Maritime Cybersecurity

Regulatory Framework

Lisbon / 6 March 2019

EMSA
European Maritime Safety Agency

AGENDA
Maritime Cybersecurity Table Top Exercise

Agenda: Cybersecurity Table Top Exercise

EMSA, Wednesday, 06 March 2019

Time	Item	Subject	Responsible
08.30 – 09:00	Registration		
09:00 – 11:00	Introductory Presentations	Welcome and Opening (10 Min) *Chairman*	
		EU Cyber Security Strategy *European Commission*	
		Regulatory framework governing maritime cybersecurity *EMSA*	
		Introduction to main cybersecurity terms *EMSA*	
		Main elements of the NIS Directive for Maritime Cybersecurity and the cyberattack history leading to it. *ENISA*	
		Most significant cyber attack cases that have affected the maritime industry in recent years *BIMCO*	
11:00 – 11:15	Coffee Break		
11:15 – 12:15	1st Case	Introduction of scenario and break-out sessions	
12:15 – 13:45	Lunch break		
13:45 – 14:45		Plenary session: Reports of breakout groups and discussion	
14.45 – 15:00	Coffee Break		
15:00 – 16:00	2nd Case	Introduction of scenario and break-out sessions	
16:00 – 17:00		Plenary session: Reports of breakout groups and discussion	
17:00 – 17:15	Coffee Break		
17:15 – 17:45	Conclusions and Closing *Chairman*		

EMSA

First thoughts ….

- Why is cybersecurity important to ships?
- Are we as maritime community prepared?
- What initiatives have already been taken?
- How is the maritime community reacting?
- How can we, as EMSA help?

Objectives

1. Raise awareness
2. Familiarisation of the participants with different legal/regulatory frameworks applicable to cybersecurity in the maritime domain
3. Encourage the development of a cyber culture in EU maritime security

