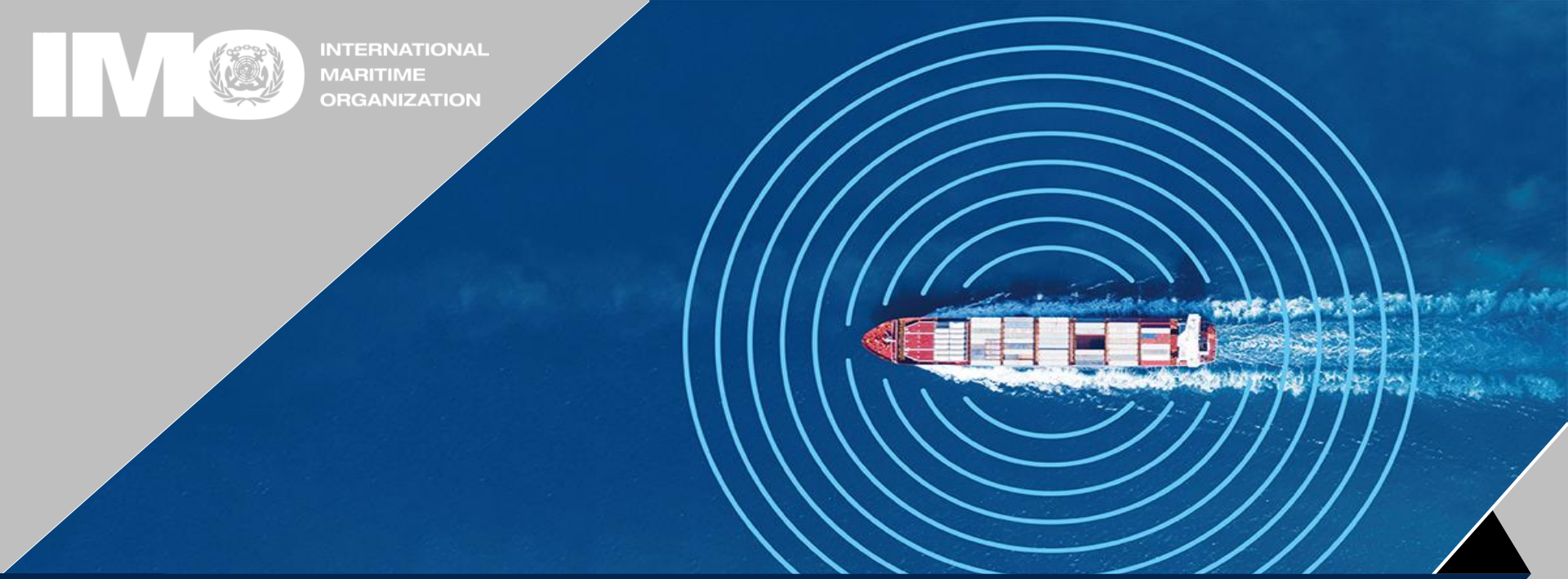
INTERNATIONAL MARITIME ORGANIZATION



IMCS CODE Proposal Considering MASS Technical Features

; INTERNATIONAL MASS CYBER SECURITY CODE

TEAM Cyber Sheriffs

INTERNATIONAL MARITIME ORGANIZATION

A Table of Contents

01

INTRODUCTION

1 - 1. Increasing Cyber Attacks on Ships

IT

In 2017, the shipping company “Maersk”, suffered a "NotPetya" ransomware attack resulting in approximately $300 million USD in damages

Cyberattack cost Maersk as much as $300 million and disrupted operations for 2 weeks

Maersk was hit by a worm dubbed NotPetya, which locked access to systems that the company uses to operate shipping terminals all over the world. Above, containers at a terminal in Germany in 2010. (Patrik Stollarz / AFP/Getty Images)

SUBSCRIBERS ARE READING

CALIFORNIA
'Friends' star Matthew Perry dead at 54, found in hot tub at L.A. home

OPINION
Opinion: Nothing has prepared me for the antisemitism I see on college campuses now

CALIFORNIA
Officials release more details about Matthew Perry's death, but determining cause will take time

USC SPORTS
Commentary: Lincoln Riley is on the verge of losing USC fans' devotion by keeping Alex Grinch

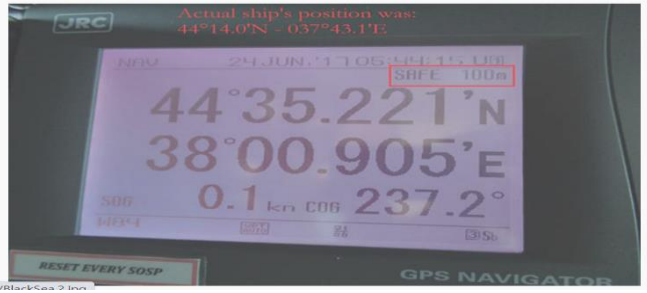
ENTERTAINMENT & ARTS

OT

In 2017, GPS spoofing attack occurred in the Black Sea, affecting more than 20 ships as their GPS signals were spoofed to Gelendzhik Airport.

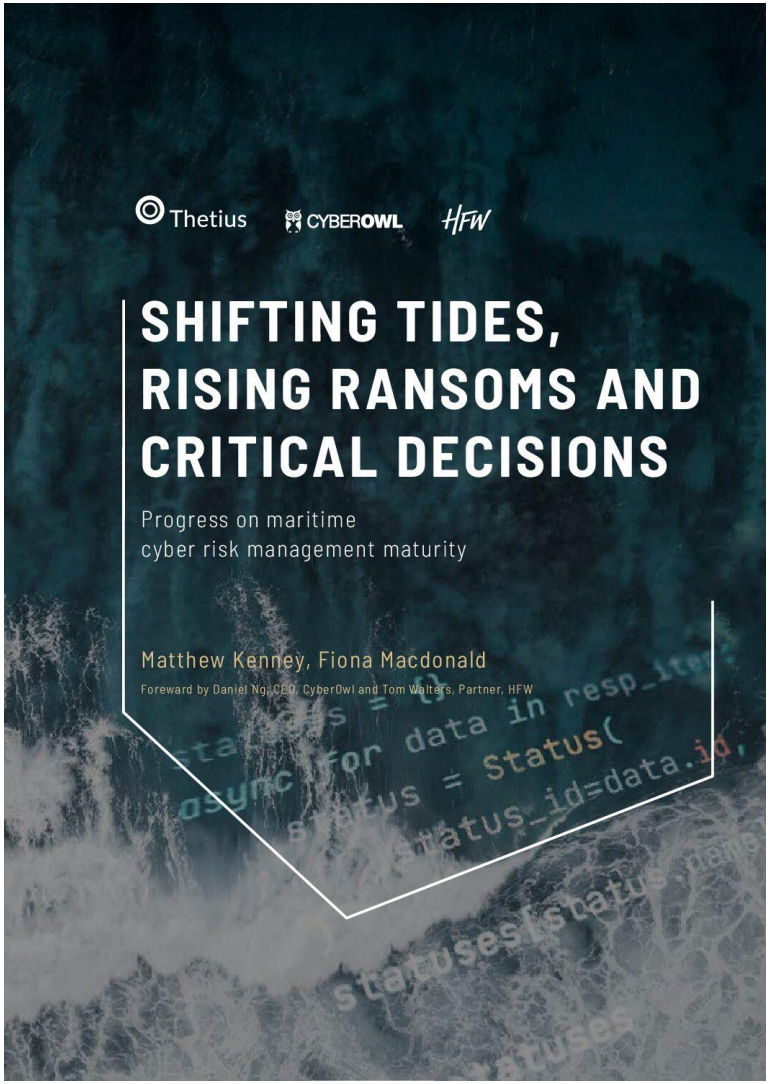
Reports of Mass GPS Spoofing Attack in the Black Sea Strengthen Calls for PNT Backup

July 24, 2017 By Inside GNSS



References : https://insidegnss.com/reports-of-mass-gps-spoofing-attack-in-the-black-sea-strengthen-calls-for-pnt-backup/
https://www.latimes.com/business/la-fi-maersk-cyberattack-20170817-story.html

1 - 2. Increasing cyber threats in the maritime industry



The cost of cyber attacks is on the rise.

