

CYBER SECURITY :

Reinforcement of **Cyber Security** Through
Revising **ISPS CODE**



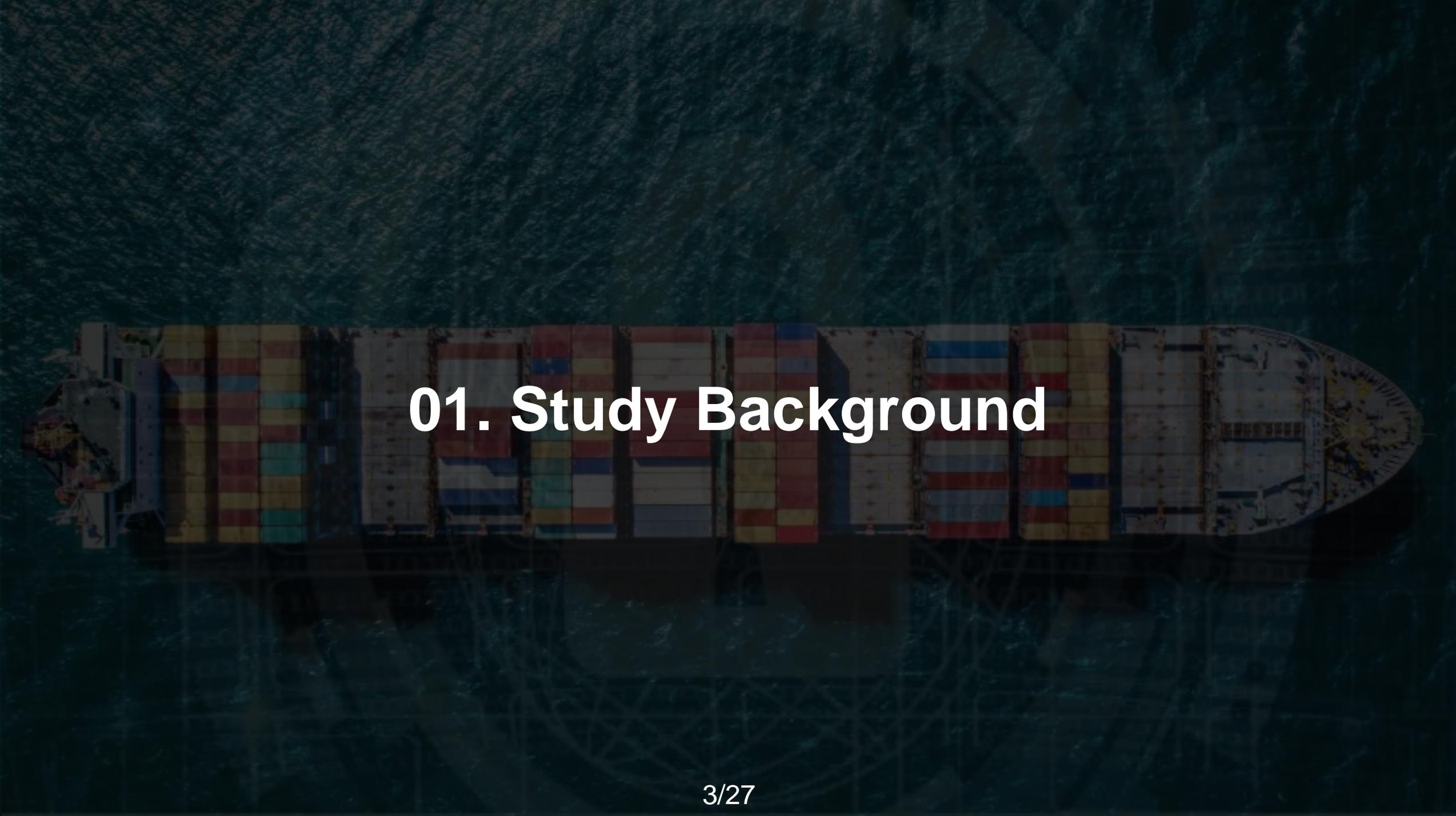
Team The Sheriff

INDEX

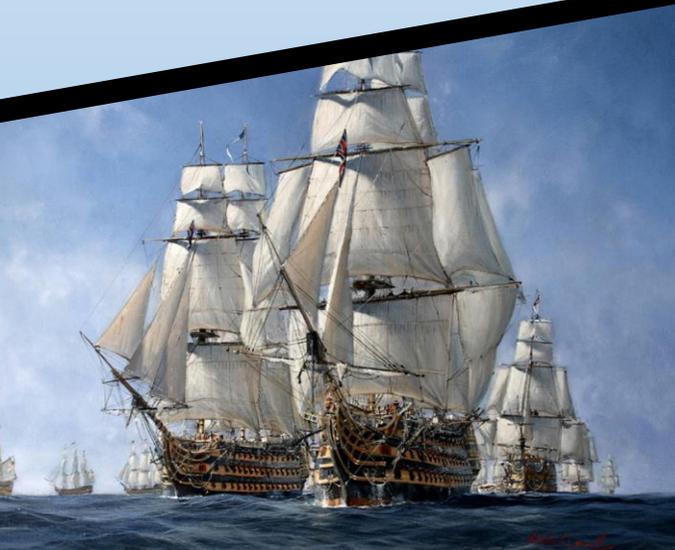
01. Study Background

**02. Vulnerabilities &
In - depth Analysis of the Problem**

03. Conclusion & Solution

An aerial photograph of a large container ship sailing on the ocean. The ship is oriented vertically in the frame, with its bow at the top. The deck is densely packed with multi-colored shipping containers in shades of red, yellow, blue, and white. The ship's superstructure, including the bridge and various masts, is visible at the top. The water is a deep blue with visible ripples and waves. The overall image has a dark, slightly desaturated aesthetic.

01. Study Background

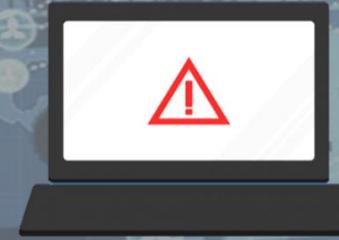


69%

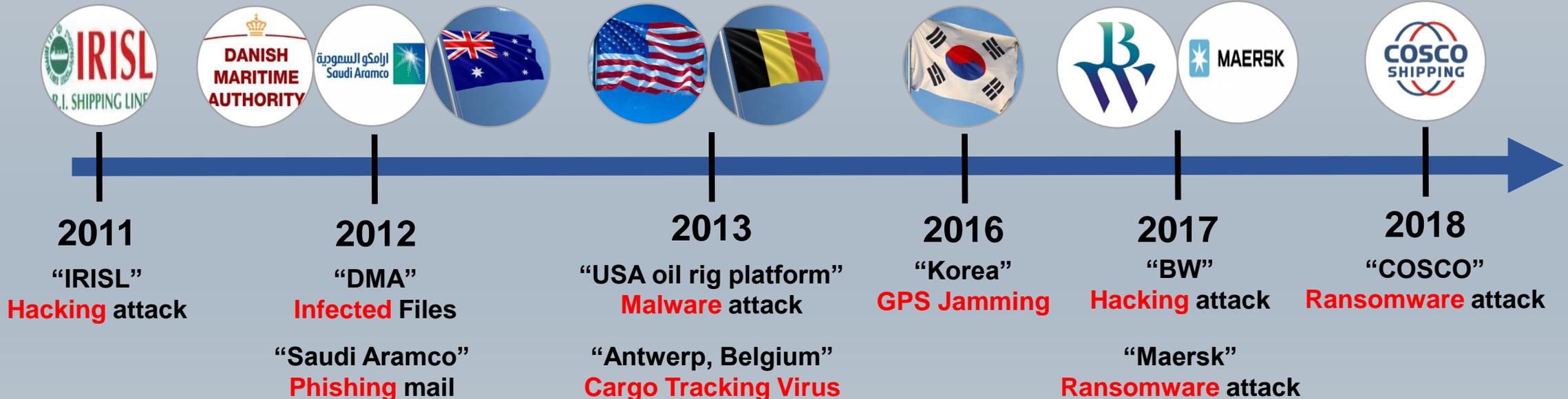
In 2017, A Survey showed that **69%** of shipping company had been subjected to **cyber attacks**.

