Maritime Cybersecurity

Luca Gargano

Project Officer for Maritime Security

Lisbon / 21-1-2020

EMSA

Hacker community

Black Hat Hacker

Is a person who attempts to find computer security vulnerabilities and exploit them for personal financial gain or other malicious reason

White Hat Hacker

Is a computer specialist who breaks into protected system and networks to test and assess their security

Grey Hat Hacker

Carries out cyber attacks but only for ethical reasons (i.e. free information access, free access to network, distrust the Authorities etc.)

Active Hacking Groups

- *Anonymous*
- *Syrian Electronic Army*
- *Chaos Computer Club*
- *etc.*

Hacker’ s tools

Password cracking

Packets analyser (sniffing)

Cloner of website (water holing)

Network scanning

to exploit vulnerabilities

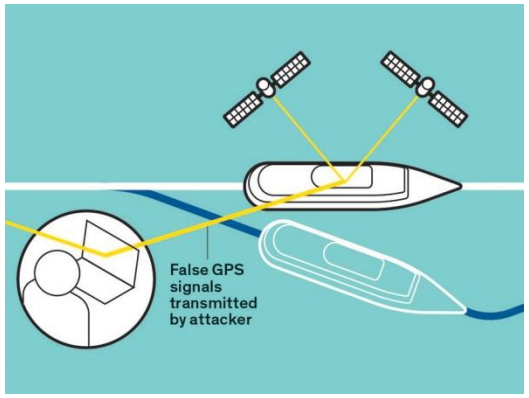
All downloadable
by Internet for free

Cyber terminology

RANSOMWARE: malware demanding for a ransom be paid in exchange for the infected party not suffering some harm

BOTNET: computer zombies controlled by a hacker without the owners' knowledge

PHISHING: Trying to get confidential information



SPOOFING: sending false information to gain illegal entry into a security system

Did it happen?

- **January 2020** hackers used Ryuk ransomware to infiltrate computer networks of a US port facility, the incident resulted in the disruption of “the entire corporate IT network, causing an outage of roughly 30 hours.

- **September 2018.** The port of Barcelona was victim of a cyber attack

- **June 2017.** The ‘NotPetya’ malware attack struck organisations in more than 60 countries worldwide, including many prominent organisations within the maritime transport sector;

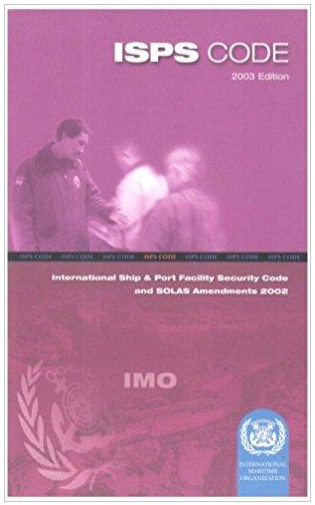
- **June 2017** . A big container shipping company was been hacked. It costed as much as $300 million in lost revenue. It was a ransomware attack that prevented people from accessing their data unless they paid $300 in bitcoin;

- **Between 2011-2013** Port of Antwerp , organized criminals breached the port IT system, facilitating heroin and cocaine smuggling;

- **April 2007**. Estonia -the entire country was cyber attacked. Banks, ministries, newspapers, broadcasters. Massive waves of spam were sent by botnets and huge amounts of automated online requests swamped servers.

“It was a great security test. We just don't know who to send the bill to“
Tanel Sepp, Estonia cyber security official at the defence ministry.

Regulatory context



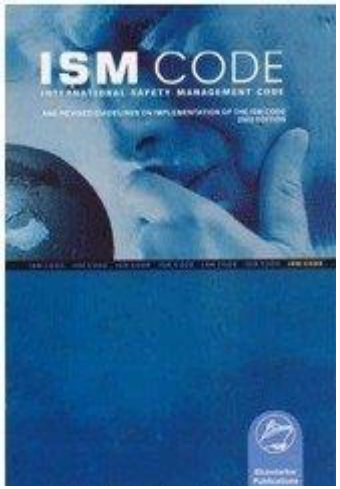
Part A/8.3.4 – A/15.5.2

….SSA/PFSA shall include identification of possible threats …… and the likelihood of their occurrence…..

Part B/8.3.5 – B/ 15.3.5

….SSA/PFSA should address the following elements ……:…… radio and telecommunications system, including computer systems and networks…..

MANDATORY



Part A/1.2.2.2

Company should …. assess all identified risks to its ships, personnel and the environment and establish appropriate safeguards……

MANDATORY

Resolution MSC. 428 (98)

ANNEX 10

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

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;

confidentiality of certain aspects of cyber risk management;

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

Why ISM?