The average damage per cyber attack in the maritime sector

2022	2023
$182K	$550K

Increased threefold in one year

Reference : Shifting tides, rising ransoms and critical decisions", Thetius, CYBEROWL, HFW

1 - 3. No rule for Cyber Security of MASS

IACS	UR E26, UR E27 (Unified Requirements for cyber security) **No mention on cyber security of MASS**
Existing Conventions	• **ISPS CODE : No rule for Cyber Security** • **ISM CODE : The regulations about cyber security are at the recommended level.**

References : IACS UR E26, UR E27, ISPS CODE, ISM CODE

1 - 4. IMO'S STRATEGIC PLAN – MASS CODE

MSC

2019, Development of temporary guidelines for MASS test operation completed (MSC-1-Circ 1604) (MSC 101)

2021, Completion of RSE for MASS operation(MSC 103)

2022, Started Development of MASS CODE

2024, Non-compulsory MASS CODE approval (MSC 109)

2025, Mandatory MASS CODE adoption (MSC 109)

2028, Compulsory MASS CODE will take effect

MASS – JWG (MSC – FAL – LEG)

2022, Discussions on common issues of each committee, such as terms and definitions

References : https://www.imo.org/en/MediaCentre/MeetingSummaries/Pages/Symposium-on-%CA%BAMaking-headway-on-the-IMO-MASS-Code%E2%80%9D-.aspx
https://www.imo.org/en/MediaCentre/MeetingSummaries/Pages/MSC-107th-session.aspx

1 - 5. Not enough mention about Cyber Security at MASS CODE

INTERNATIONAL MARITIME ORGANIZATION

MARITIME SAFETY COMMITTEE
107th session
Agenda item 5

MSC 107/WP.9
7 June 2023
Original: ENGLISH

DISCLAIMER
As at its date of issue, this document, in whole or in part, is subject to consideration by the IMO organ to which it has been submitted. Accordingly, its contents are subject to approval and amendment of a substantive and drafting nature, which may be agreed after that date.

DEVELOPMENT OF A GOAL-BASED INSTRUMENT FOR MARITIME AUTONOMOUS SURFACE SHIPS (MASS)

Section 2.7 (Communications/Connectivity)

49 The Group discussed at length the need for a communications section in part 2, bearing in mind that section 3 in part 3 already contained goals and Functional requirements (FRs) which covered the SOLAS-like part of communications.

50 In the ensuing discussions the following views were expressed:

.1 there was a clear distinction between communication and connectivity and the former was addressed in detail in part 3, section 3, whereas connectivity should be included in section 2.7;

Cyber security should be considered in the context of communications and connectivity between the MASS and ROC. (MASS CODE 2.7.)

.5 cybersecurity should be considered in this context.

1 - 6. Not enough mention about Cyber Security at MASS CODE

INTERNATIONAL MARITIME ORGANIZATION

MARITIME SAFETY COMMITTEE
107th session
Agenda item 5

MSC 107/WP.9
7 June 2023
Original: ENGLISH

DEVELOPMENT OF A GOAL-BASED INSTRUMENT FOR MARITIME AUTONOMOUS SURFACE SHIPS (MASS)

9 SECURITY

9.1 Goal

The goal of this section is to fulfil the security objectives of SOLAS and the ISPS Code, taking into account the number of persons, [and the property] on board and [the level of autonomy] [mode of operation].

9.2 High Level Functional Requirements

FR9.1.1: A MASS should comply with all relevant SOLAS security requirements for all security levels as modified by the specific Functional Requirements below.

.1 To detect security threats and take preventive measures against security incidents affecting ships.

.2 To ensure confidence that adequate and proportionate maritime security

Cyber security is not considered at the Part 3.9. SECURITY.

02

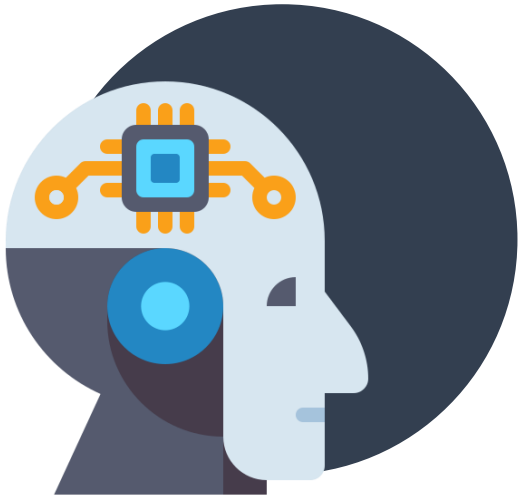
PROBLEM ANALYSIS

The subject of judgement

Conventional Ship

Seafarer with eyes, decision

MASS



AI with data, decision

On behalf of existing crew members,
AI collects and analyzes data from sensors.