Automation and digitization on board …

… network-based systems …

…. Increasingly dependent

Critical Ship Infrastructure

On Board System

Shore System

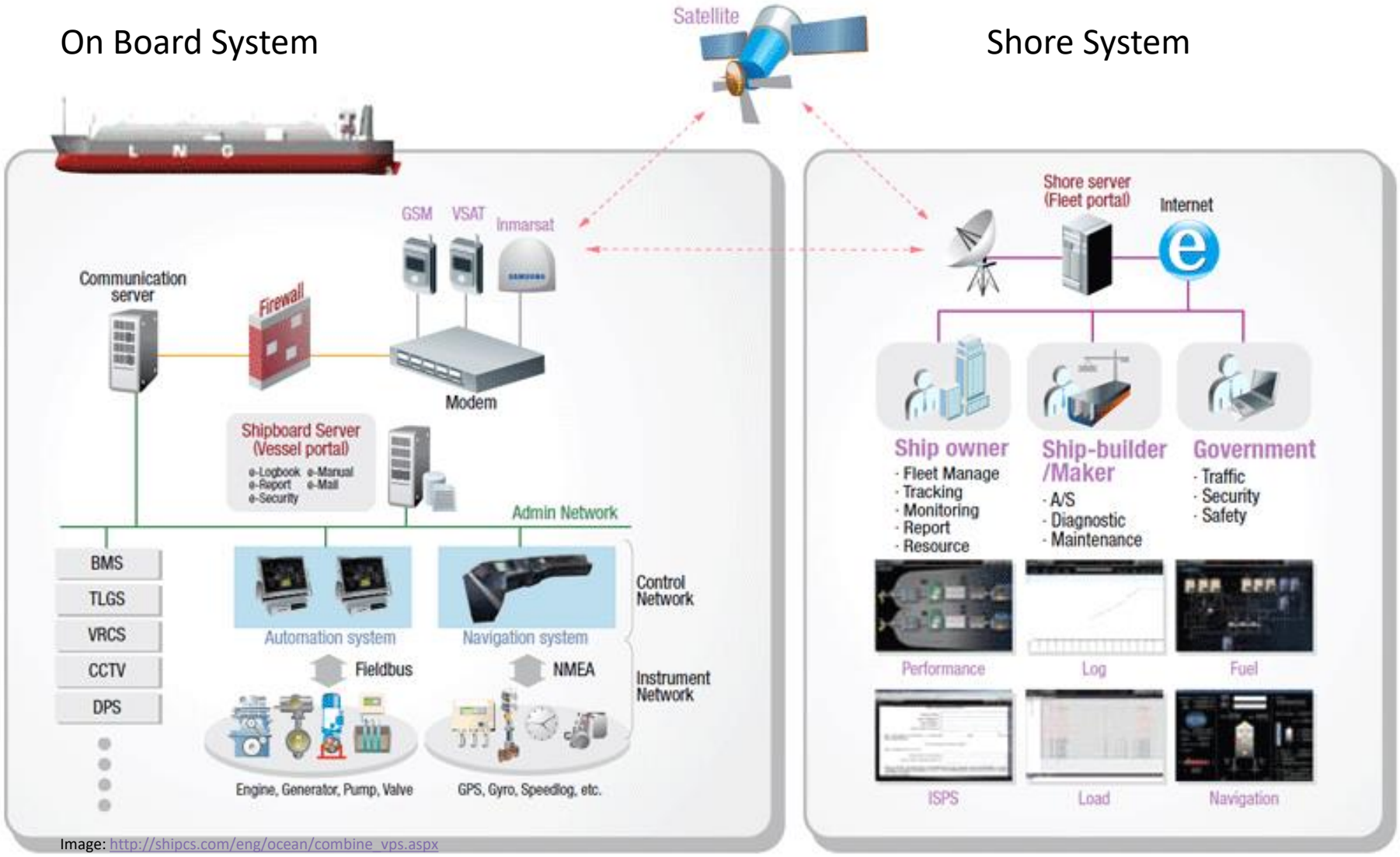
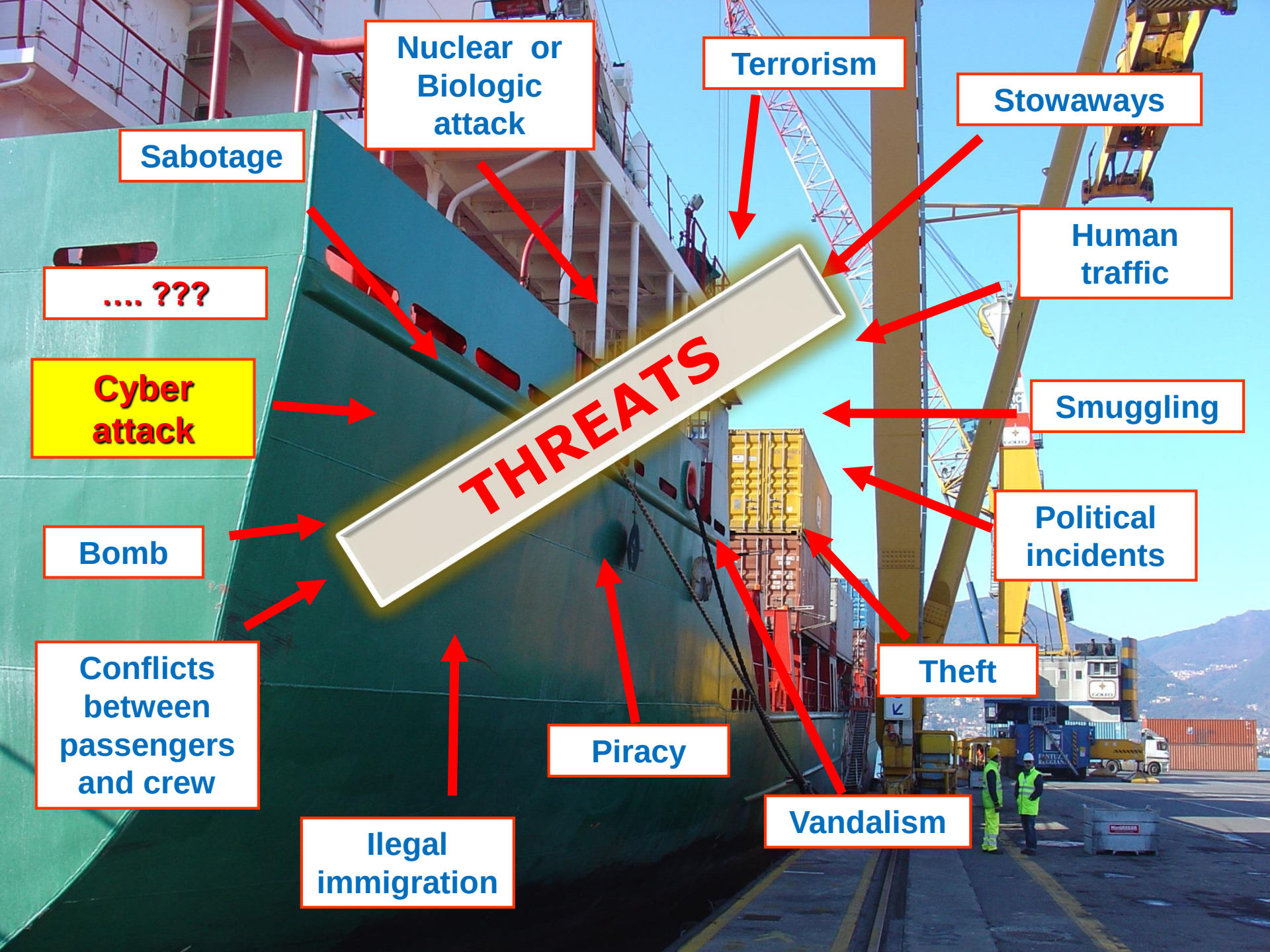


