High Level Conference on Cyber Security in Civil Aviation

Panel 2: Cyber in the multimodal transport context

Mr. Markku Mylly

Executive Director of EMSA

EMSA

Content

- Cyber Risks in Maritime Community
- EU Cyber Security Strategy
- EMSA and Maritime Cyber Security

Cyber Risks in Maritime Community

Definition

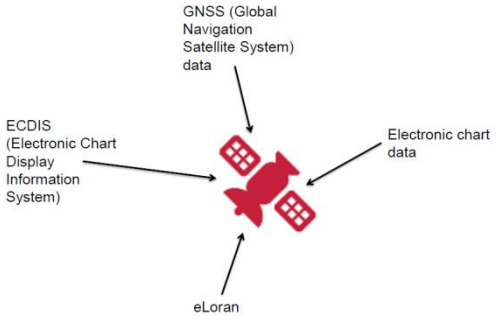
[IMO MSC.1/Circ.1526, 1 June 2016]

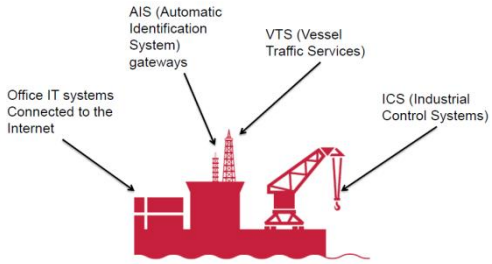
Maritime cyber risk *refers to a* ***measure*** *of the extent to which a technology asset could be threatened by a potential circumstance or event, which* ***may result*** *in shipping-related operational,* ***safety or security failures*** *as a consequence of information or systems being corrupted, lost or compromised.*

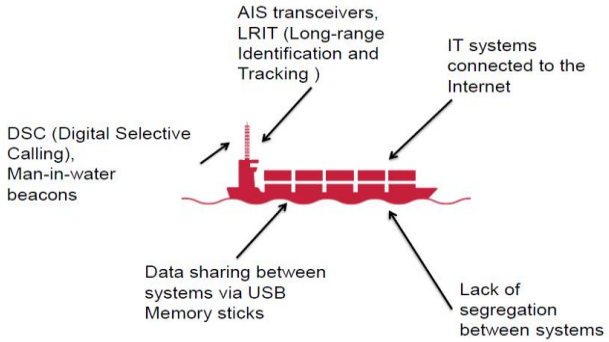
Cyber Risks in Maritime Community

The four major Critical Information Assets identified within the Maritime Sector are:

- **Critical digital traffic/communication systems;**
- **Critical information/databases;**
- **Critical infrastructures;**
- **Automated terminal and vessel systems.**







* Images source: Brendan Saunders – Maritime Lead, Transport Cyber Security Practice

Cyber Risks in Maritime Community

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

- **Losing** information sovereignty on ship position and distance to ports/coast guard/special vessels;
- **Disruption** of communication, traffic and navigational systems;
- **Distortion** of (e-)navigational data leading to accidents, hijackings and environmental pollution;
- **Concealing** ship movements or cargo data by cracking related systems/ databases;
- **Distortion** of critical infrastructure architecture (i.e. port automated cargo systems or off-shore energy producing facilities).

Source BIMCO guidelines

EMSA

Cyber Risks in Maritime Community

How ships could be cyber-hijacked

The increasing reliance on automation in the maritime industry means key components, including navigational systems, can be hacked.

