Enhancing maritime supply chain cybersecurity: EMSA's perspective

2nd ENISA Maritime Cybersecurity Conference

Chronis Kapalidis / Project Officer for Maritime Security

Unit 2.1 : Safety & Security

Lisbon / 14 October 2022

EMSA

EMSA - Overview

27 EU Member States
and the Commission

+

2 EFTA Member States
and EFTA SA

Staff: ~ 250 people

~ 25 nationalities

Annual Budget:
~80 million EUR

Headquarters:
Lisbon, Portugal

Modern maritime supply chain: A sea of data

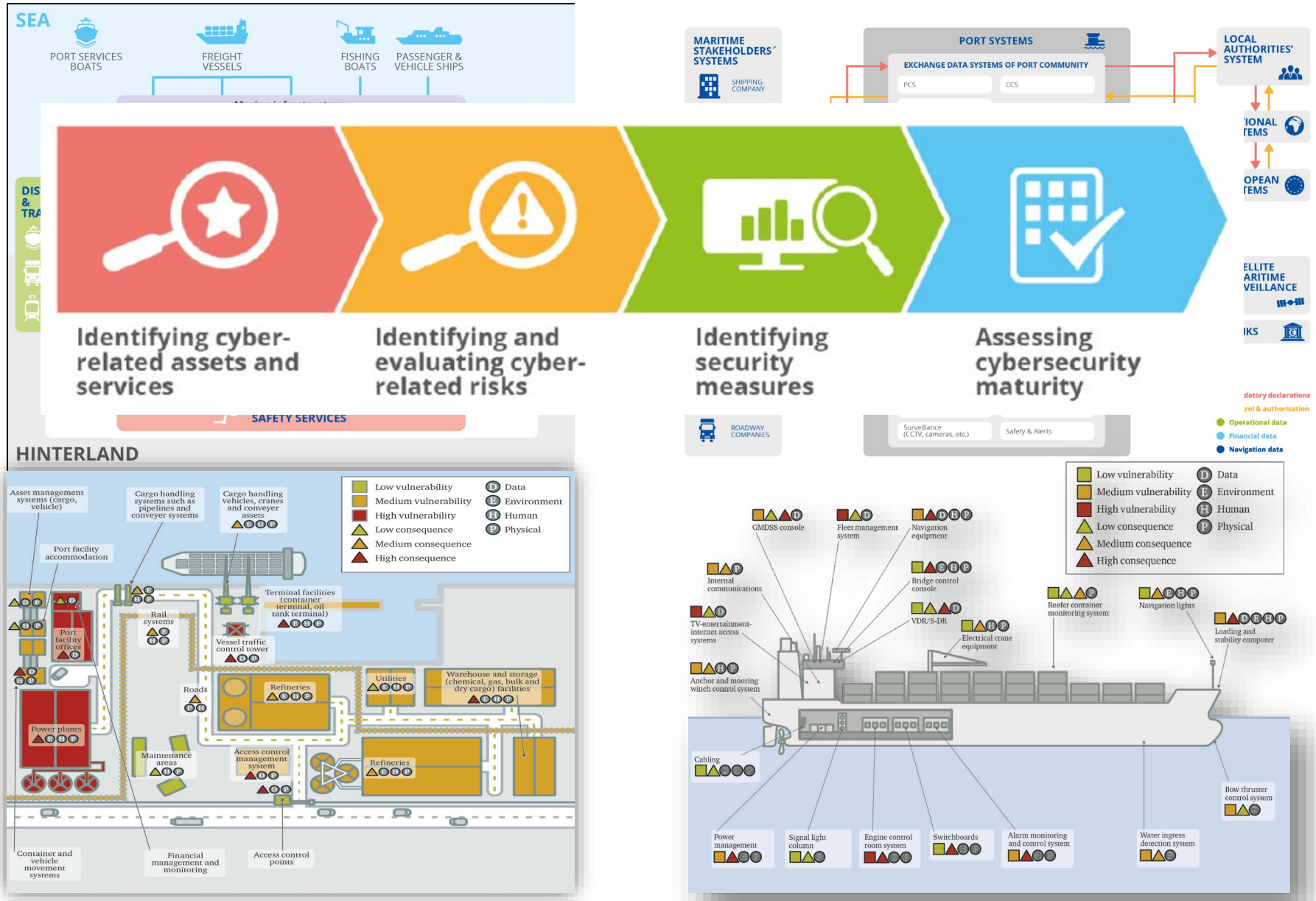
Rewards
- Customer visibility (cargo)
- Predicative Maintenance
- Navigation improvements
- Bunker efficiencies
- Fleet management
- Autonomous vessels
- Customer engagement (cruise)