Image: http://shipcs.com/eng/ocean/combine_vps.aspx

Cyber Risks in Maritime Community …

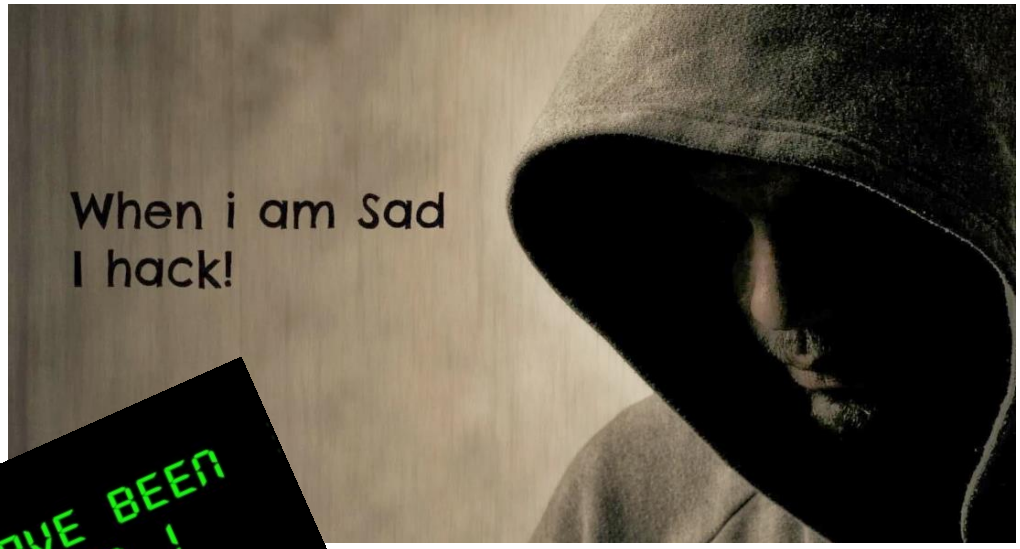
For each of these **critical information assets** there are **cyber risks** involved which may lead to:

- **Losing** information;
- **Disruption** of communication, traffic and navigational systems;
- **Distortion** of (e-)navigational data
- **Concealing** ship movements or cargo;
- **Distortion** of critical infrastructure architecture


Nuclear or Biologic attack
Terrorism
Stowaways
Sabotage
Human traffic
…. ???
THREATS
Cyber attack
Smuggling
Political incidents
Bomb
Conflicts between passengers and crew
Theft
Piracy
Vandalism
Ilegal immigration

Hacker profile …

Criminals…



Anonymous…

Opportunists…

Activists…

States & Terrorist Organisations…

EMSA

Cyber News …

U.S. Coast Guard
Sector Ohio Valley
Port Security Information Bulletin

January 31, 2019

01-2019

Suspicious Cyber Incident

On January 26 2019, a commercial vessel received an email from an individual or entity claiming to represent an official port state control body. The email originated from an email address noted as "port@pscgov.org" and was sent directly to the vessel's Master requesting sensitive information about the vessel, its crew, and its cargo. The Master was skeptical about the request and immediately activated elements of the vessel security plan related to this type of suspicious cyber incident. The vessel Master reported the incident and forwarded the suspicious email and information to the local USCG Captain of the Port for investigation and follow-up.