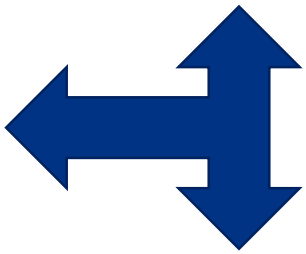
Identify: define personnel roles and responsibilities and systems, assets, data and capabilities that, when disrupted, pose risks to ship operations

Protect: Implement risk control processes and measures to protect against a cyber event and ensure continuity of shipping operations

Detect: develop and implement activities necessary to detect a cyber event in a timely manner

A cyber risk management should

prevention



reaction

Recover : Identify measures to back-up and restore cyber systems necessary for shipping operations

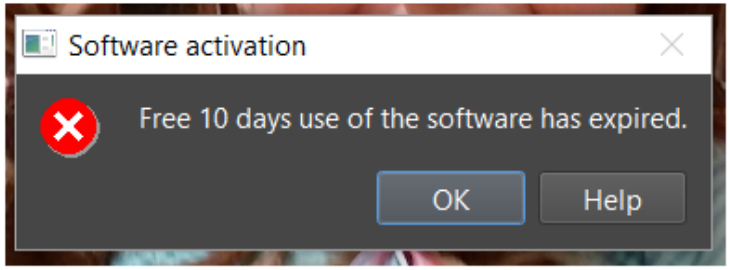
Respond : Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations

Why ISM?

Malicious actions
(e.g. hacking or introduction of malware)

Intentional

Benign actions
(e.g. software maintenance or users permissions)



Unintentional

Why ISM?

ISPS scope

- Passenger ships, including high-speed passenger craft;
- Cargo ships, including high-speed craft, of 500 gross tonnage and upwards; and
- Mobile offshore drilling units.

Engaged on international voyages.

SSP must be approved

ISM scope

like ISPS and ...

- cargo ships (more than 500 gt) and passenger ships engaged exclusively on domestic voyages, regardless of their flag.

SMS manual no need approval

Assets on board to protect

- Bridge systems
- Cargo handling
- Propulsion and machinery management
- Access control systems
- Passenger serving and management system
- Passenger facing public networks
- Administrative and crew welfare system
- Communication system

ISPS B section 8.3

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;

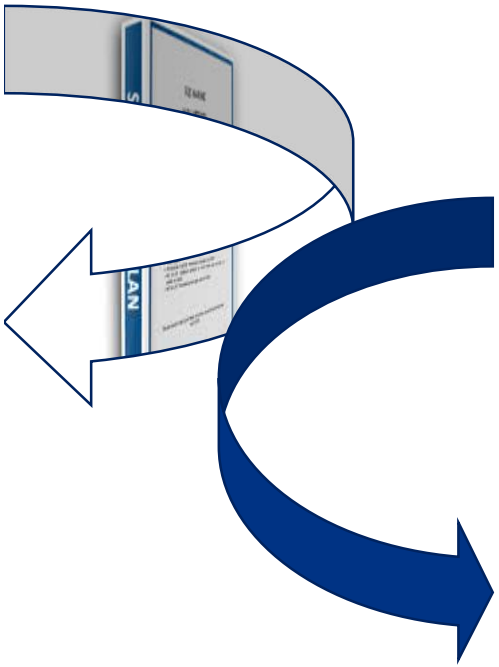
.4 procedural policies;

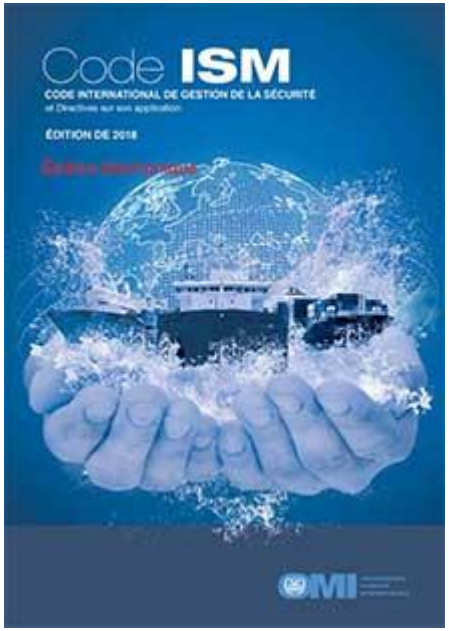
.5 radio and telecommunication systems, including computer systems and networks; and

.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.