Danish Shipping Survey

Type of Threat



- Malware
- Social engineering
- Water holing
- Scanning
- Ransomware
- Dos
- Brute force
- Spoofing
- Sniffing
- Homepage Modulation





Ship Inspection Report (SIRE) Programme

Vessel Inspection Questionnaires for Oil
Tankers, Combination Carriers, Shuttle Tankers,
Chemical Tankers and Gas Tankers, Seventh
Edition (VIQ 7)

22 February 2019

Oil Companies International Marine Forum

Chapter 7 Maritime Security.

Notes: The International Ship and Port Facility Security Code came into force on 1st July 2004. Inspectors should not request to sight sensitive material but verbally confirm with the Master/SSO, that procedures or records are available or maintained.

Cyber Security

7.14 Are *Cyber Security Policy* and Procedures part of the Safety Management System and is there *a Cyber Response Plan onboard?*

7.15 Are the crew *aware* of the company policy on the control of physical access to all shipboard IT/OT system?

7.16 Does the company *have a policy or guidance* on the use of personal devices onboard?

7.17 Is Cyber Security awareness actively promoted by the company and onboard?

BIMCO

- Vulnerability and Relationship with Stakeholders
- Identify Threats and Risk Assessment
- Protection Measures
- Contingency Plans and Recovery Plan

NIST

- The Cyber Security Framework Components :
Identify Protect Detect Respond Recover
- Present about How the Framework can be used

KR

- Risk Assessment (Vulnerability Identification and Risk Analysis)
- Risk Management (Education and Technical activity)
- Response Plan and Accident analysis
- Recovery Plan



Strategic Plan for the Organization for six- year period 2018 to 2023 (Resolution A .1110(30))

SD 5: Enhance global facilitation and security of international trade

26 Shipping moves around 80%¹ of world trade, making it an integral part of the global economy and supply chain. The prevention of disruption to international shipping is therefore in the interest of all. Continued effort is needed to ensure that ships move from port to port without undue delay arising from arrival and departure formalities, to provide for safe transportation and effective facilitation of international trade, and to ensure that appropriate security measures are in place on all international voyages.

27 Threats such as piracy and armed robbery against ships could disrupt international trade, threaten lives, and increase the burden on maritime transport. Furthermore, to ensure the security of the maritime transport network, including vital shipping lanes, IMO will continue to raise awareness of IMO measures for security and to encourage a cooperative approach among

28 Shipping operations are increasingly dependent on electronics and digital technologies and as such are exposed to cyber risks. The Organization will continue to monitor the issue and encourage a cooperative approach among Member States and stakeholders.

29 Electronic transmission of relevant information, such as, but not limited to, documents and certificates, simplifies communications between ships, ports and authorities and reduces the administrative burden for those on board and ashore. The challenge is to ensure that information is transmitted securely in a universally accepted form and is verifiable. To take full advantage of the electronic exchange of information, closer cooperation is needed between authorities and the industry at the national and, in certain instances, regional levels.

30 To achieve this, IMO will seek further international consensus on reducing, simplifying and standardizing the information required. It will develop global solutions that reduce the burdens by facilitating electronic information exchange and that balance the needs of authorities ashore with the interests of the shipping industry.

Guidelines on Maritime Cyber Risk Management



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 management to safeguard shipping from 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 su **These Guidelines are recommendatory.**



Resolution MSC 428(98)