Risks
- Cyber piracy
- Hacks
- Extortion
- Malware

Targets
- IoT
- ICS
- GPS
- ECDIS
- AIS
- Satellite Comms
- Third parties
- Pax

Common Vulnerabilities
- Unpatched systems
- Legacy systems
- Inadequate network and systems security (IPS, IDS, NGFW, etc.)
- Lack of staff / crew awareness
- Lack of cyber-specific procedures

Relevant work



How can EMSA help?
EMSA's Maritime Cybersecurity Activities

Overall Objective as defined by EMSA 5-year Strategy:

Enhance EMSA's role and activities in maritime cybersecurity

through

providing the platform to exchange best practices and ensure cross-sectoral cooperation on cybersecurity for the maritime cluster

and

cross-collaboration with EC, EU agencies and industry stakeholders

EMSA's Maritime Cybersecurity Work Programme

EMSA established a Cyber Task Force aiming to:

- Provide support to Commission and the Member States in the development, identification and exchange of best practices and cross-sectoral cooperation on cybersecurity for the maritime cluster.

- Contribute to European inter-agency co-operation on cybersecurity issues in the maritime transport sector.

EMSA's Maritime Cybersecurity Task Force

EMSA cybersecurity TF concluded a mapping and gap analysis exercise in 2021 where key gaps and challenges were identified.

Step 1: Mapping Exercise: 265 documents were recorded and analysed in the context of this exercise from 60 sources, including EU entities, academia and industry bodies.

Step 2: Gap identification and analysis: On-line questionnaire to EU MS.

Step 3: Development of cybersecurity action plan.

EMSA Gap Analysis: Presenting the gaps

Gap 3

Lack of EU guidelines on the implementation of the ISPS Code requirements on ship cybersecurity

Gap 5

Lack of guidelines to assist the boards on implementing maritime cybersecurity

Gap 6

Lack of guidelines on implementation of the ISPS Code requirements on port facility cybersecurity, at European level

Gap 7

Lack of guidelines on maritime cybersecurity exercises

Gap 8
Lack of guidelines to assist the shipping companies on embedding cyber hygiene among the crews

Gap 9

Reporting maritime cyber incidents

Gap 10

Cyber incidents in the context of EU maritime security

Gap 11

Gathering maritime cybersecurity information at EU level

Gap 12

Cybersecurity during crisis/emergencies

Gap 13

Maritime cyberattacks database

Gap 14

Seafarers and Ship Management personnel training and certification in cyber security

Gap 15

Integration of Cybersecurity in the Security Plans (SSP & PFSP)

Gap 16
Lack of technical skills for crew to respond and fix cybersecurity incidents on board

Gap 17

Confidentiality in Cybersecurity risk management

Gap 18

Remotely operated ships and the prevention measures within the ISPS to avoid cyber-attacks

Gap 20

Guidelines and best practices on how to conduct a cyber risk assessment for ships

Gap 21

Lack of requirements for network devices under SOLAS Convention

Gap 23

Lack of cybersecurity requirements for marine equipment for maritime navigation and radiocommunication

Gap 24

Increased security and safety of the ship by duplicating network devices connected to systems of category II and III

Gap 26

Type of cables for network applications on board ships

Gap 27

Shipborne network elements suitable for marine application

Gap 28

Segregation and segmentation of telecommunication networks

Gap 29

Lack of alternatives to global satellite navigation systems for establishing and updating the ship's position by automatic means

Gap 30

Requirements for back-up arrangements of (ECDIS) should take into account cyber-attacks

Gap 31

Lack of harmonised guidelines to enforce cybersecurity aspects during Commission inspections.