Enhanced Connectivity

Between the IT system and OT system

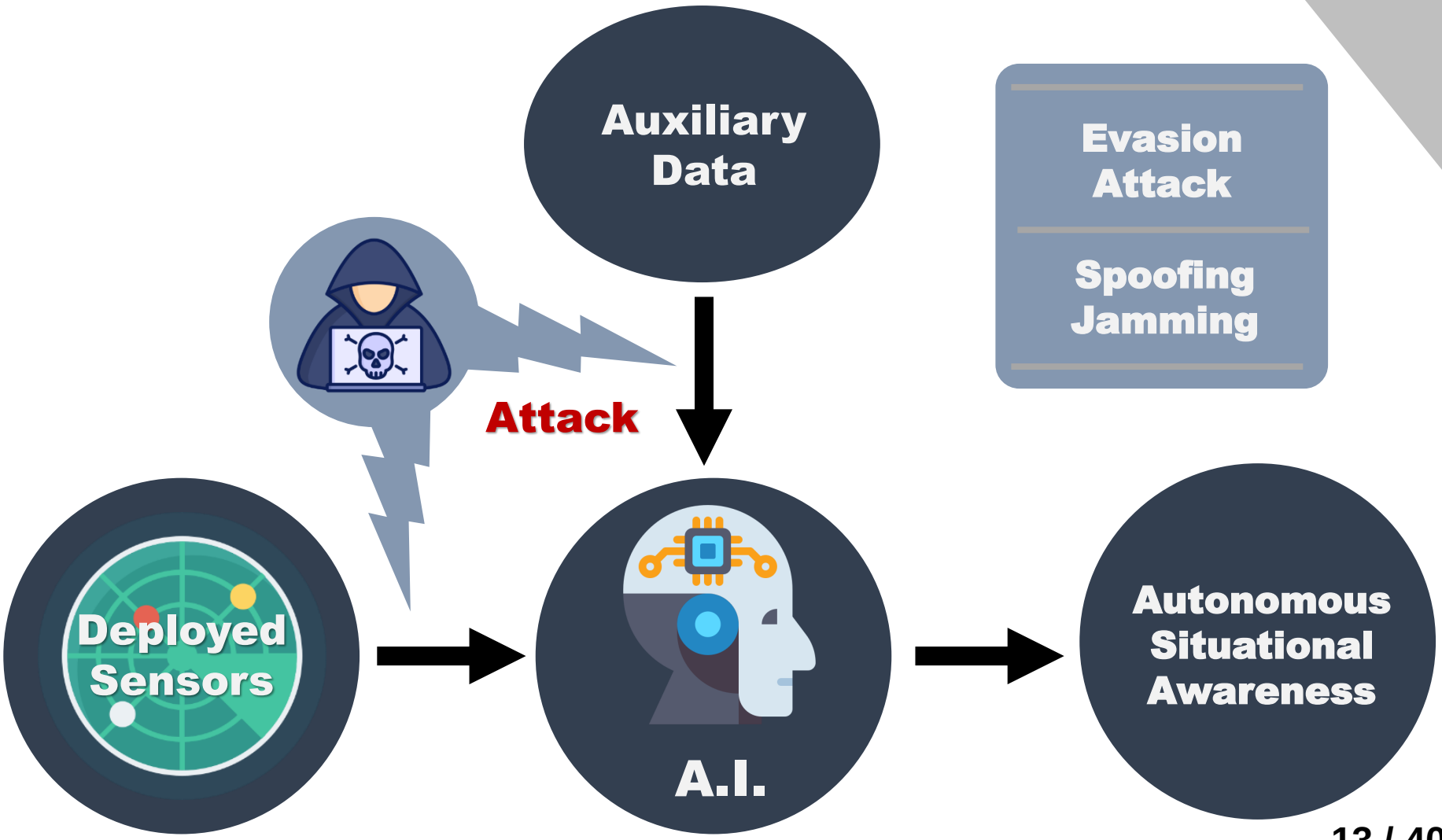
IT — OT

Between the ROC and MASS

ROC — MASS

2 - 3. The new types of cyber attack on MASS

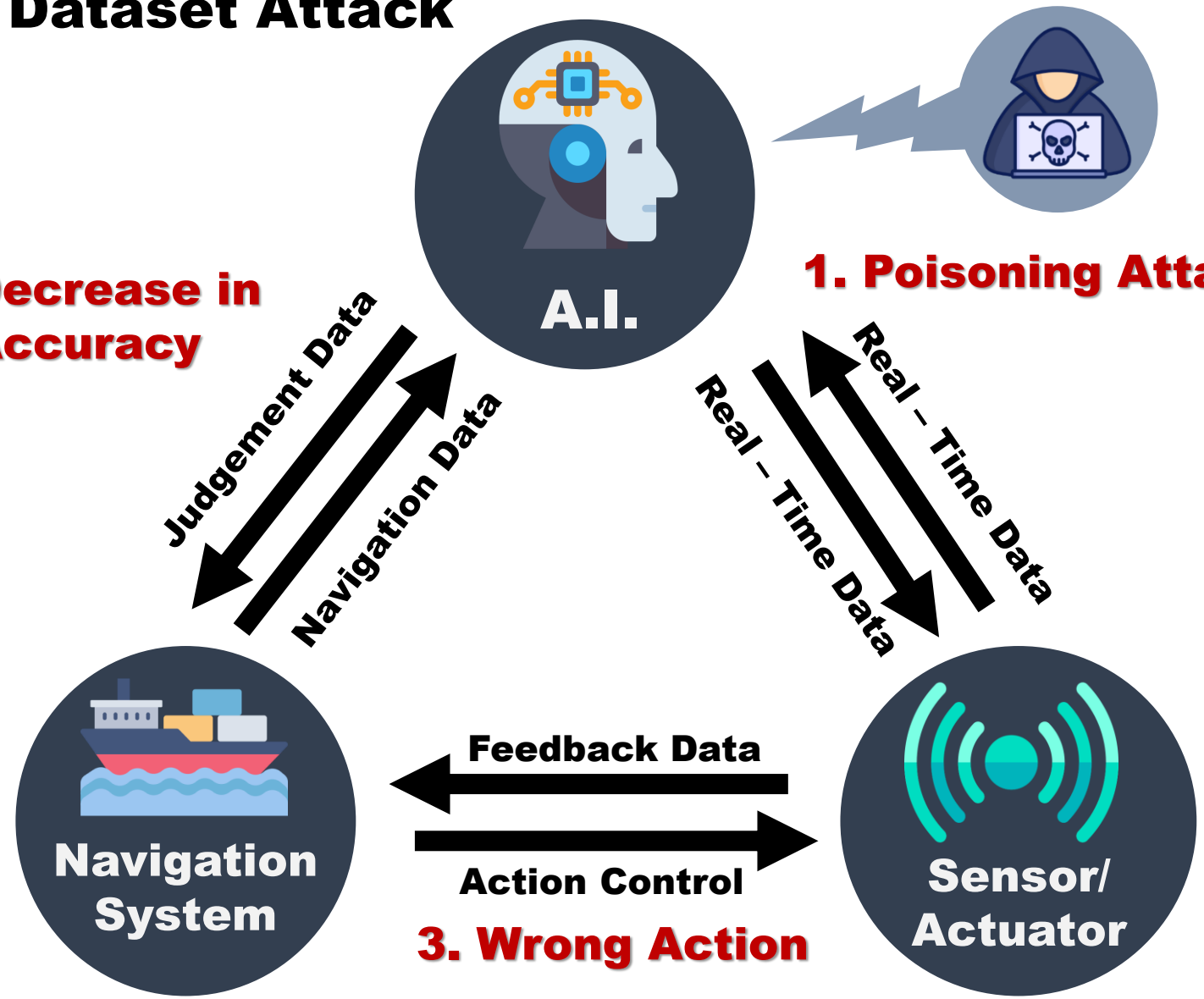
Sensor Data Attack



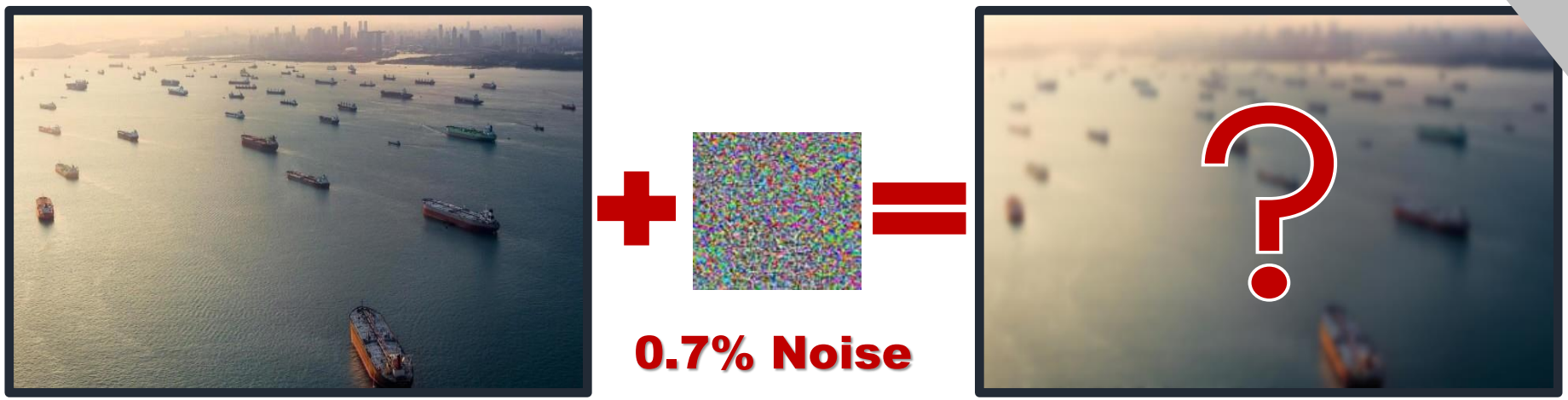
Reference : Jiwoon Yoo, Artificial Intelligence for Autonomous Ship : A Study on Potential Cyber Threats and Security Requirements