Cyber Security Management



ISM code

Vulnerabilities

Different Company and Flag States have different responses

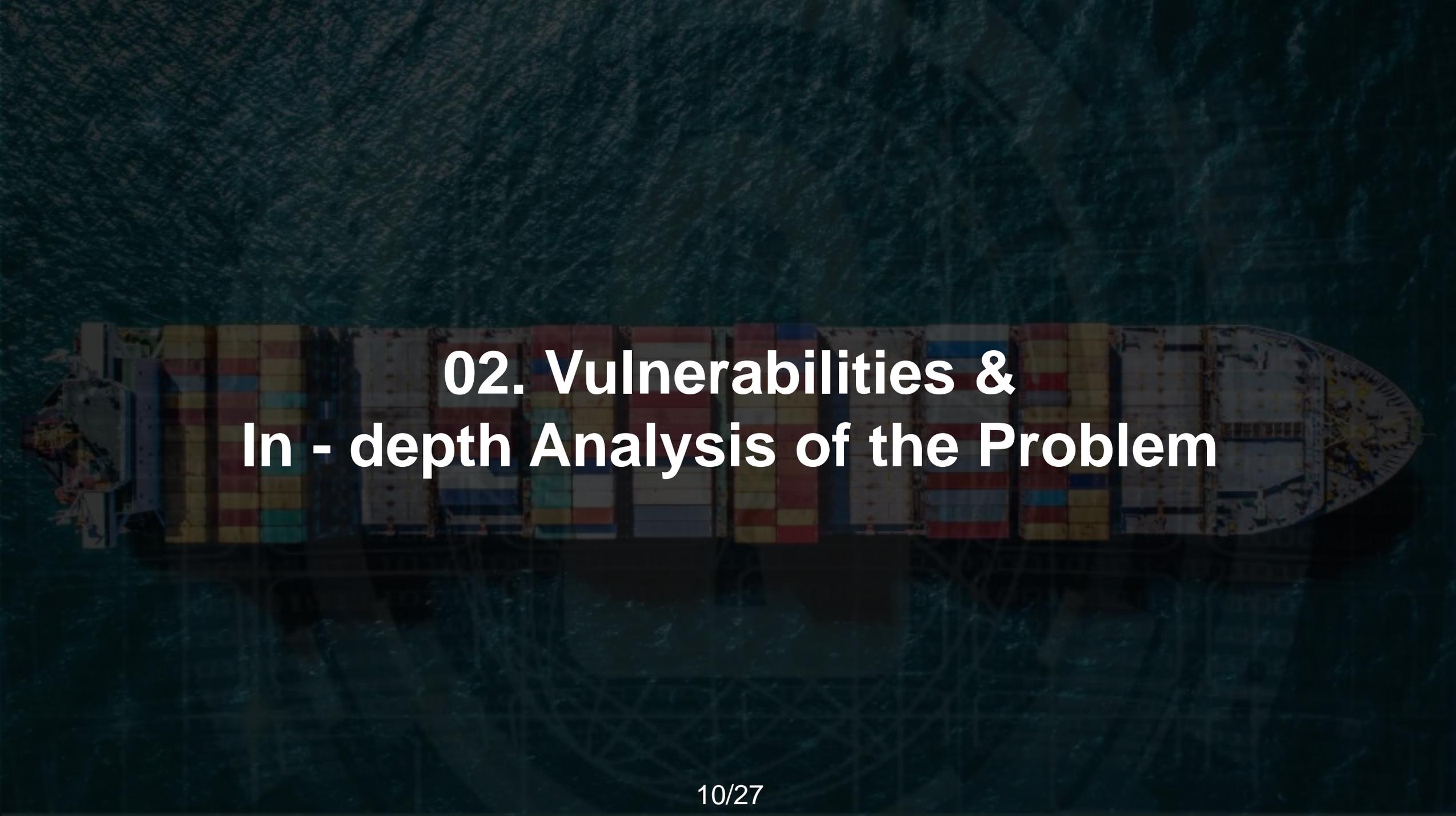


The Standards are Vague and Ineffective

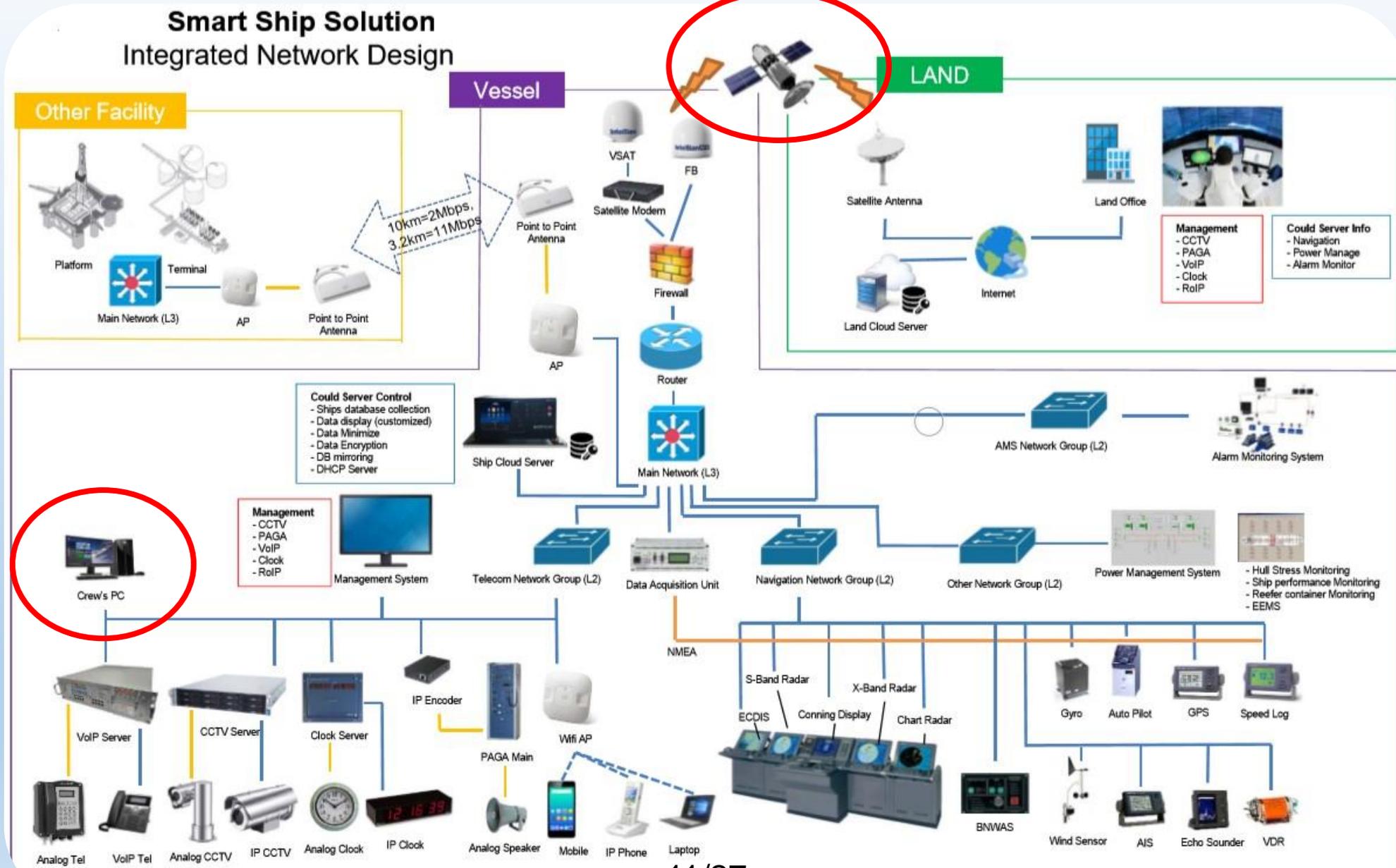
Cyber Security Management

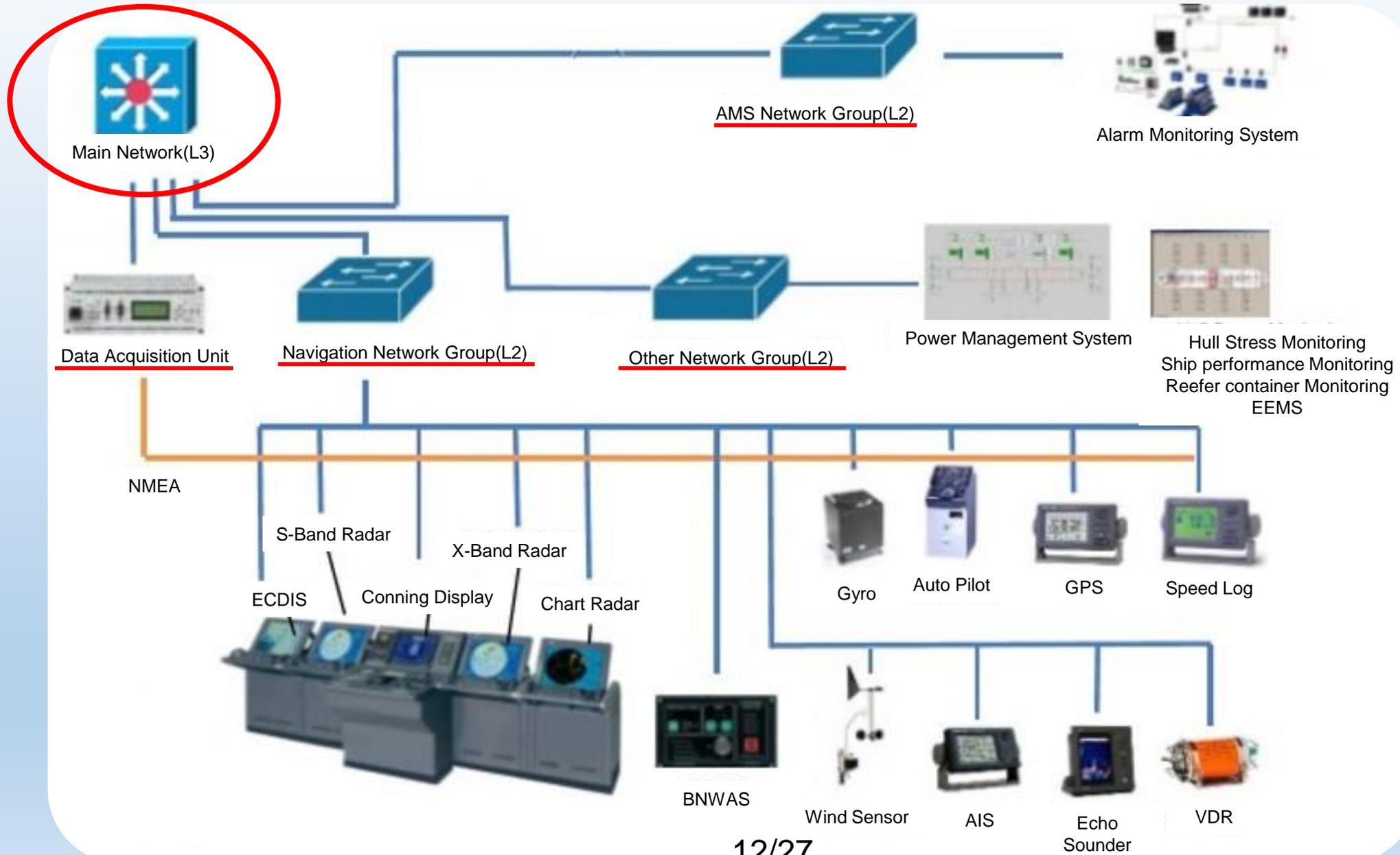


SOLAS ISPS code ?

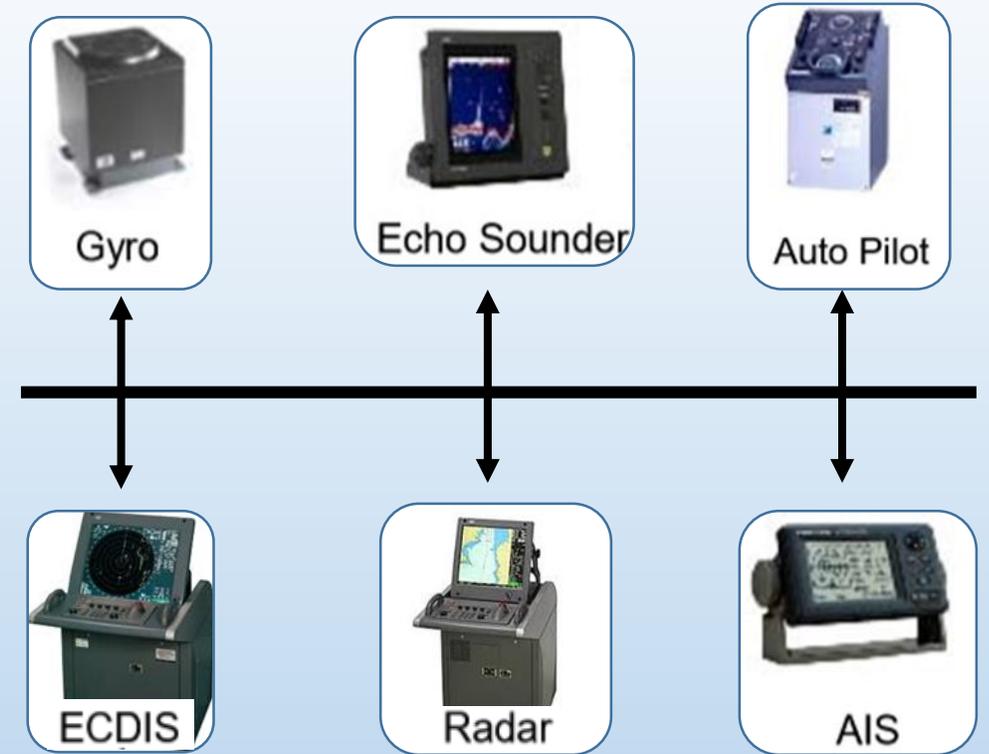
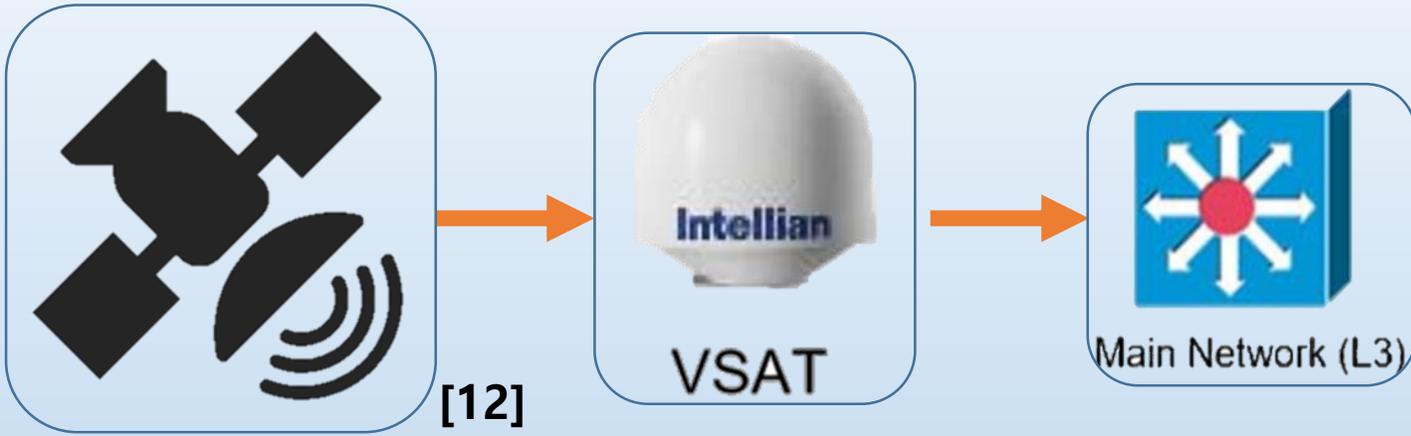
An aerial photograph of a large container ship sailing on the open ocean. The ship is viewed from above, showing its deck