How hackers are targeting the shipping industry

Published on: Mon, 08/21/2017 - 10:24

When staff at CyberKeel investigated email activity at a medium-sized shipping firm, they made a shocking discovery.

"Someone had hacked into the systems of the company and planted a small virus," explains co-founder Lars Jensen. "They would then monitor all emails to and from people in the finance department."

Whenever one of the firm's fuel suppliers would send an email asking for payment, the virus simply changed the text of the message before it was read, adding a different bank account number.

"Several million dollars," says Mr Jensen, were transferred to the hackers before the company cottoned on. After the NotPetya cyber-attack in June, major firms including shipping giant Maersk were badly affected.

In fact, Maersk revealed this week that the incident could cost it as much as $300 million (£155 million) in profits.

To Move Drugs, Traffickers Are Hacking Shipping Containers

Workers at a container terminal in Antwerp began to wonder why entire containers—containing cargo like bananas and timber—were disappearing from the port.

https://motherboard.vice.com/en_us/article/bmjgk8/how-traffickers-hack-shipping-containers-to-move-drugs

BBC NEWS Sign in

News Sport Weather Shop Reel Travel

Home Video World UK Business Tech Science Stories Entertainment & Arts

World Africa Asia Australia Europe Latin America Middle East US & Canada

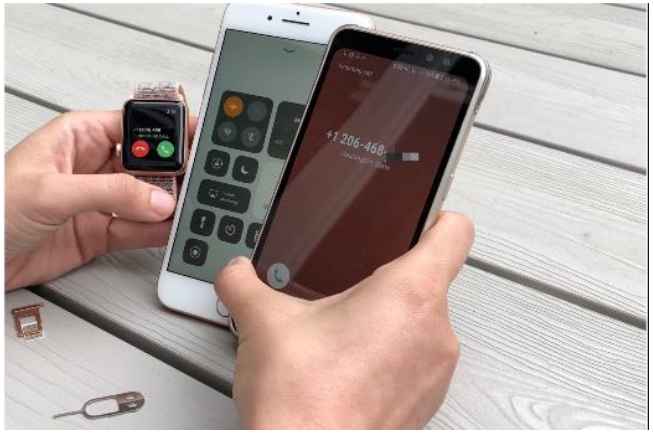
https://www.bbc.com/news/39655415

How a cyber attack transformed Estonia

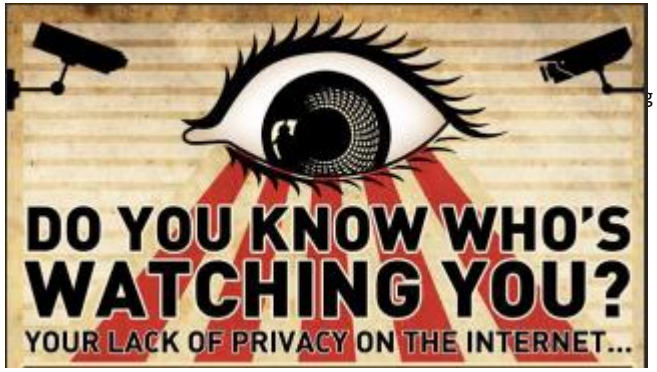
EMSA

The increase of open “doors”…

The use of digital equipment by the crew …



The use of social media …



The use of equipment in open public spaces using wi-fi…

Regulatory framework

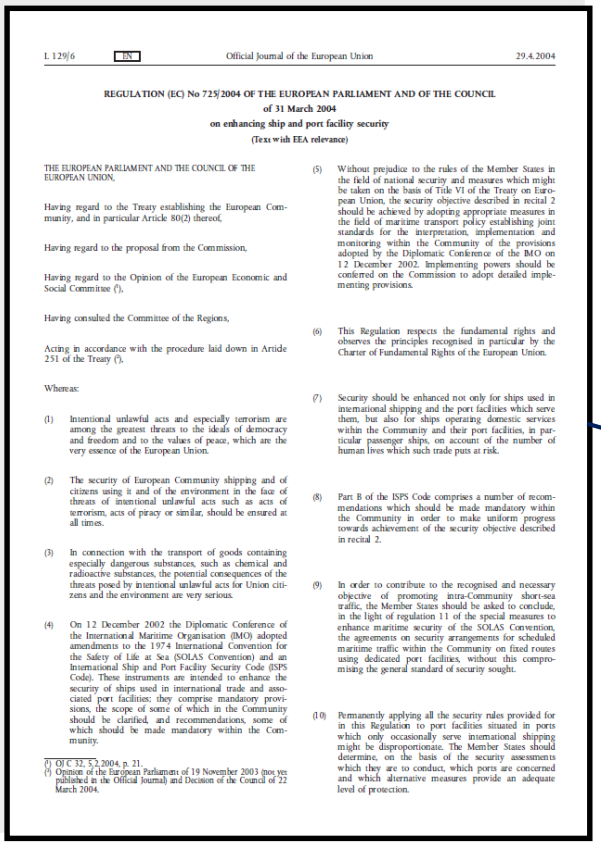
Regulatory framework

International legal framework applicable to the maritime domain

Things to remember

Regulatory framework

- Regulation (EU) No. 725/2004 on enhancing ship and port facility security, March 2004



L 129/6 EN Official Journal of the European Union 29.4.2004

REGULATION (EC) No 725/2004 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 31 March 2004
on enhancing ship and port facility security
(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 80(2) thereof,

Having regard to the proposal from the Commission,

Having regard to the Opinion of the European Economic and Social Committee (1),

Having consulted the Committee of the Regions,

Acting in accordance with the procedure laid down in Article 251 of the Treaty (2),

Whereas:

(1) Intentional unlawful acts and especially terrorism are among the greatest threats to the ideals of democracy and freedom and to the values of peace, which are the very essence of the European Union.

(2) The security of European Community shipping and of citizens using it and of the environment in the face of threats of intentional unlawful acts such as acts of terrorism, acts of piracy or similar, should be ensured at all times.

(3) In connection with the transport of goods containing especially dangerous substances, such as chemical and radioactive substances, the potential consequences of the threats posed by intentional unlawful acts for Union citizens and the environment are very serious.

(4) On 12 December 2002 the Diplomatic Conference of the International Maritime Organisation (IMO) adopted amendments to the 1974 International Convention for the Safety of Life at Sea (SOLAS Convention) and an International Ship and Port Facility Security Code (ISPS Code). These instruments are intended to enhance the security of ships used in international trade and associated port facilities; they comprise mandatory provisions, the scope of some of which in the Community should be clarified, and recommendations, some of which should be made mandatory within the Community.

(1) OJ C 32, 5.2.2004, p. 21.
(2) Opinion of the European Parliament of 19 November 2003 (not yet published in the Official Journal) and Decision of the Council of 22 March 2004.

(5) Without prejudice to the rules of the Member States in the field of national security and measures which might be taken on the basis of Title VI of the Treaty on European Union, the security objective described in recital 2 should be achieved by adopting appropriate measures in the field of maritime transport policy establishing joint standards for the interpretation, implementation and monitoring within the Community of the provisions adopted by the Diplomatic Conference of the IMO on 12 December 2002. Implementing powers should be conferred on the Commission to adopt detailed implementing provisions.

(6) This Regulation respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union.

(7) Security should be enhanced not only for ships used in international shipping and the port facilities which serve them, but also for ships operating domestic services within the Community and their port facilities, in particular passenger ships, on account of the number of human lives which such trade puts at risk.

(8) Part B of the ISPS Code comprises a number of recommendations which should be made mandatory within the Community in order to make uniform progress towards achievement of the security objective described in recital 2.

