Programme of the European Union

- DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016, concerning measures for a high common level of security of network and information systems across the Union
- DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (the NIS Directive)
- SOLAS Convention 1974
- ISM (*International Safety Management*) 1998 (IX chapter of SOLAS)
- International Ship and Port Facility Security (ISPS) Code
- Regulation EU 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (Cybersecurity Act)
- REGULATION (EU) 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC - «EIDAS» - *Electronic Identification Authentication and Signature*
- Regulation (EC) 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security

Websites:

- BIMCO
- EC – European Commission
- European Commission Factsheet - The EU's Cybersecurity Strategy in the Digital Decade
- BIMCO – The Guidelines on Cyber Security onboard Ships – version 4
- DNV Italia – Cyber Security
- DCSA – Cyber Security Guide
- ENISA – European Union Agency for Cybersecurity
- ICS – International Chamber of Shipping
- IMO – International Maritime Organization
- IMO – Maritime Cyber Risk
- NIST – National Institute of Standards and Technology
- International Chamber of Commerce – Commercial Crime Services (ICC – CCS)
- ISO/IEC 27001 and related standards - Information security management
- ANSSI - Agence nationale de la sécurité des systèmes d'information

Co-funded by the
Erasmus+ Programme
of the European Union