and the numerous colorful shipping containers stacked on it. The water is a deep blue, and the ship's wake is visible. The text is overlaid on the center of the image.

02. Vulnerabilities & In - depth Analysis of the Problem





1. Entry via Satellite



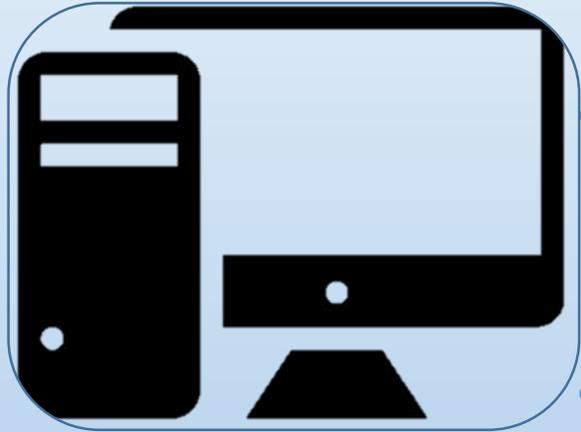
2. Entry via USB



IT : Information Technology



Computer
Personal phone



Internet Browser
USB device

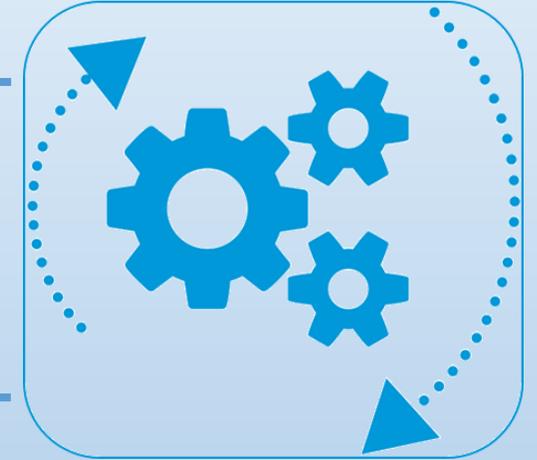


Information Technology is the systems used for office work, email, and web-browsing