2 - 4. The new types of cyber attack on MASS

Ship Dataset Attack



Ship Dataset Attack – Poisoning Attack

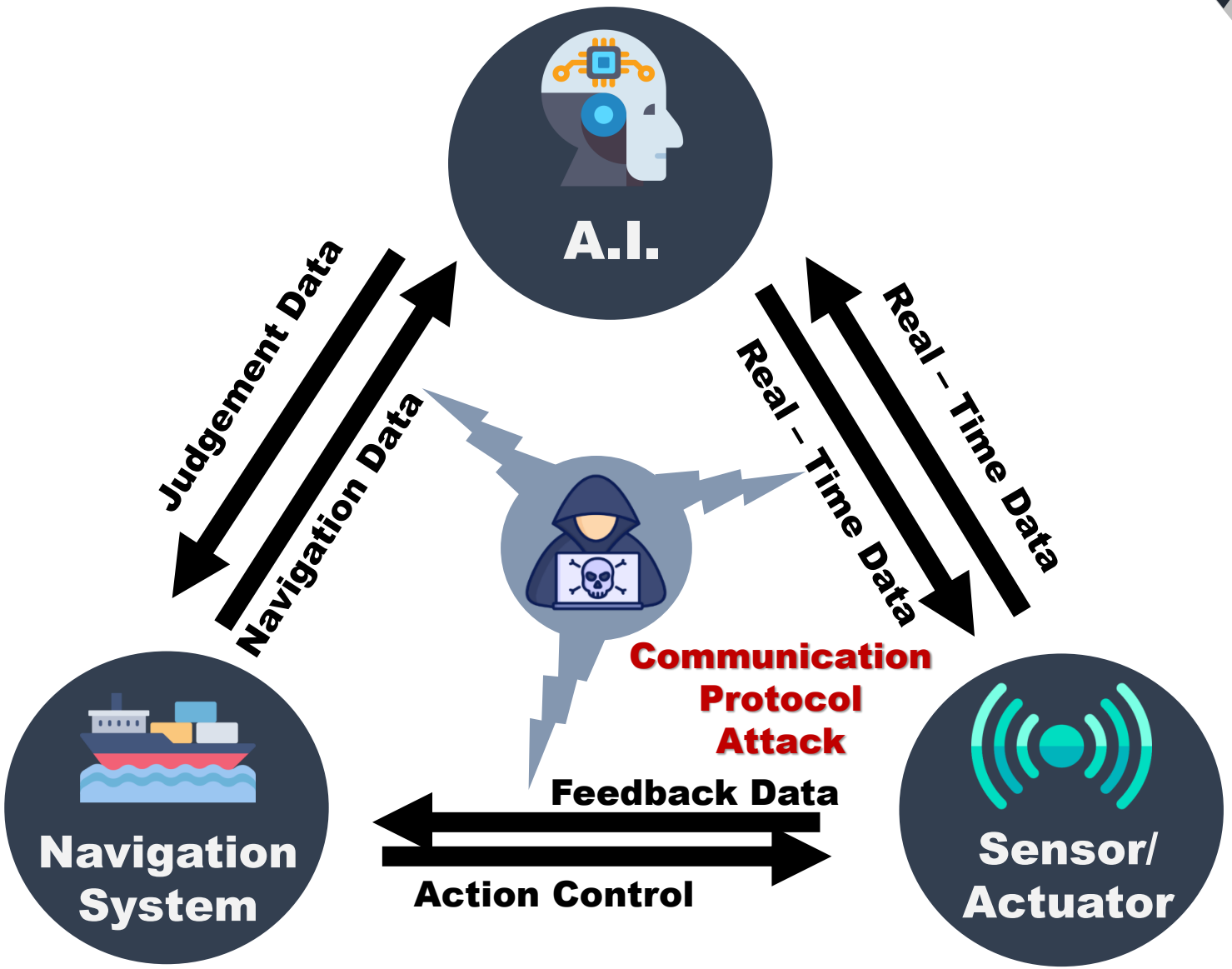


By adding only 0.7% noise to the image,

A.I. can misclassify the image of ship.

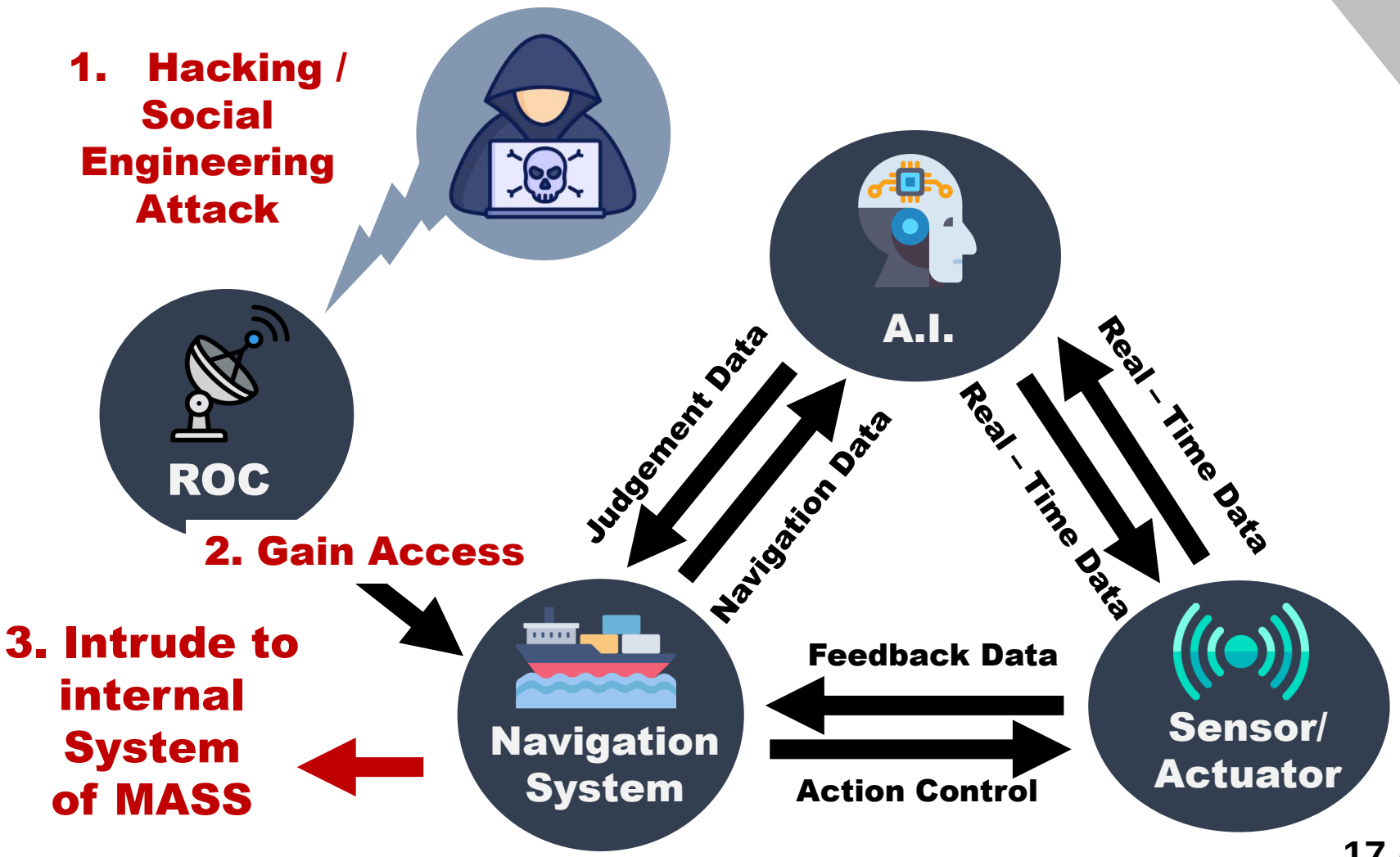
Reference : Jiang, Wenbo, et al. "Poisoning and evasion attacks against deep learning algorithms in autonomous vehicles." IEEE transactions on vehicular technology 69.4 (2020): 4439-4449.

Communication Protocol Attack



2 - 7. The new types of cyber attack on MASS

Gain Access through ROC (Remote Operation Centre)



Reference : Jiwoon Yoo, Artificial Intelligence for Autonomous Ship : A Study on Potential Cyber Threats and Security Requirements

03

SOLUTION


IMO
INTERNATIONAL
MARITIME
ORGANIZATION
HAMBURG SÜD
ZIM EUROPE
MONROVIA

3 - 1. What is the IMCS CODE?

What is the IMCS CODE?

International code for the cyber security of MASS, port facilities and remote operation center (ROC).

What is the purpose of IMCS CODE?

To enhance cyber security regulations to respond to and prevent cyber attacks targeting MASS, port facilities, and remote operation center (ROC).

3 - 2. Applicable IMO's Strategic Direction

SD 2 : Integrate new and advancing technologies in the regulatory framework

17 As technological development accelerates, new and advancing technologies will significantly affect shipping, creating a more interconnected and efficient industry more closely integrated with the global supply chain. New and advancing technologies have already brought about changes at all levels in the way ships are designed, constructed, equipped and operated, and have had equal impact on personnel, both on board and on shore. Such technologies may also provide access to a large amount of data associated with shipping.