HOW SHIPS NAVIGATE

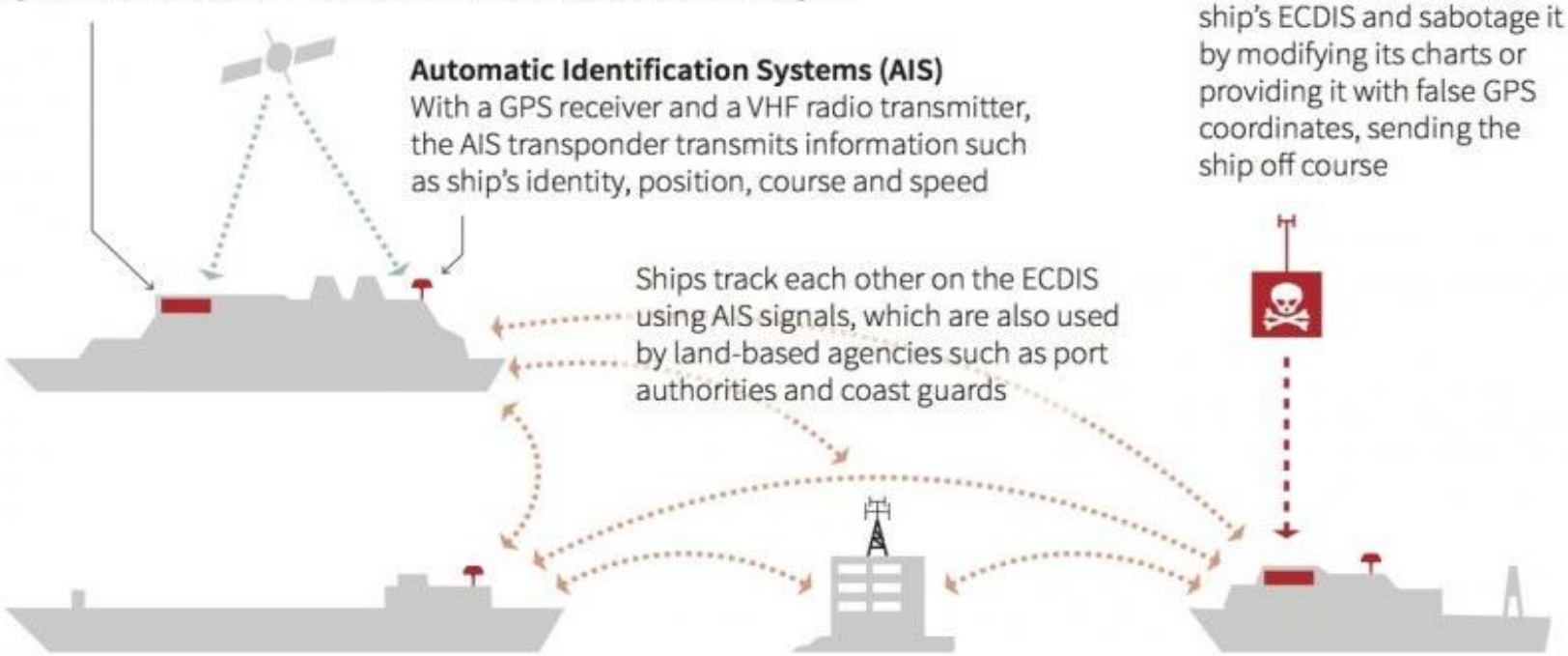
Electronic Chart Display and Information Systems (ECDIS)
Using GPS* and electronic navigational charts, the ECDIS displays digital maps and other information which the crew use to navigate

Automatic Identification Systems (AIS)
With a GPS receiver and a VHF radio transmitter, the AIS transponder transmits information such as ship's identity, position, course and speed

Ships track each other on the ECDIS using AIS signals, which are also used by land-based agencies such as port authorities and coast guards

HOW HACKERS COULD ATTACK

With a VHF radio transmitter, hackers could hack into a ship's ECDIS and sabotage it by modifying its charts or providing it with false GPS coordinates, sending the ship off course