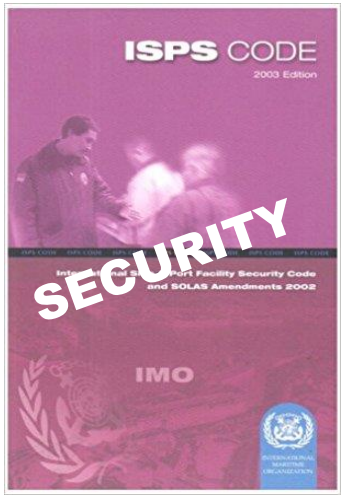
(9) In order to contribute to the recognised and necessary objective of promoting intra-Community short-sea traffic, the Member States should be asked to conclude, in the light of regulation 11 of the special measures to enhance maritime security of the SOLAS Convention, the agreements on security arrangements for scheduled maritime traffic within the Community on fixed routes using dedicated port facilities, without this compromising the general standard of security sought.

(10) Permanently applying all the security rules provided for in this Regulation to port facilities situated in ports which only occasionally serve international shipping might be disproportionate. The Member States should determine, on the basis of the security assessments which they are to conduct, which ports are concerned and which alternative measures provide an adequate level of protection.

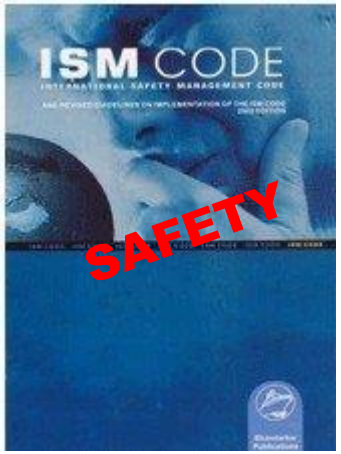
- **17 Recital**
- **15 Articles**
- **Annex I – SOLAS 74, as amended, Chapter XI-2**
- **Annex II – ISPS Code, Part A , mandatory**
- **Annex III – ISPS Code, Part B, mandatory for paragraphs listed in Article 3.5**

Regulatory framework

Are cyber risks taken into account in the existing management systems ?

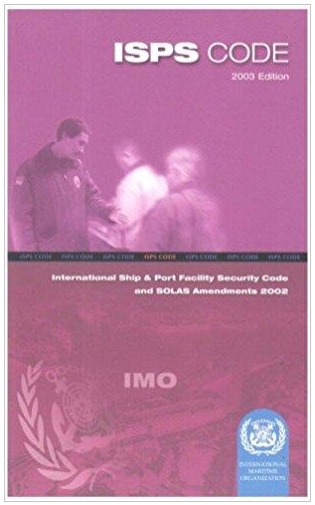


?



?

Regulatory framework



Ships…

8.4 The ship security assessment shall include an on-scene security survey and, at least, the following elements:

.1 identification of existing security measures, procedures and operations;

.2 identification and evaluation of key shipboard operations that it is important to protect;

.3 identification of possible threats to the key shipboard operations and the likelihood of their occurrence, in order to establish and prioritise security measures; and

.4 identification of weaknesses, including human factors, in the infrastructure, policies and procedures.

Port Facilities…

15.5 The port facility security assessment shall include, at least, the following elements:

.1 identification and evaluation of important assets and infrastructure it is important to protect;

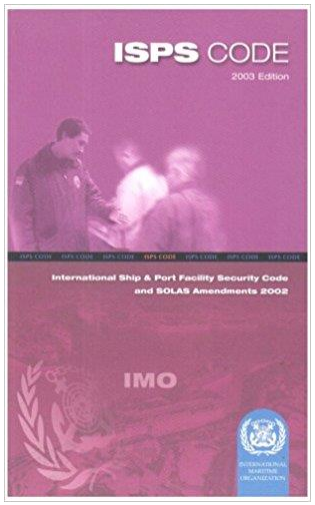
.2 identification of possible threats to the assets and infrastructure and the likelihood of their occurrence, in order to establish and prioritise security measures;

.3 identification, selection and prioritisation of countermeasures and procedural changes and their level of effectiveness in reducing vulnerability; and

.4 identification of weaknesses, including human factors, in the infrastructure, policies and procedures.

Part A of the ISPS Code - Risk Assessment

Regulatory framework



Ships…

8.3 A SSA should address the following elements on board or within the ship:

.1 physical security;

.2 structural integrity;

.3 personnel protection systems;

.4 procedural policies;

.5 radio and telecommunication systems, including computer systems and networks; and

.6 other areas that may, if damaged or used for illicit observation, pose a risk to persons, property, or operations on board the ship or within a port facility.