18 Since technological advances present opportunities as well as challenges, their introduction needs to be considered carefully in order for them to be accommodated appropriately into the regulatory framework of the Organization. This involves balancing the benefits derived from new and advancing technologies against safety and security concerns, the impact on the environment and on international trade facilitation, the potential costs to the industry, and finally their impact on personnel, both on board and ashore.

19 The Organization's regulatory framework will be continually adapted to the challenges and global developments facing the shipping industry, with a view to ensuring safety, security and environmental protection. The Organization will strive towards a legal framework that accommodates new and advancing technologies and approaches; it will do so by being technology neutral, developing IMO instruments and performance standards without preference or hindrance of one technology over another.

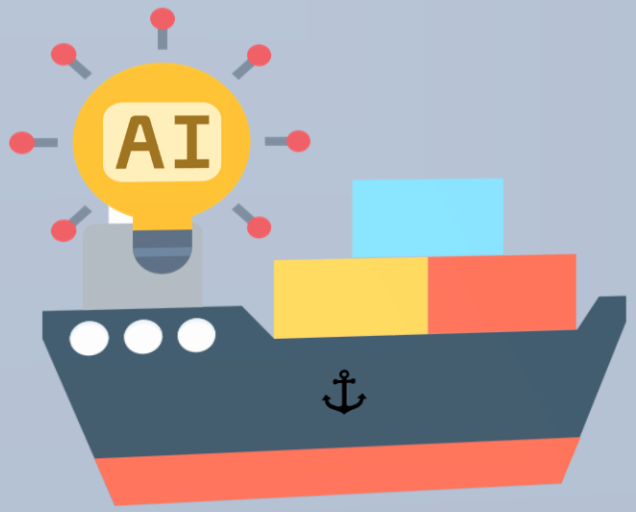
2.23 (New)	Development of a goal-based instrument for maritime autonomous surface ships (MASS)	2025	MSC		

Reference : A32/Res.1149. " Revised strategic plan for the organization for the six-year period 2018 to 2023"

3 - 3. Application of the IMCS CODE

Mandatory Application

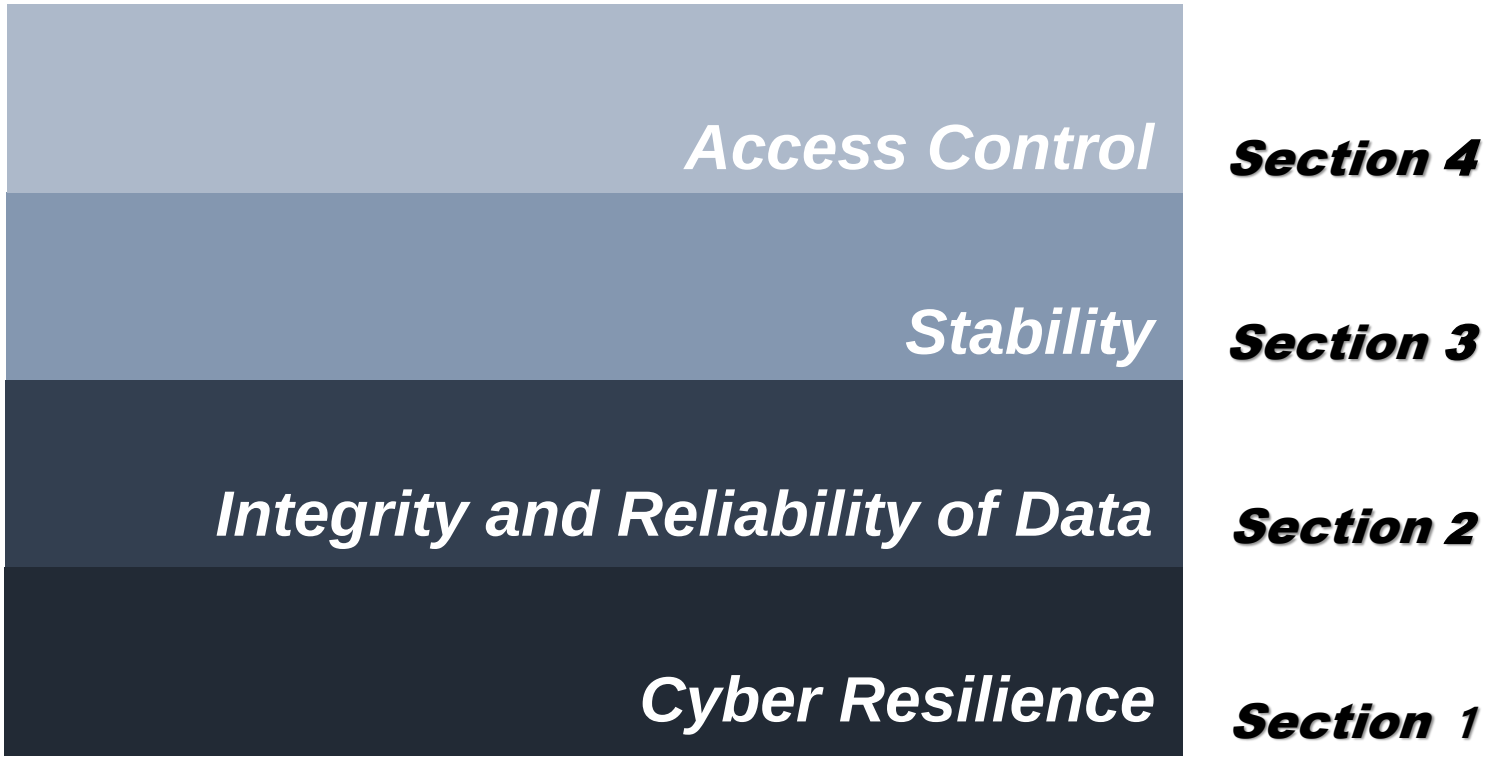
Degree 3, 4
(no seafarers onboard)