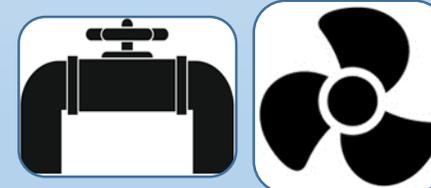


Centrifugal Pump
Generator

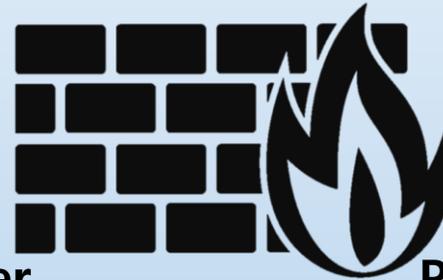
OT : Operational Technology



Pipe
Rudder



Operational Technology is the systems which are used to operate the ship

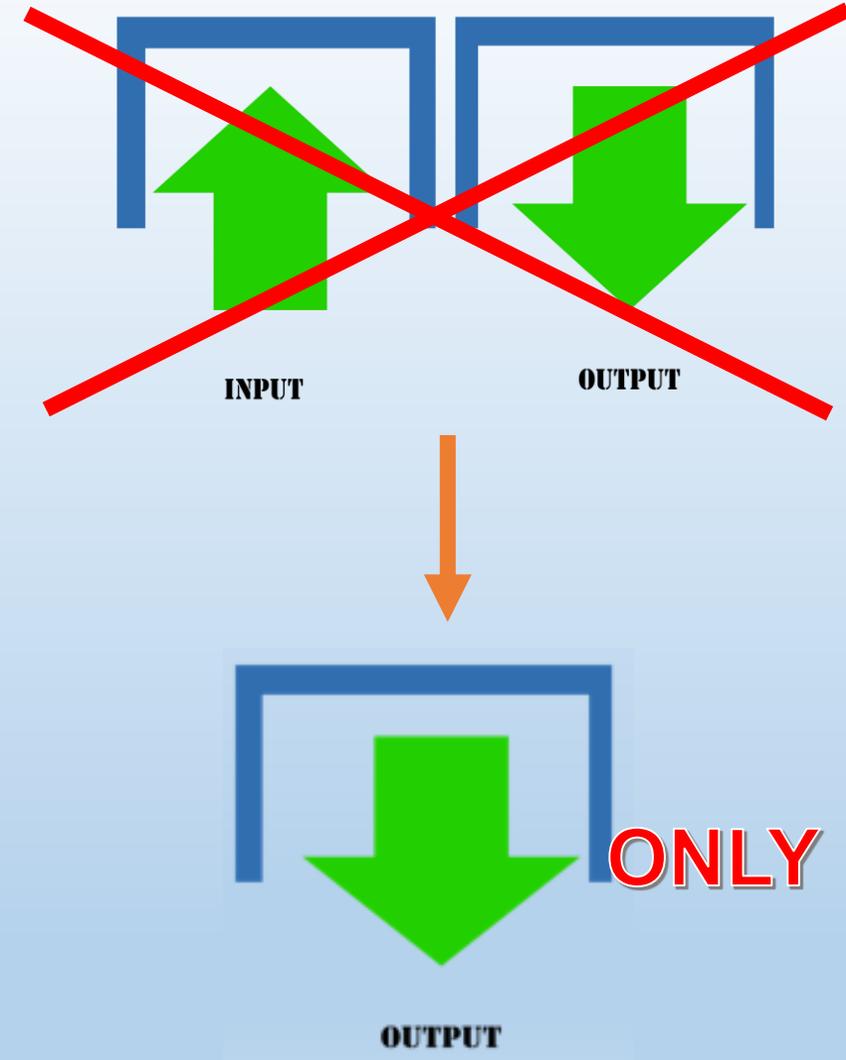


Firewall Non-existent

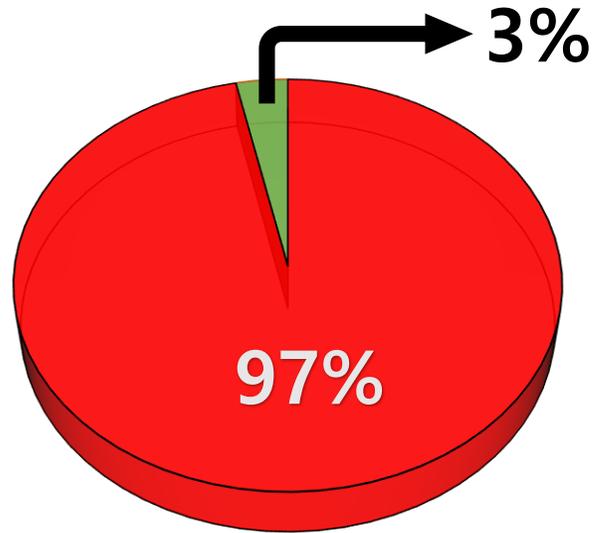
Classification by Importance of Equipment

LEVEL 1	Weather Telefax, Course Recorder
LEVEL 2	Voyage Data Recorder, Incinerator, Boiler, Ship's Clock
LEVEL 3	Echo Sounder, Car Deck Fan, G.S. Pump
LEVEL 4	GPS, Bow Thruster, Ballast System
<u>LEVEL 5</u>	<u>ECDIS, AIS, Engine, Radar, Propeller, Autopilot</u>

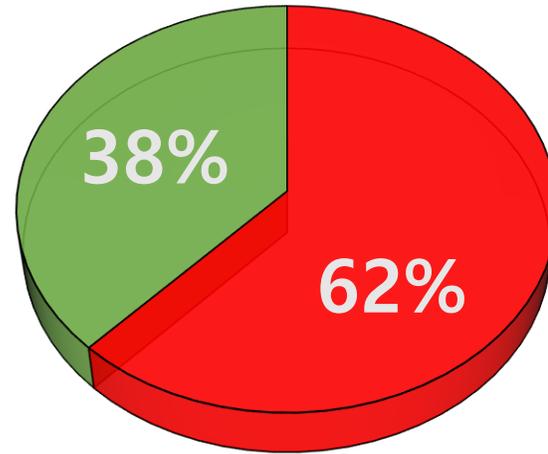
→ We believe the risks in 'input' and someone to manage these risks