MANDATORY

Cross-reference





Provided that…….

SSO/CSO are aware of (in terms of responsability)

Same standard of confidentiality

Same standard of language (EN, FR or SP)

Must be approved

Port facility cybersecurity

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;

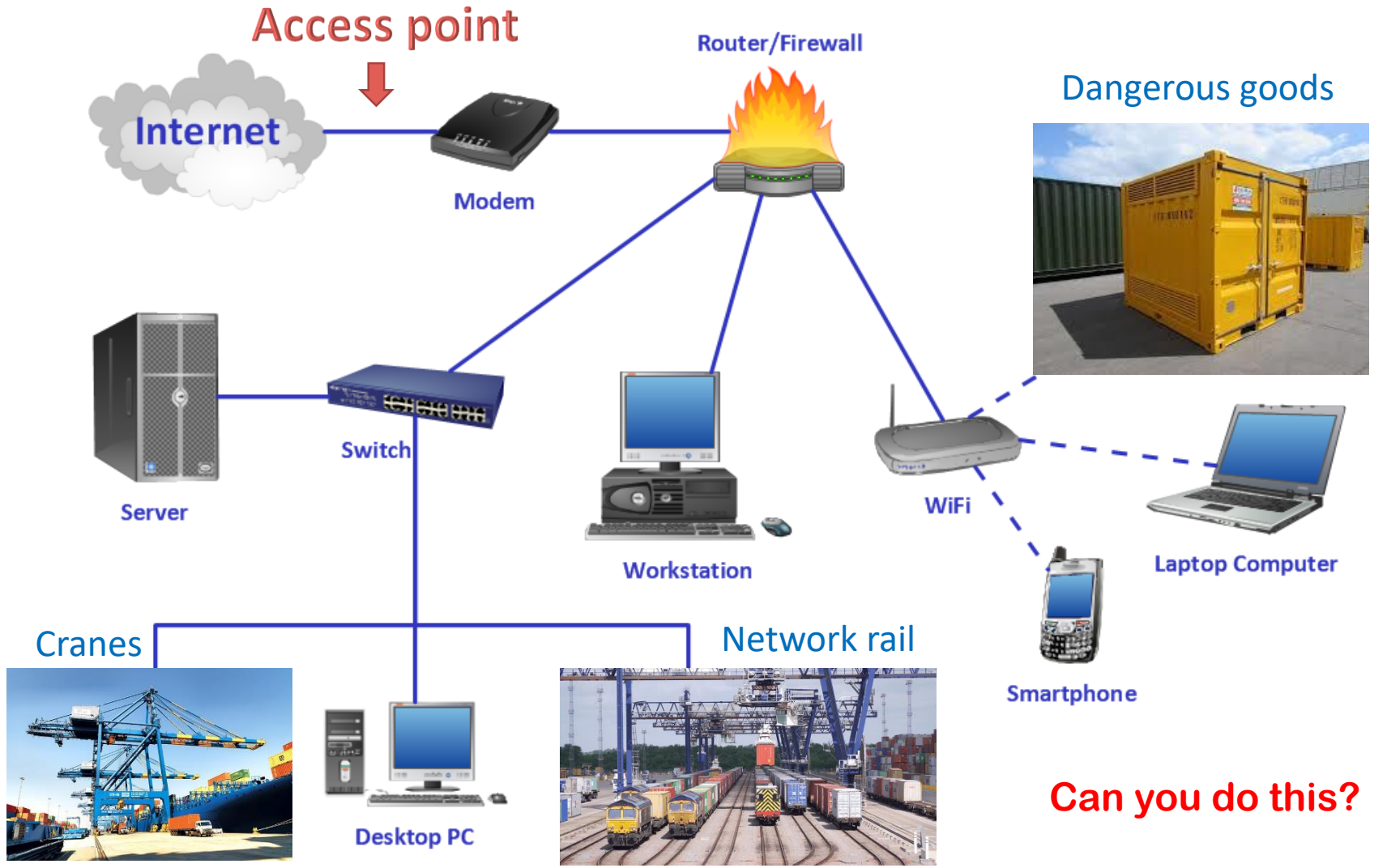
.6 relevant transportation infrastructure;

.7 utilities; and

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

MANDATORY

Port facility cybersecurity



Port facility cybersecurity

15.4 Those involved in a PFSA should be able to draw upon expert assistance in relation to:

.1 knowledge of current security threats and patterns;

.2 recognition and detection of weapons, dangerous substances and devices;

.3 recognition, on a non-discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten security;

.4 techniques used to circumvent security measures;