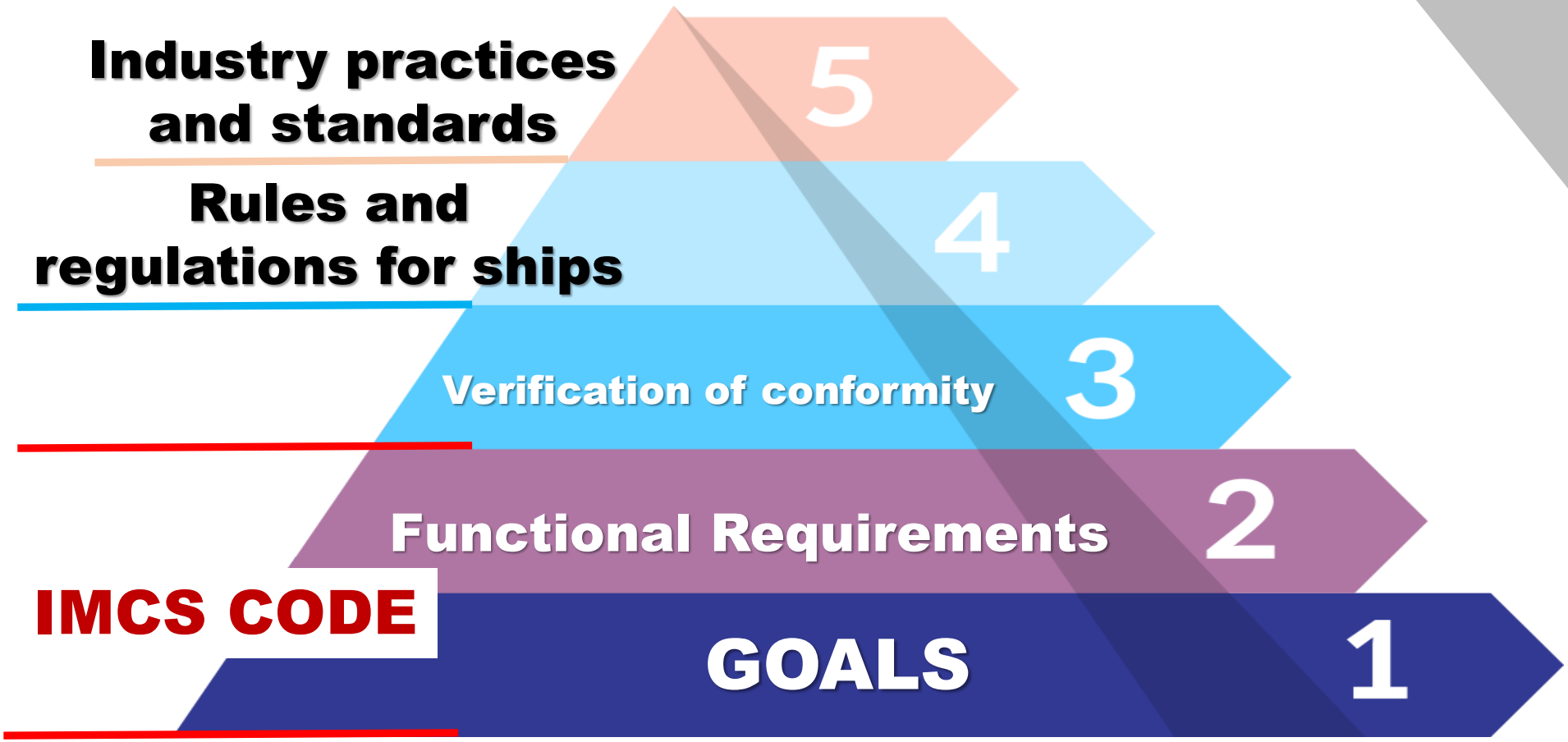
Recommended Application

Degree 1, 2
(seafarers onboard)

IMCS CODE (based on GBS)



IMCS CODE (based on GBS)



Reference : MSC.1/Circ.1394/Rev.2, “GENERIC GUIDELINES FOR DEVELOPING IMO GOAL-BASED STANDARDS”

3 - 6. Section 1. Cyber Resilience

GOAL

Ensure Cyber Resilience
to protect MASS operations from cyber attacks

Functional Requirements

1. *Development of procedures for the cyber security assessment of MASS*

2. *Establishment of a security organization considering the operational features of MASS*

3. *Development of procedures for remote control change over in the event of a cyber security incident*

3 - 6. Section 1. Cyber Resilience

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/Rev.2
7 June 2022

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 The Maritime Safety Committee, at its 104th session (4 to 8 October 2021), and the Facilitation Committee, at its forty-sixth session (9 to 13 May 2022), approved an update to the additional guidance and standards included in paragraph 4.2 of the Guidelines.

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

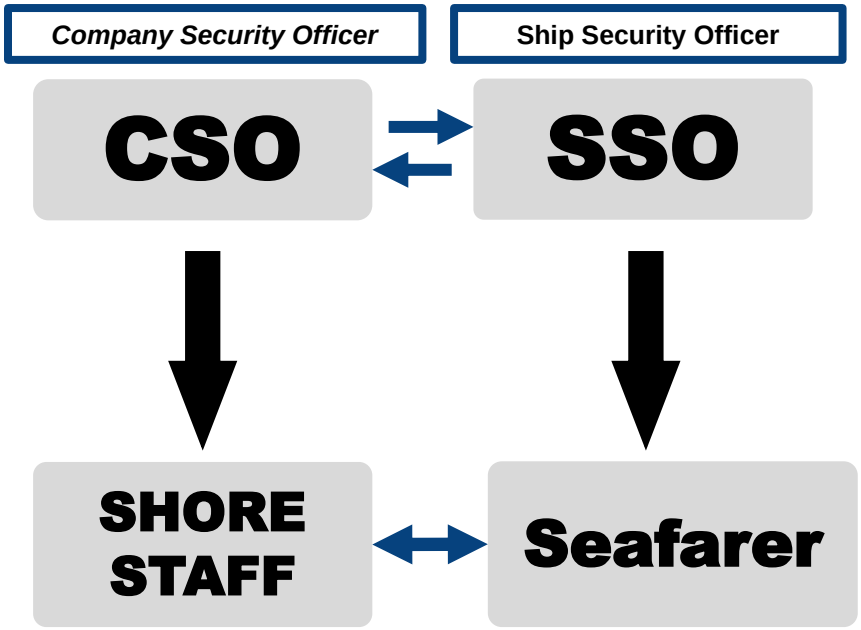
5 This circular and any revisions supersede the interim guidelines contained in MSC.1/Circ.1526.

Based on the guidelines on maritime cyber risk management (MSC-FAL.1/Circ.3/Rev.2),

Cyber risk assessment procedure for mass is mandatory.

Reference : MSC-FAL.1/Circ.3/Rev.2," GUIDELINES ON MARITIME CYBER RISK MANAGEMENT"

3 - 6. Section 1. Cyber Resilience



ISPS's current

security organization chart

On degree 3,4 MASS

There is no seafarer on board.

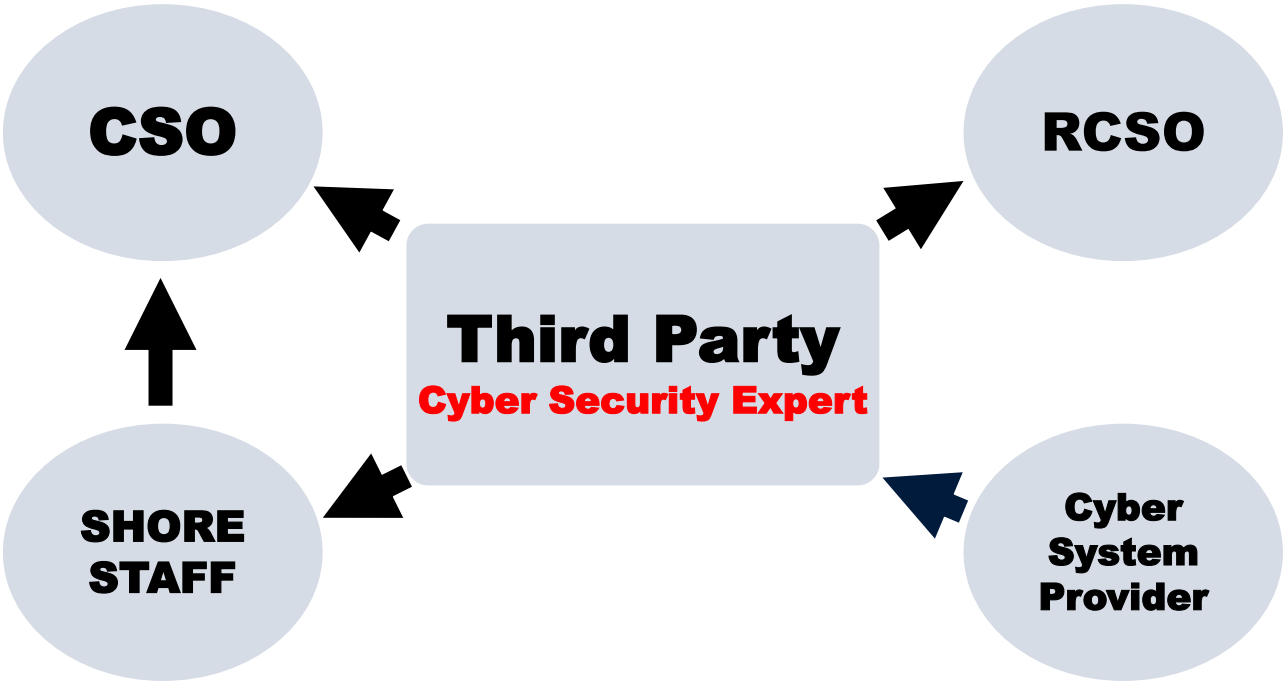
No need for SSO

RCSO

New Need for RCSO

(Remote control Center Security Officer)