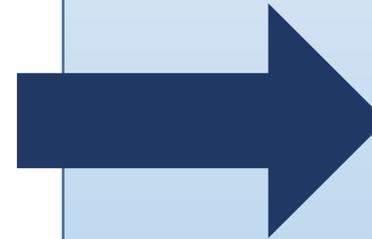
Response of 60 Surveyors



→ Over 97% of crew haven't received training for cyber security



→ 62% of crew didn't feel confident in handling a virus

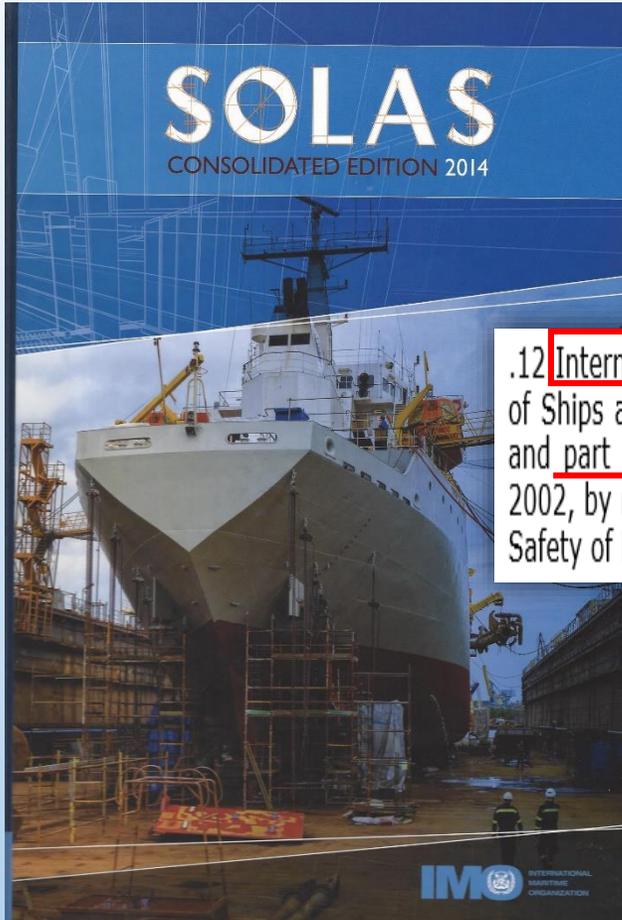


Calls for urgent measures to be taken



An aerial photograph of a large container ship sailing on the ocean. The ship is viewed from above, showing its deck and the stacks of colorful shipping containers. The water is a deep blue-green color. The ship is oriented horizontally across the frame.

03. Conclusion & Solution



SOLAS

(International Convention for the Safety of Life at Sea, 1974)

CHAPTER XI-2
SPECIAL MEASURES TO ENHANCE MARITIME SECURITY

Regulation 1
Definitions

1 For the purpose of this chapter, unless expressly provided otherwise:

.12 International Ship and Port Facility Security (ISPS) Code means the International Code for the Security of Ships and of Port Facilities consisting of **Part A (the provisions of which shall be treated as mandatory)** and **part B (the provisions of which shall be treated as recommendatory)**, as adopted, on 12 December 2002, by resolution 2 of the Conference of Contracting Governments to the International Convention for the Safety of Life at Sea, 1974 as may be amended by the Organization, provided that:

goods or the provisions of port services to or from the ship.

.9 Port facility is a location, as determined by the Contracting Government or by the Designated Authority, where the ship/port interface takes place. This includes areas such as anchorages, waiting berths and approaches from seaward, as appropriate.

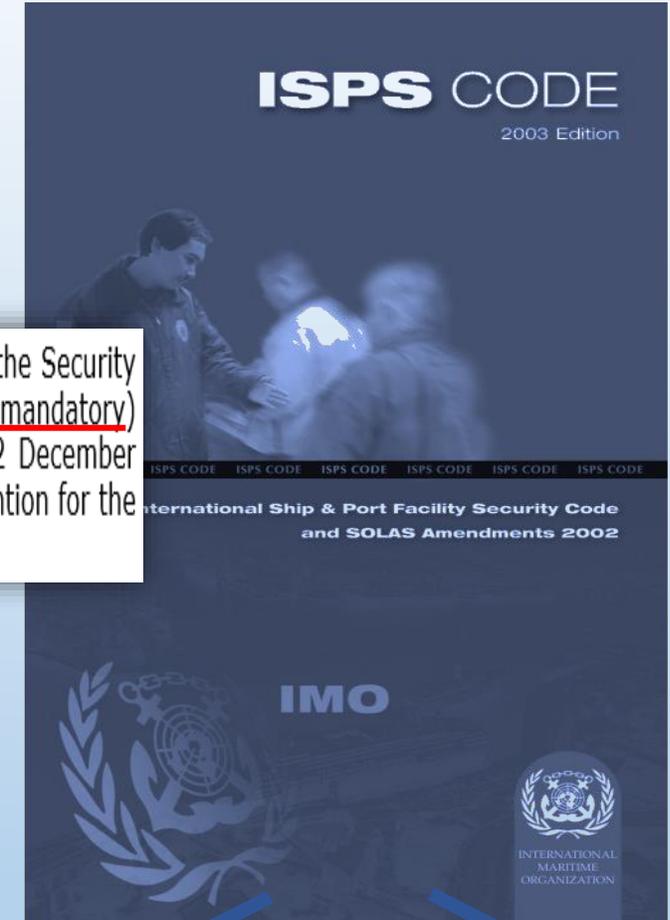
.10 Ship to ship activity means any activity not related to a port facility that involves the transfer of goods or persons from one ship to another.

.11 Designated Authority means the organization(s) or the administration(s) identified, within the Contracting Government, as responsible for ensuring the implementation of the provisions of this chapter pertaining to port facility security and ship/port interface, from the point of view of the port facility.

.12 International Ship and Port Facility Security (ISPS) Code means the International Code for the Security of Ships and of Port Facilities consisting of Part A (the provisions of which shall be treated as mandatory) and part B (the provisions of which shall be treated as recommendatory), as adopted, on 12 December 2002, by resolution 2 of the Conference of Contracting Governments to the International Convention for the Safety of Life at Sea, 1974 as may be amended by the Organization, provided that:

.1 amendments to part A of the Code are adopted, brought into force and take effect in accordance with article VIII of the present Convention concerning the amendment procedures applicable to the Annex other than chapter 1; and

.2 amendments to part B of the Code are adopted by the Maritime Safety Committee in accordance with its Rules of Procedure.



CHAPTER A
Mandatory

CHAPTER B
Recommendatory

ISPS

International Ship and Port Facility Security

13 TRAINING, DRILLS AND EXERCISES ON SHIP SECURITY

13.1 The company security officer and appropriate shore-based personnel shall have knowledge and have received training, taking into account the guidance given in part B of this Code.

13.2 The ship security officer shall have knowledge and have received training, taking into account the guidance given in part B of this Code.

13.3 Shipboard personnel having specific security duties and responsibilities shall understand their responsibilities for ship security as described in the ship security plan and shall have sufficient knowledge and ability to perform their assigned duties, taking into account the

13.4 To ensure the effective implementation of the ship security plan, drills shall be carried out at appropriate intervals taking into account the ship type, ship personnel changes, port facilities to be visited and other relevant circumstances, taking into account the guidance given in part B of this Code.

be visited and other relevant circumstances, taking into account the guidance given in part B of this Code.

13.5 The company security officer shall ensure the effective coordination and implementation of ship security plans by participating in exercises at appropriate intervals, taking into account the guidance given in part B of this Code.

Drills and exercises

13.5 The objective of drills and exercises is to ensure that shipboard personnel are proficient in all assigned security duties at all security levels and the identification of any

13.6 To ensure the effective implementation of the provisions of the ship security plan, drills should be conducted at least once every three months. In addition, in cases where more than 25 percent of the ship's personnel has been changed, at any one time, with personnel that has not previously participated in any drill on that ship, within the last 3 months, a drill should be conducted within one week of the change. These drills should test individual elements of the plan such as those security threats listed in paragraph 8.9.

elements of the plan such as those security threats listed in paragraph 8.9.