Sources: Reuters; International Maritime Organization; Marine Traffic

* Global Positioning System

EMSA

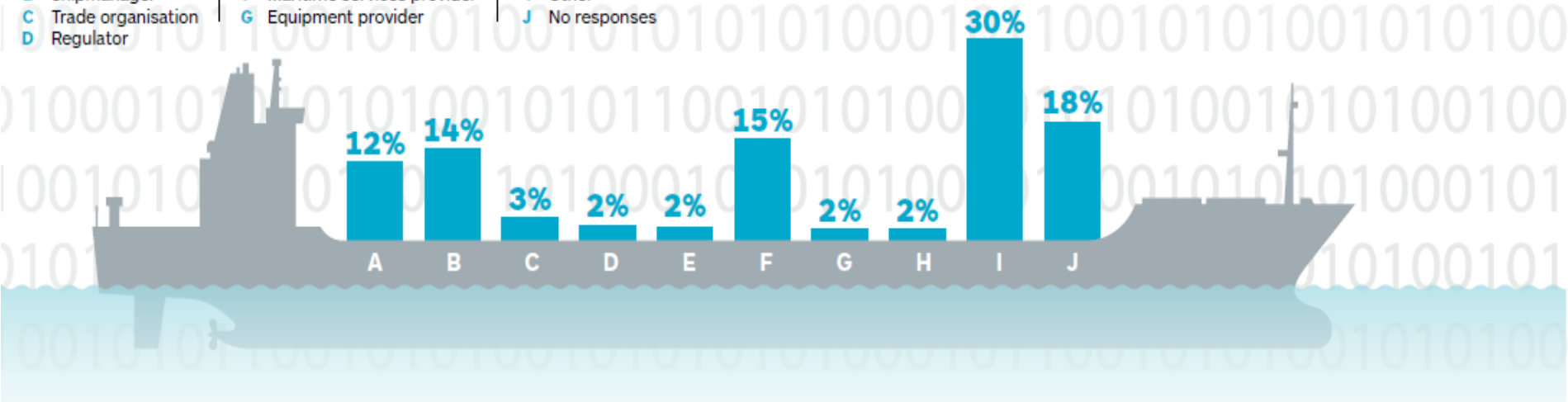
Cyber Risks in Maritime Community

Phenomenon in numbers

IHS Markit and BIMCO launched the maritime cyber security survey on 22 July. The survey, which ran for four weeks, was promoted on social media and via email. More than 300 industry players responded. Of the 300 respondents, 65 had been a victim of a cyber attack. Here are some of the highlights of the insights gathered from respondents to the maritime cyber security survey.

Who responded?

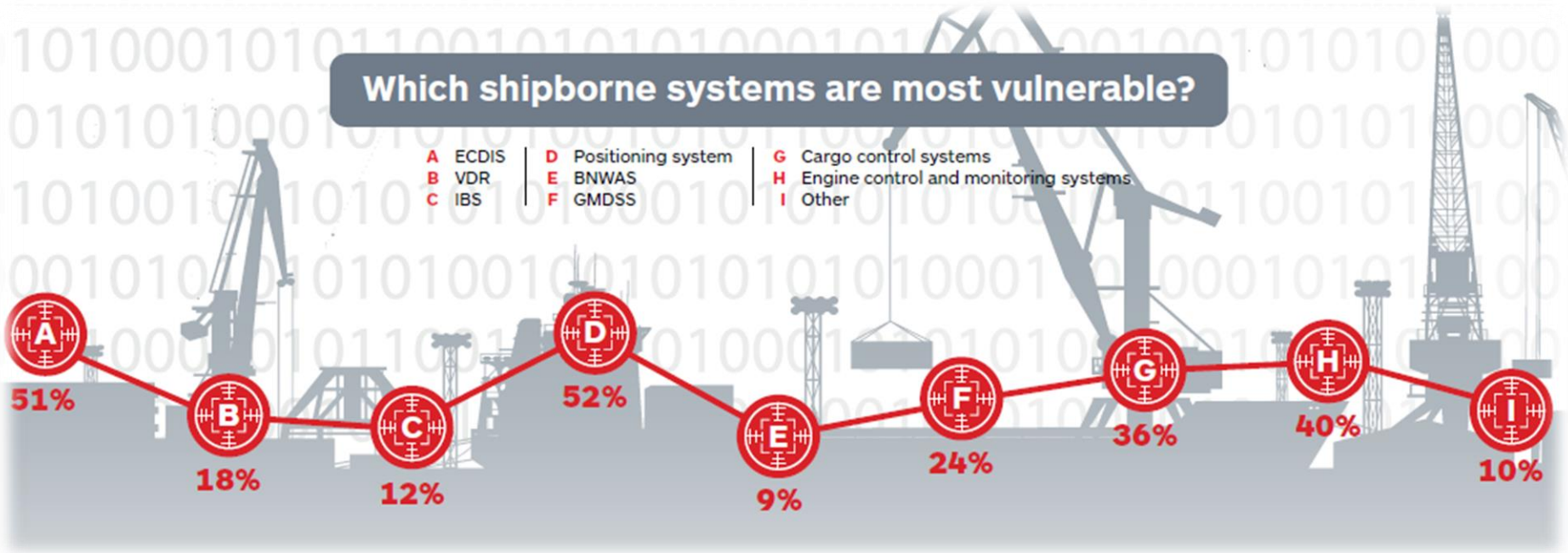
- A Shipowner
- B Shipmanager
- C Trade organisation
- D Regulator
- E Port authority
- F Maritime services provider
- G Equipment provider
- H Shipyard
- I Other
- J No responses