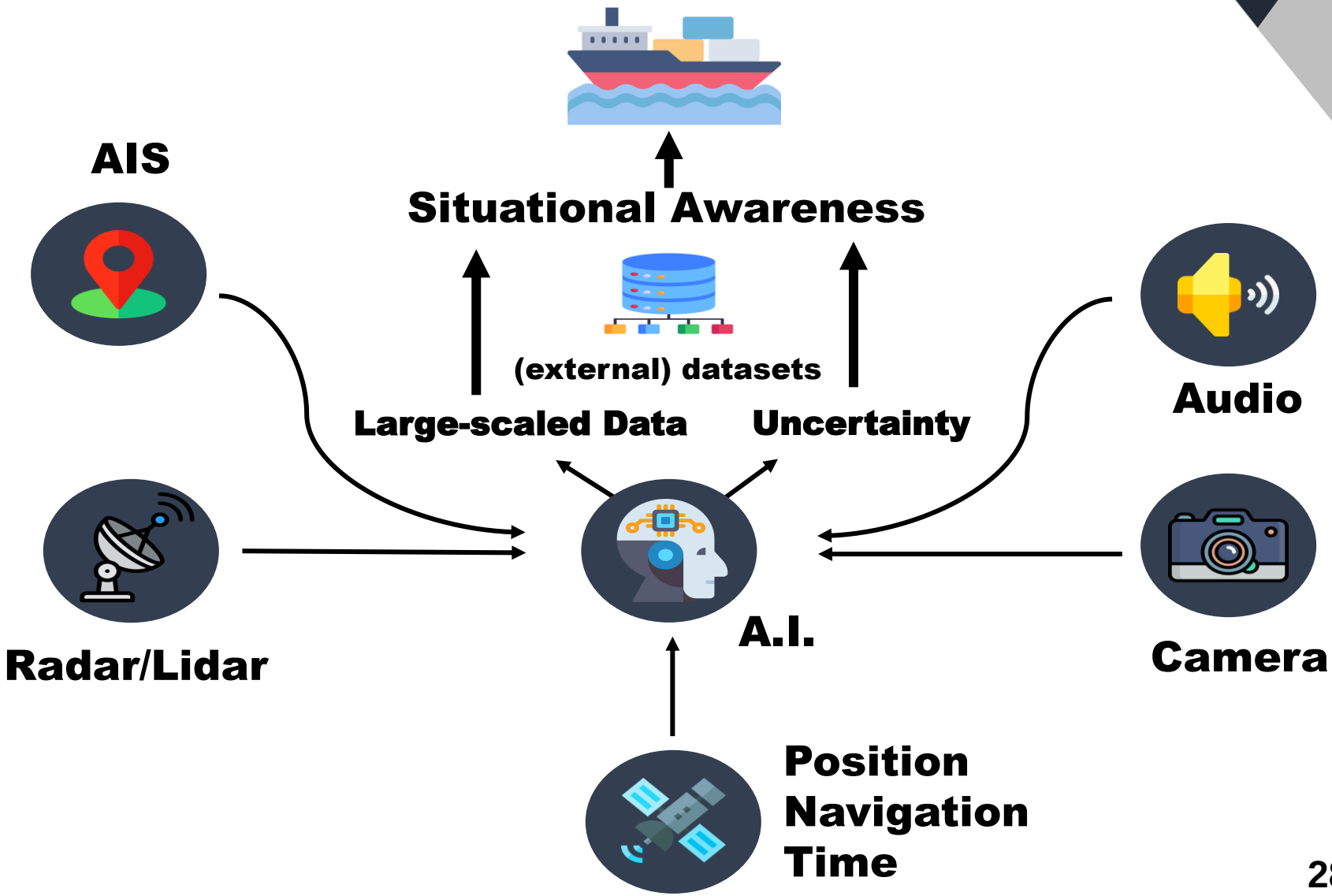
3 - 6. Section 1. Cyber Resilience



ISPS's current security organization have ruled out the participation of external experts because of security.

The new organization should require the participation of external cyber security experts.

3 - 7. Section 2. Integrity, Reliability of Data



Reference : Jiwoon Yoo, Artificial Intelligence for Autonomous Ship : A Study on Potential Cyber Threats and Security Requirements

3 - 7. Section 2. Integrity, Reliability of Data

GOAL

To ensure the integrity and reliability of Data.

With the assurance of such integrity and reliability, safe navigation of the MASS becomes possible.

Functional Requirements

1. *MASS must have a device in place to protect against tampering that may occur during sensor data transmission.*

2. *MASS should use an encryption protocol to protect communication data.*

3. *MASS should provide a verification function for the data of sensor.*

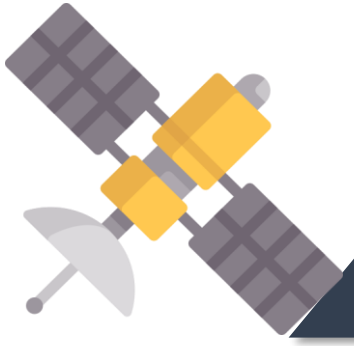
3 - 7. Section 2. Integrity, Reliability of Data

Data transmission Protocol (Now using)

: CAN BUS, NMEA Protocol (for sensor)

Make it mandatory to use secure transmission protocols.
Make it mandatory to use AIS standard considered security.

The AIS standard did not consider cyber security.



SOLAS (1999/2000 Amendment Chapter 5, Rule 19)

Installation of “AIS” is mandatory.

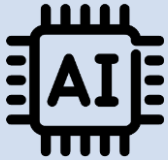
Reference : Goudosis, Athanasios, and Sokratis Katsikas. "Secure AIS with identity-based authentication and encryption." (2020)

3 - 8. Section 3. Stability

GOAL

To ensure the stability of the autonomous navigation system which is based on A.I.

Functional Requirements



1. A.I. should be trained using trustworthy training data.

2. To prevent the external leakage of data used in A.I. deep learning, the security system must be put in place.

3. Verification mechanisms should be in place to ensure the use of trustworthy training data.

3 - 9. Section 4. Access Control

GOAL

To prevent cyber security breaches through the network.

Functional Requirements

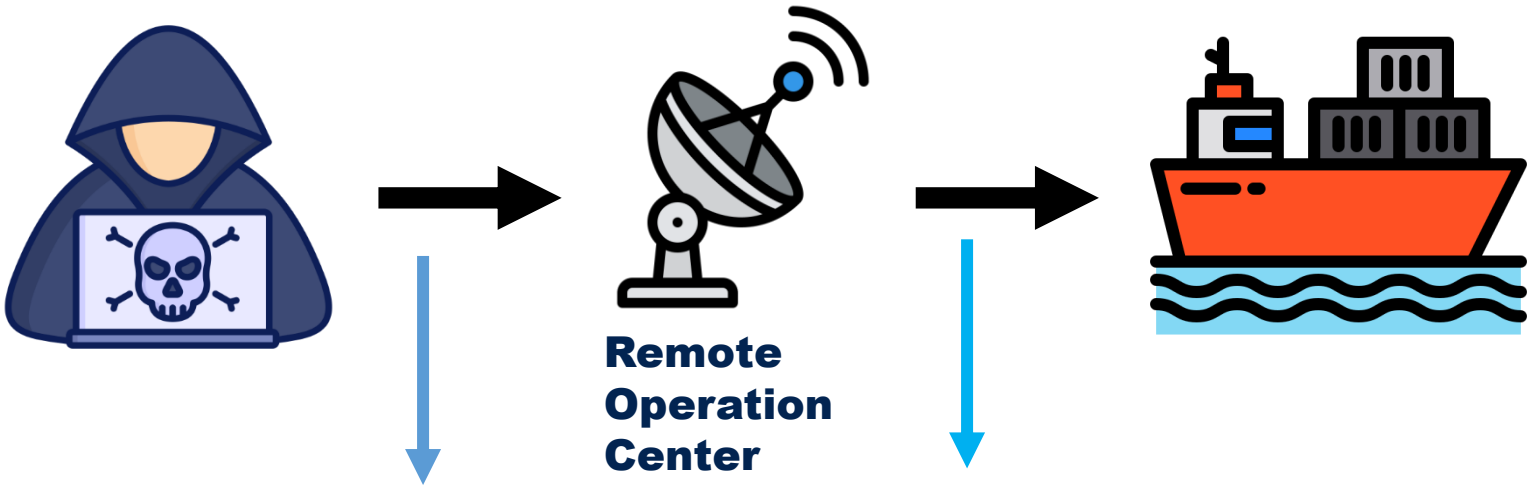
1. User identification and multi-factor authentication must be performed during remote access.