13.7 Various types of exercises which may include participation of company security officers, port facility security officers, relevant authorities of Contracting Governments as ship security officers, if available, should be carried out at least once each calendar year with no more than 18 months between the exercises. These exercises should test communications, coordination, resource availability, and response. These exercises may be:

1. full scale or live;

2. tabletop simulation or seminar; or

3. combined with other exercises held such as search and rescue or emergency response exercises.

13.8 Company participation in an exercise with another Contracting Government should be recognized by the Administration.

8.9 The SSA should consider all possible threats, which may include the following types of security incidents:

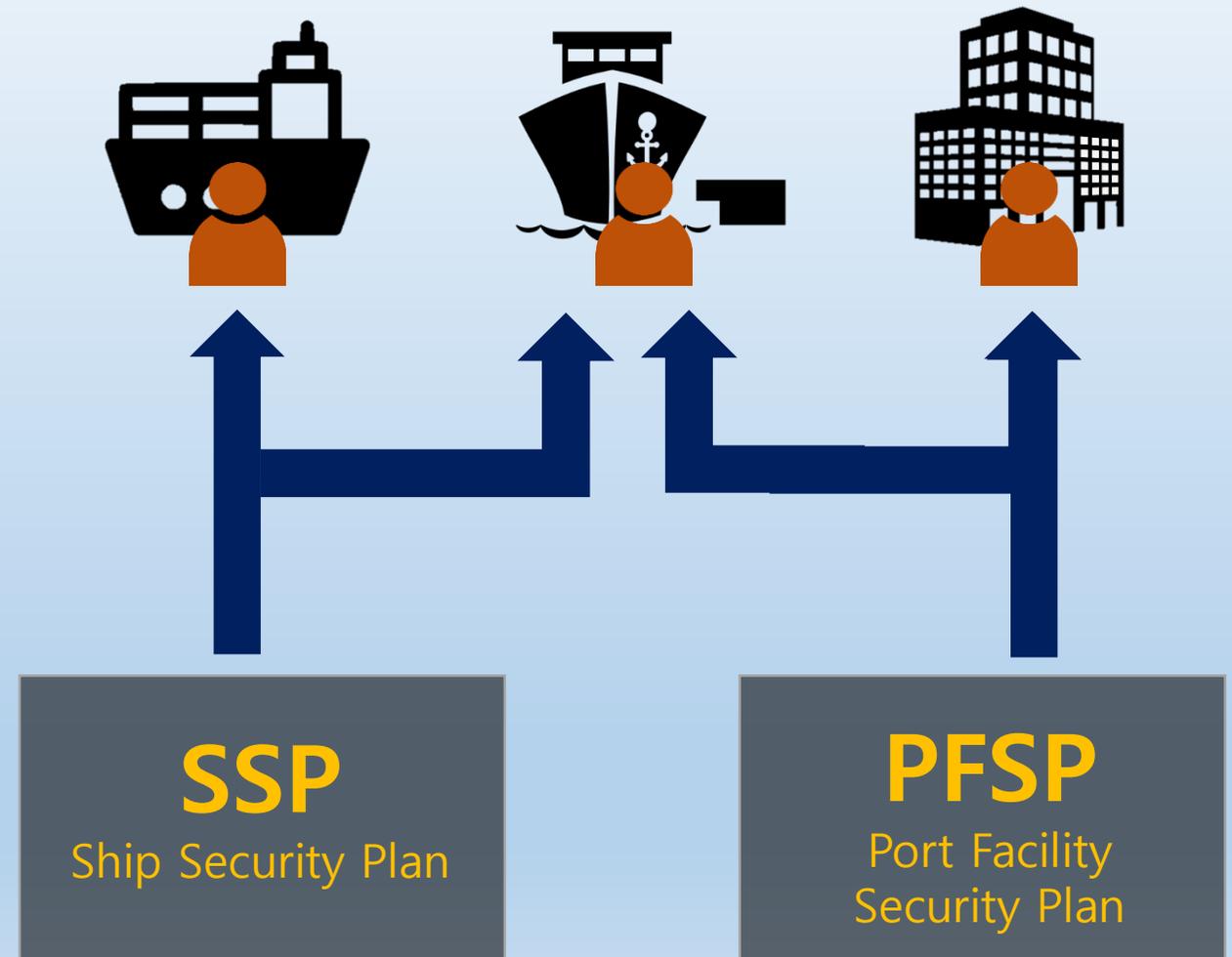
1. damage to, or destruction of, the ship or of a port facility, e.g. by explosive devices, arson, sabotage or vandalism;
2. hijacking or seizure of the ship or of persons on board;
3. tampering with cargo, essential ship equipment or systems or ship's stores;
4. unauthorized access or use, including presence of stowaways;
5. smuggling weapons or equipment, including weapons of mass destruction;
6. use of the ship to carry those intending to cause a security incident and/or their equipment;
7. use of the ship itself as a weapon or as a means to cause damage or destruction;
8. attacks from seaward whilst at berth or at anchor; and
9. attacks whilst at sea.

ISPS

International Ship and Port Facility Security

2.1 For the purpose of this part, unless expressly provided otherwise:

- .1 *Convention* means the International Convention for the Safety of Life at Sea, 1974 as amended.
- .2 *Regulation* means a regulation of the Convention.
- .3 *Chapter* means a chapter of the Convention.
- .4 *Ship security plan* means a plan developed to ensure the application of measures on board the ship designed to protect persons on board, cargo, cargo transport units, ship's stores or the ship from the risks of a security incident.
- .5 *Port facility security plan* means a plan developed to ensure the application of measures designed to protect the port facility and ships, persons, cargo, cargo transport units and ship's stores within the port facility from the risks of a security incident.
- .6 *Ship security officer* means the person on board the ship, accountable to the master, designated by the Company as responsible for the security of the ship, including implementation and maintenance of the ship security plan and for liaison with the company security officer and port facility security officers.
- .7 *Company security officer* means the person designated by the Company for ensuring that a ship security assessment is carried out; that a ship security plan is developed, submitted for approval, and thereafter implemented and maintained and for liaison with port facility security officers and the ship security officer.
- .8 *Port facility security officer* means the person designated as responsible for the development, implementation, revision and maintenance of the port facility security plan and for liaison with the ship security officers and company security officers.



ISPS

International Ship and Port Facility Security

2.1 For the purpose of this part, unless expressly provided otherwise:

- .1 *Convention* means the International Convention for the Safety of Life at Sea, 1974 as amended.
- .2 *Regulation* means a regulation of the Convention.
- .3 *Chapter* means a chapter of the Convention.

.4 *Ship security plan* means a plan developed to ensure the application of measures on board the ship designed to protect persons on board, cargo, cargo transport units, ship's stores or the ship from the risks of a security incident.

**Ship's network,
Ship's network-
based service**

.5 *Port facility security plan* means a plan developed to ensure the application of measures designed to protect the port facility and ships, persons, cargo, cargo transport units and ship's stores within the port facility from the risks of a security

Company security officer means the person on board the ship, accountable to the Company as responsible for the security of the ship, the development, implementation and maintenance of the ship security plan and for liaison with the company security officer and port facility security officers.