Gap 32

Maritime Cybersecurity in EMSA's webpage

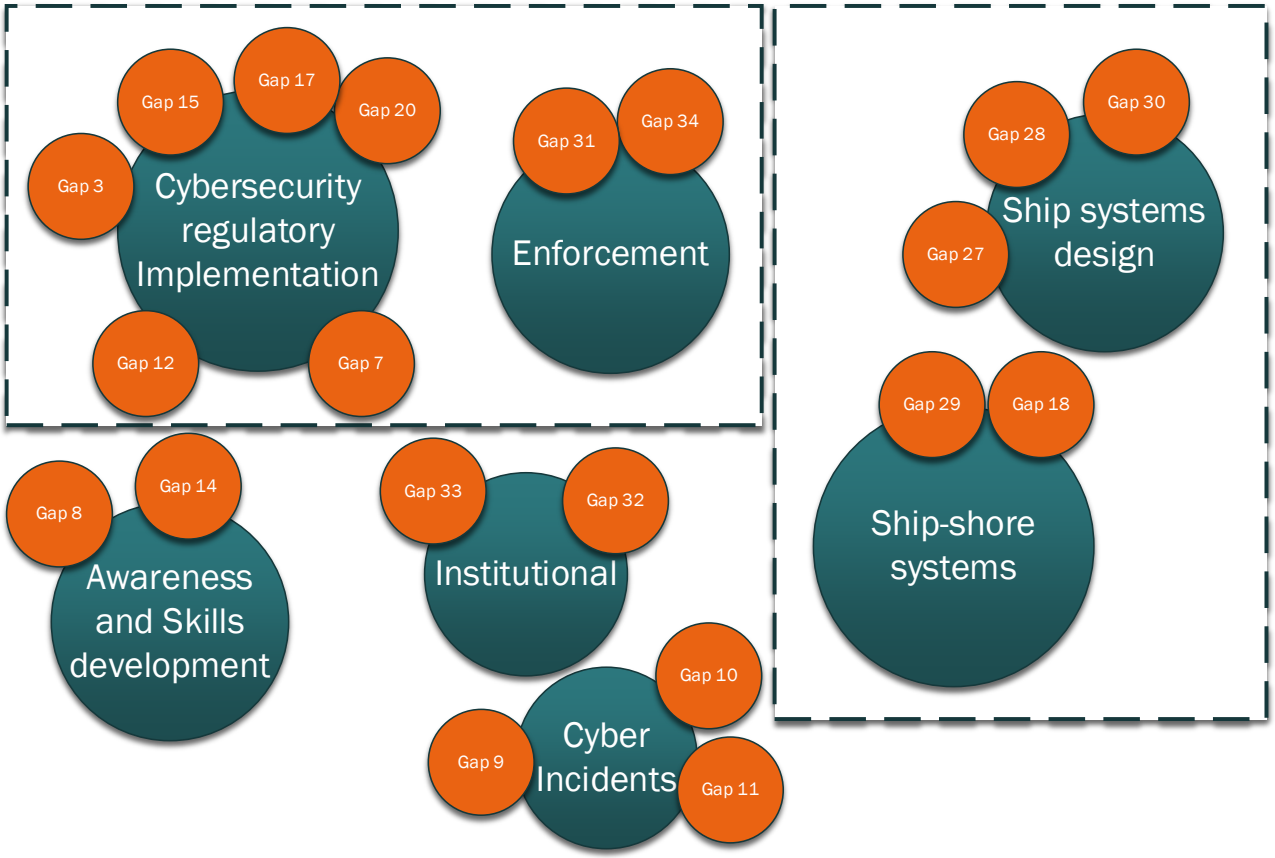
Gap 33

Contribute to the development of the network of experts on cybersecurity and cyber-defence for the maritime field within the EUMSS framework

Gap 34

Technical skills of DAO

EMSA Gap Analysis: Grouping the gaps and priority areas



1. Preparedness Ships

2. Preparedness Ports

3. Incident information management and response

4. Regulatory and enforcement

5. MASS

EMSA Gap Analysis: An example of where to focus

There is no harmonised approach in implementing maritime cybersecurity.

- Shipping mostly addresses cybersecurity through the IMO MSC. 428(98) resolution, incorporating cyber risk into SMS.

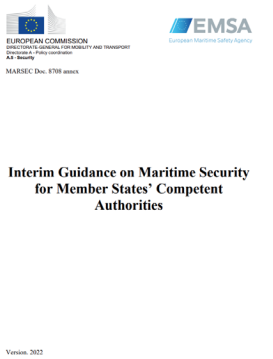
- The ISPS Code includes elements of cybersecurity which are mandatory only for EU MS (EC/ Reg. 725/2004) {Ships & Port Facilities}

- Ports can be considered Operators of Essential Services under EU NIS Directive and need to comply with specific requirements, such as incident reporting.

EMSA's Maritime Cybersecurity WP (Cyber Task Force Action Plan 2022-23)

Actions include:

- Support for the development of the EMSA Academy maritime cybersecurity training course
- Further introduction of cybersecurity in the Interim Guidance on Maritime Security for Member States' Competent Authorities
- Integration of specific cybersecurity items within the checklists for Commission maritime security inspections
- Raising awareness about and further address the cybersecurity issues related to the ongoing developments of MASS
- Organising the 1st EMSA maritime cybersecurity workshop in December 2022.



Let’s continue to work together

twitter.com/emsa_lisbon
facebook.com/emsa.lisbon

EMSA
European Maritime Safety Agency