Port Facilities…

15.3 A PFSA should address the following elements within a port facility:

.1 physical security;

.2 structural integrity;

.3 personnel protection systems;

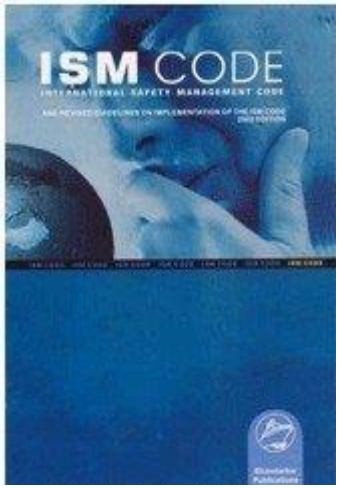
.4 procedural policies;

.5 radio and telecommunication systems, including computer systems and networks;

.6 relevant transportation infrastructure;

Part B of the ISPS Code - Risk Assessment

Regulatory framework



Part A – Implementation

1.2 Objectives

1.2.2 Safety management objectives of the Company should, inter alia: (…)

*1.2.2.2 " **assess** all **identified risk to its ships personnel** and the environment and establish appropriate safeguards; (…)"*

Regulatory framework

What is the answer of IMO to the question?

IMO INTERNATIONAL MARITIME ORGANIZATION

E

4 ALBERT EMBANKMENT
LONDON SE1 7SR
Telephone: +44 (0)20 7735 7611 Fax: +44 (0)20 7587 3210

MSC-FAL.1/Circ.3
5 July 2017

GUIDELINES ON MARITIME CYBER RISK MANAGEMENT

1 The Facilitation Committee, at its forty-first session (4 to 7 April 2017), and the Maritime Safety Committee, at its ninety-eighth session (7 to 16 June 2017), having considered the urgent need to raise awareness on cyber risk threats and vulnerabilities, approved the *Guidelines on maritime cyber risk management*, as set out in the annex.

2 The Guidelines provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyberthreats and vulnerabilities. The Guidelines also include functional elements that support effective cyber risk management.

3 Member Governments are invited to bring the contents of this circular to the attention of all stakeholders concerned.

4 This circular supersedes the interim guidelines contained in MSC.1/Circ.1526.

***

RESOLUTION MSC.428(98)
(adopted on 16 June 2017)

MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS

THE MARITIME SAFETY COMMITTEE,

RECOGNIZING the urgent need to raise awareness on cyber risk threats and vulnerabilities to support safe and secure shipping, which is operationally resilient to cyber risks,

RECOGNIZING ALSO that Administrations, classification societies, shipowners and ship operators, ship agents, equipment manufacturers, service providers, ports and port facilities, and all other maritime industry stakeholders should expedite work towards safeguarding shipping from current and emerging cyber threats and vulnerabilities,

BEARING IN MIND MSC-FAL.1/Circ.3 on *Guidelines on maritime cyber risk management* approved by the Facilitation Committee, at its forty-first session (4 to 7 April 2017), and by the Maritime Safety Committee, at its ninety-eighth session (7 to 16 June 2017), which provides high-level recommendations for maritime cyber risk management that can be incorporated into existing risk management processes and are complementary to the safety and security management practices established by this Organization,

RECALLING resolution A.741(18) by which the Assembly adopted the International Management Code for the Safe Operation of Ships and for Pollution Prevention (International Safety Management (ISM) Code) and recognized, inter alia, the need for appropriate organization of management to enable it to respond to the need of those on board ships to achieve and maintain high standards of safety and environmental protection,

NOTING the objectives of the ISM Code which include, inter alia, the provision of safe practices in ship operation and a safe working environment, the assessment of all identified risks to ships, personnel and the environment, the establishment of appropriate safeguards, and the continuous improvement of safety management skills of personnel ashore and aboard ships,

1 AFFIRMS that an approved safety management system should take into account cyber risk management in accordance with the objectives and functional requirements of the ISM Code;

2 ENCOURAGES Administrations to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021;

3 ACKNOWLEDGES the necessary precautions that could be needed to preserve the confidentiality of certain aspects of cyber risk management;

4 REQUESTS Member States to bring this resolution to the attention of all stakeholders.

***

EMSA

Now …

What should I do?

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

EMSA
European Maritime Safety Agency