2. We should block unauthorized wireless network connections.

3. Unnecessary internal network exposure to the external network and connections to the system must be restricted.

3 - 10. Section 4. Access Control

Firewall, Intrusion Prevention System (IPS)
Proxy server must be installed at each network layer.

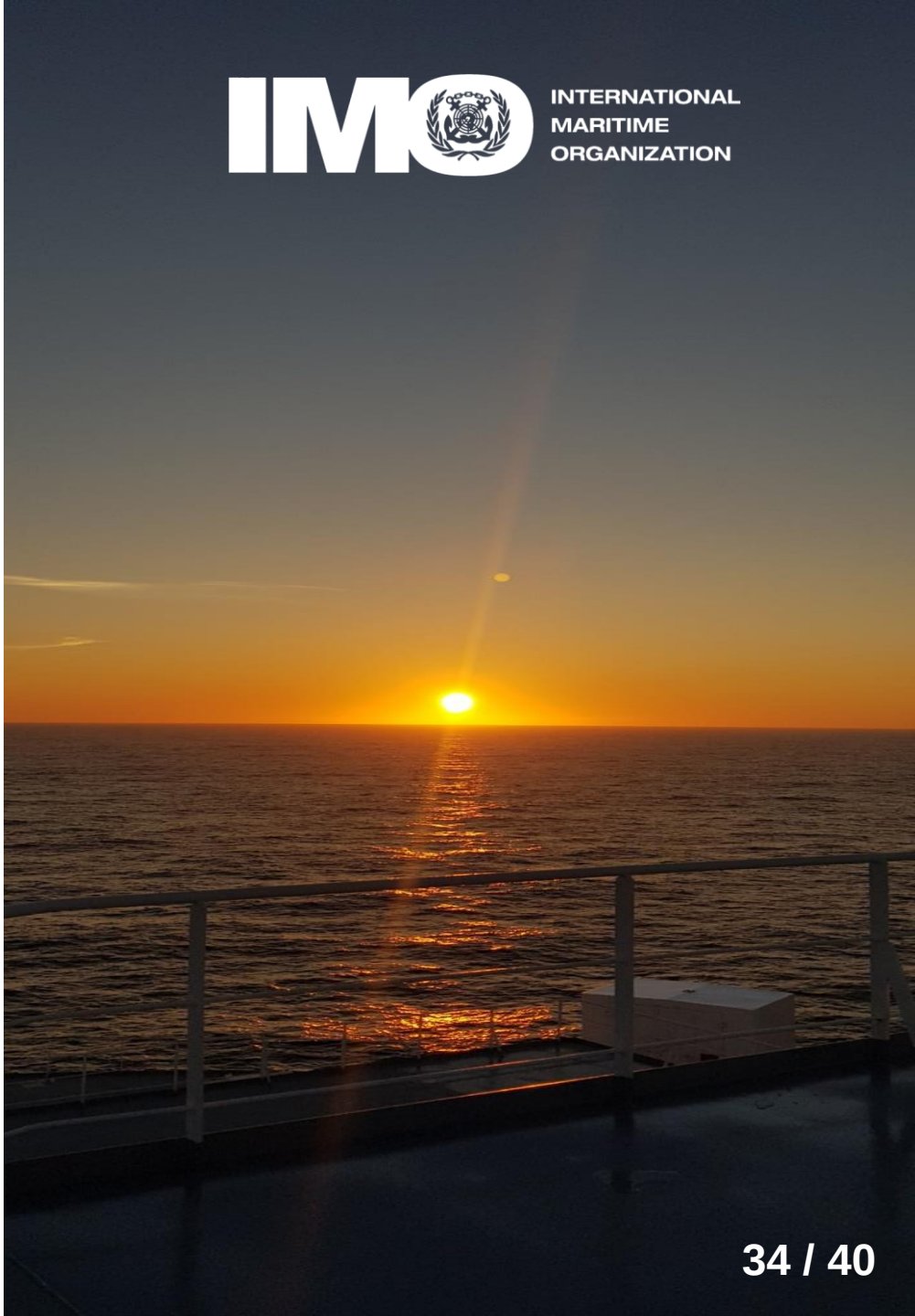


It is mandatory to install an Intrusion Detection System (IDS) for the network inside MASS and the network inside the Remote Operation Center(ROC).

Reference : Nam-Seon Kang , Analysis of onboard ship cybersecurity, Journal of the Korean Society of Marine Engineering, Vol. 42, No. 6 pp. 463~471, 2018

04

CONCLUSION



“ IMCS CODE ”

Consideration of technical features of MASS

Consideration of operational features of MASS

4 - 2. Actions requested of IMO

The IMCS CODE working group needs to be established.

In this proposal, we propose a set of terms of reference for the cyber security of MASS.

Image source: Pixabay

4 - 2. Actions requested of IMO

With MASS CODE under development,

We agree that the IMCS CODE should not repeat provisions or regulations of MASS CODE.

Through discussions within the working group,

We must determine the format for addressing our proposals.

1. Incorporate our proposals into the MASS CODE

2. Provide guidelines in the form of a resolution

3. The development of the IMCS CODE

References

[1] ISM CODE [2] ISPS CODE

[3] https://www.imo.org/en/MediaCentre/MeetingSummaries/Pages/Symposium-on-%CA%BAMaking-headway-on-the-IMO-MASS-Code%E2%80%9D-.aspx

[4] https://www.imo.org/en/MediaCentre/MeetingSummaries/Pages/MSC-107th-session.aspx

[5]Jiwoon Yoo, Artificial Intelligence for Autonomous Ship : A Study on Potential Cyber Threats and Security Requirements

[6] KR Maritime Cyber Safety News & Report Vol.058 June 2023

[7] IACS UR E26, UR E27

[8] 해사안전 Vol.47(2020년 4월호)

[9] Goudosis, Athanasios, and Sokratis Katsikas. "Secure AIS with identity-based authentication and encryption." (2020)

[10] MSC. 1/Circ. 1638. "Outcome of the Regulatory Scoping Exercise for the Use of Maritime Autonomous Surface Ships (MASS)

[11] A32/Res.1149. " Revised strategic plan for the organization for the six-year period 2018 to 2023"

[12] Nam-Seon Kang , Analysis of onboard ship cybersecurity, Journal of the Korean Society of Marine Engineering, Vol. 42, No. 6 pp. 463~471, 2018

[13] MSC.1/Circ.1394/Rev.2, "GENERIC GUIDELINES FOR DEVELOPING IMO GOAL-BASED STANDARDS"

[14] MSC 107/WP.9," DEVELOPMENT OF A GOAL-BASED INSTRUMENT FOR MARITIME AUTONOMOUS SURFACE SHIPS (MASS) "

References

[15] MSC-FAL.1/Circ.3/Rev.2," GUIDELINES ON MARITIME CYBER RISK MANAGEMENT"

[16] https://insidegnss.com/reports-of-mass-gps-spoofing-attack-in-the-black-sea-strengthen-calls-for-pnt-backup/

[17] https://www.latimes.com/business/la-fi-maersk-cyberattack-20170817-story.html

[18] Wang, J., and S. M. Zhang. "Management of human error in shipping operations." Professional safety 45.10 (2000): 23

[19] Jiang, Wenbo, et al. "Poisoning and evasion attacks against deep learning algorithms in autonomous vehicles." IEEE transactions on vehicular technology 69.4 (2020): 4439-4449.

[20] "Shifting tides, rising ransoms and critical decisions", Thetius, CYBEROWL, HFW

INTERNATIONAL
MARITIME
ORGANIZATION

THANK YOU