.5 methods used to cause a security incident;

.6 effects of explosives on structures and port facility services;

.7 port facility security;

.8 port business practices;

.9 contingency planning, emergency preparedness and response;

.10 physical security measures, e.g. fences;

.11 radio and telecommunications systems, including computer systems and networks;

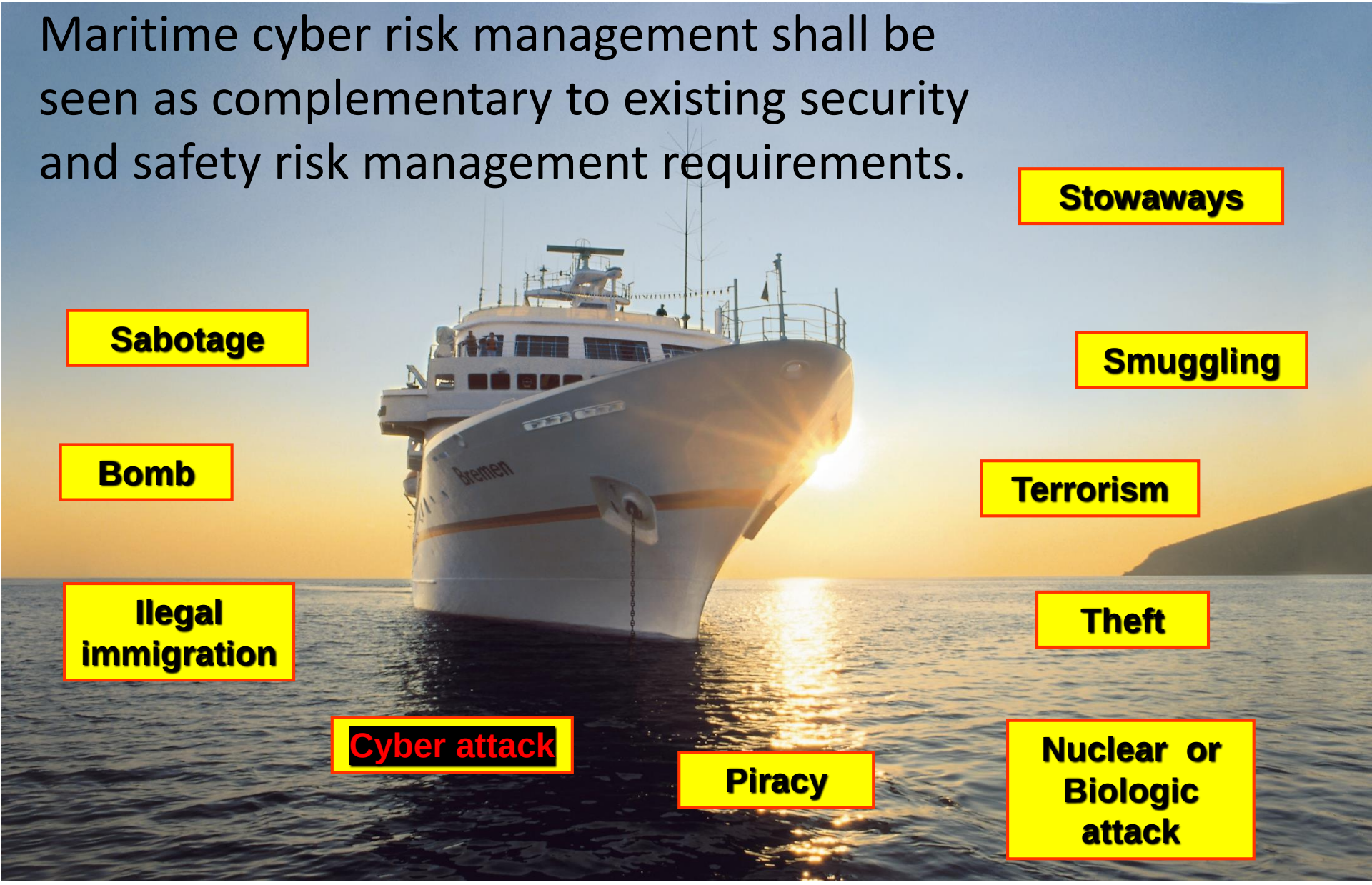
.12 transport and civil engineering; and

.13 ship and port operations.

MANDATORY

Conclusion

Maritime cyber risk management shall be seen as complementary to existing security and safety risk management requirements.



Maritime cybersecurity

twitter.com/emsa_lisbon

facebook.com/emsa.lisbon

EMSA

European Maritime Safety Agency