.7 *Company security officer* means the person designated by the Company for ensuring that a ship security assessment is carried out; that a ship security plan is developed, submitted for approval, and thereafter implemented and maintained and for liaison with port facility security officers and the ship security officer.

.8 *Port facility security officer* means the person designated as responsible for the development, implementation, revision and maintenance of the port facility security plan and for liaison with the ship security officers and company security officers.

9 SHIP SECURITY PLAN

9.4 Such a plan shall be developed, taking into account the guidance given in part B of this Code and shall be written in the working language or languages of the ship. If the language or languages used is not English, French or Spanish, a translation into one of these languages shall be included. The plan shall address, at least, the following:

.1 measures designed to prevent weapons, dangerous substances and devices intended for use against persons, ships or ports and the carriage of which is not authorized from being taken on board the ship;



.15 procedures to ensure the inspection, testing, calibration, and maintenance of any security equipment provided on board;

.16 frequency for testing or calibration of any security equipment provided on board;

.17 identification of the locations where the ship security alert system activation points are provided;¹ and

.18 procedures, instructions and guidance on the use of the ship security alert system, including the testing, activation, deactivation and resetting and to limit false alerts.¹

.19 Procedures for installing ship network security equipment and preventing or responding to unauthorized access on the onboard network

ISPS

International Ship and Port Facility Security

9 SHIP SECURITY PLAN

General

9.1 The Company Security Officer (CSO) has the responsibility of ensuring that a Ship Security Plan (SSP) is prepared and submitted for approval. The content of each individual SSP should vary depending on the particular ship it covers. The Ship Security Assessment (SSA) will have identified the particular features of the ship and the potential threats and vulnerabilities. The preparation of the SSP will require these features to be addressed in detail. Administrations may prepare advice on the preparation and content of a SSP.

9.2 All SSPs should:

- .1 detail the organizational structure of security for the ship;
- .2 detail the ship's relationships with the Company, port facilities, other ships and relevant authorities with security responsibility;
- .3 detail the communication systems to allow effective continuous communication within the ship and between the ship and others, including port facilities;
- .4 detail the basic security measures for security level 1, both operational and physical, that will always be in place;
- .5 detail the additional security measures that will allow the ship to progress without delay to security level 2 and, when necessary, to security level 3;
- .6 provide for regular review, or audit, of the SSP and for its amendment in response to experience or changing circumstances; and
- .7 reporting procedures to the appropriate Contracting Governments contact points.



USB FILTER



**FIREWALL
BETWEEN
OT & IT**



**REGULAR
UPDATES OF
VACCINE
PROGRAM**



**SETTING OF
SECURITY LEVEL**



SSO

Ship Security Officer

13 TRAINING, DRILLS AND EXERCISES ON SHIP SECURITY

13.1 The company security officer and appropriate shore-based personnel shall have knowledge and have received training, taking into account the guidance given in part B of this Code.

13.2 The ship security officer shall have knowledge and have received training, taking into

13.2 The ship security officer shall have knowledge and have received training, taking into account the guidance given in part B of this Code.

their responsibilities for ship security as described in the ship security plan and shall have sufficient knowledge and ability to perform their assigned duties, taking into account the guidance given in part B of this Code.

13.4 To ensure the effective implementation of the ship security plan, drills shall be carried out at appropriate intervals taking into account the ship type, ship personnel changes, port facilities to be visited and other relevant circumstances, taking into account the guidance given in part B of this Code.

13.5 The company security officer shall ensure the effective coordination and implementation of ship security plans by participating in exercises at appropriate intervals, taking into account the guidance given in part B of this Code.

Training

13.1 The Company Security Officer (CSO) and appropriate shore based Company personnel, and the Ship Security Officer (SSO), should have knowledge of, and receive training, in some or all of the following, as appropriate:

- .1 security administration;
- .2 relevant international conventions, codes and recommendations;
- .3 relevant Government legislation and regulations;
- .4 responsibilities and functions of other security organizations;
- .5 methodology of ship security assessment;
- .6 methods of ship security surveys and inspections;
- .7 ship and port operations and conditions;
- .8 ship and port facility security measures;
- .9 emergency preparedness and response and contingency planning;
- .10 instruction techniques for security training and education, including security measures and procedures;
- .11 handling sensitive security related information and security related communications;
- .12 knowledge of current security threats and patterns;
- .13 recognition and detection of weapons, dangerous substances and devices;
- .14 recognition, on a non discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten security;
- .15 techniques used to circumvent security measures;
- .16 security equipment and systems and their operational limitations;
- .17 methods of conducting audits, inspection, control and monitoring;
- .18 methods of physical searches and non-intrusive inspections;
- .19 security drills and exercises, including drills and exercises with port facilities; and
- .20 assessment of security drills and exercises.



.21 methodology of ship cyber security assessment
.22 methods of ship cyber security surveys and inspections;

STCW

The International Convention on Standards of Training, Certification and Watchkeeping for Seafarers

MODEL COURSE

The program of model training courses developed out of suggestions from a number of IMO Member Governments to facilitate access to the knowledge and skills demanded by increasingly sophisticated maritime technology.



Ship Security Officer

MODEL COURSE
3.19

SHIP SECURITY OFFICER

2012 Edition

EXIST,
Need to update when
ISPS is revised



ALL CREW MEMBER

MODEL COURSE

?

CYBER SECURITY

DOES NOT EXIST,
Should be made
when ISPS is revised



Version - up of ISPS code

We must prepare and prevent a response because cyber attack is an imminent threat in the shipping industry and is not limited for anyone.

※ Reference

- [1] Maritime Technology System 2030 – ECMAR
- [2] The Autonomous Ship - MUNIN
- [3] The Maritime Commons : Digital Repository of the WMU
- [4] The Guidelines on Cyber Security Onboard Ships – BIMCO
- [5] Framework for Improving Critical Infrastructure Cybersecurity – NIST
- [6] 해상사이버보안가이드라인 – KR
- [7] SIRE VIQ Edition 7 - OCIMF
- [8] Strategic Plan for the Organization for the six year period 2018 to 2023 – IMO Resolution A.1110(30)
- [9] Guidelines on Maritime Cyber Risk Management – IMO MSC – FAL.1/Circ.3
- [10] SOLAS (International Convention for the Safety of Life at Sea) Chapter XI – 2
- [11] Resolution MSC 428(98) – IMO
- [12] ISM code
- [13] Jeon, Dong-Keun. "Conventional Layered Ship Area Network Architecture Based on International Standards." *Semantic Scholar*, 2017, [d3i71xaburhd42.cloudfront.net/0145550146cfa49842beae989d192c11680c87b4/3-Figure1-1.png](https://www.semanticscholar.org/document/0145550146cfa49842beae989d192c11680c87b4/3-Figure1-1.png).
- [14] NG, SAT. "Cybersecurity for UNOLS." *University National Oceanographic Laboratory System*, 2017, www.unols.org/sites/default/files/201717rvt_breakout2_CyberSecurity.pdf.

An aerial photograph of a large cargo ship sailing on a dark blue sea. The ship's deck is covered with numerous colorful shipping containers in shades of yellow, red, blue, and green. The ship's hull is white, and the name 'THE SHERIFF' is visible on the side. The water shows a slight wake behind the vessel.

Thank You

Team The Sheriff

27/27