* source: BIMCO. Data collected are updated to July 2016

Cyber Risks in Maritime Community

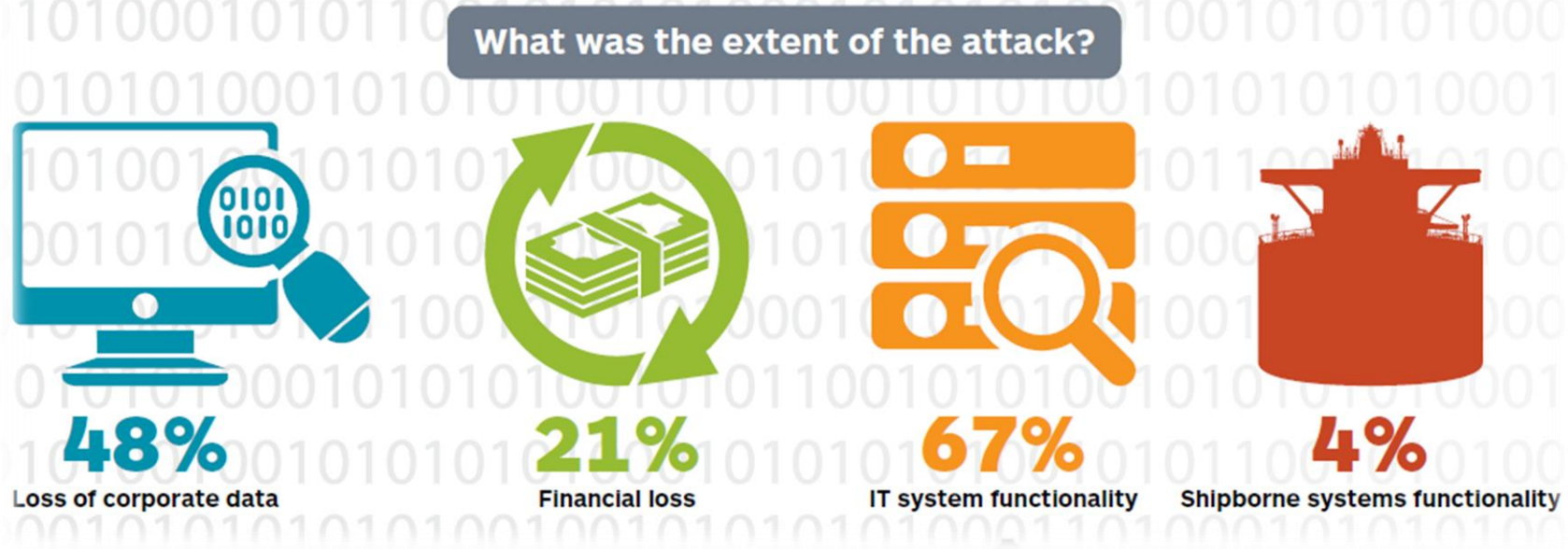
Phenomenon in numbers



* source: BIMCO. Data collected are updated to July 2016

Cyber Risks in Maritime Community

Phenomenon in numbers



* source: BIMCO. Data collected are updated to July 2016

The potential impact of marine cyber attacks includes potential revenue loss, environmental damage and loss of life

Cyber Security Culture

Cyber security should be considered at all levels of the company, from senior management ashore to crew on board, as an inherent part of the safety and **security culture** necessary for safe and efficient ship operations.

Training and awareness programs should be tailored to the appropriate levels to enhance organization's cyber security posture.

Creating a Cybersecurity Culture

EU Cyber Security Strategy

DIRECTIVE (EU) 2016/1148 of 6 July 2016

on measures for a high common level of security of network and information systems across the Union (**NIS**)

Requirements:

- Member States to adopt a **national strategy on the security of network**
- To create a **Cooperation Group**
- To create **computer security incident response teams**
- To establish **security and notification requirements**
- Member States to designate **national competent authorities**, **single points of contact**

Deadlines

9 May 2018 – transposition

9 November 2018 - identify the operators of essential services

EMSA

EMSA and maritime cyber security

At institutional level…

EMSA
European Maritime Safety Agency

IMO

European Commission

MARSEC Committee

At operational level…

- Workshop in maritime cyber attack prevention
- Distance Learning Programme (DLP)
- Cyber security reporting/information sharing

EUROPEAN COAST GUARD FUNCTIONS FORUM
German Chairmanship 2017/2018
BUNDESPOLIZEI
ZOLL

Cyber security next steps …

Relevant Elements

- Cyber Security Awareness uneven across the maritime transportation system;
- Successful cyber attacks could have large scale impact on maritime sector;
- Maritime regulations and policies do not adequately cover Cyber Security in the same way as other physical aspects of security and safety;
- Fragmented maritime governance (i.e. international, European, national).

Considering the above elements:

- Analysis of the threats in the cyber environment and how cyber systems support maritime transportation operations should be carried out;
- Assessment of the potential vulnerabilities associated with these cyber systems;
- Regulatory or voluntary requirements should be included in safety and security management systems;
- Best practices and tools to enhance an organization's cyber security posture should be encouraged.

twitter.com/emsa_lisbon

facebook.com/emsa.lisbon

EMSA

European Maritime Safety Agency