The Company of Master Mariners of India

Maritime Cyber Security - The Challenges Ahead

CMMI – Monthly Lecture Meeting
16th Jan 2025

(Delivered by Capt Viraf Chichgar – Fleet Management Training Institute)

Major Marine Attacks - 'Not Petya' !

- 2017 – Global Attack which cost a Global Shipping and Logistic MNC, well **over 300 Million USD,** and associated partners **400 million USD**. Global losses were estimated at **10 Billion USD**.
- Within **10 minutes**, 49000 Computers, 6200 servers, 1200 applications, and all IP-based equipment were unusable. Most of these were rendered obsoleted and destroyed.
- Servers with synched domain controllers were damaged in all countries, leading to **no access** due to the absence of verification and authentication.
- Hundreds of IT professionals and some ***GHANIAN luck**, allowed limp–back restoration after 10 days.
- *(* The Ghana office had a black-out just before the attack and it's system image survived due to luck, as just this one domain server did not sync with the other infected ones)*

A.I DRIVEN CYBER ATTACKS: Attack Surface - Ports

Fun Fact !

The average number of cyber attacks targeting the Port of Los Angeles in 2023 was around 63 million / per month!!

A majority of Cyber Attack attempts are now driven by A.I supported technology.

Vessel NUC; But Under Remote Command !

- Hackers took **'full control'** of container ship's navigation systems **for 10 hours**
- In **February 2017** hackers reportedly took control of the **navigation systems** of a German-owned 8,250 TEU container vessel en-route from Cyprus to Djibouti for 10 hours.
- Suddenly, the captain **could not manoeuvre**, an industry source who did not wish to be identified told *Safety At Sea* (*SAS*). "The OT system of the vessel was completely hacked."
- While details are limited, according to the source, the 10-hour attack was carried out by **'pirates'** who gained full control of the vessel's navigation system, intending to steer it to an area where they **could board and take over**.
- The crew attempted to regain control of the navigation system but had **to bring IT experts on board,** who eventually managed to get them running again after hours of work.

- *Article credit Tanya Blake / Editor Safety at Sea*

CYBER THREAT EXPOSURE – OT AND IT

Information Technology (IT):

The application of science to the processing of data according to programmed instructions in order to derive results.

Operational Technology (OT):

A hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise. It includes devices, sensors, software and associated networking that monitor and control onboard systems.

Source Credit : IR CLASS

CYBER THREAT EXPOSURE – OT AND IT

Information Technology (IT)

- Administration, accounts, crew lists, etc.
- Planned maintenance
- Spares management and requisitioning
- Electronic manuals and certificates
- Permits to work
- Charter party, notice of readiness, etc.

At risk:
Mainly finance and reputation

Operation Technology (OT)

- PLCs, SCADA
- On-board measurement and control
- ECDIS, GPS
- Remote support for engines
- Data loggers
- Engine and cargo control
- Dynamic positioning, etc.

At risk:
Life, property & environment
+
all of the above

Source Credit : DNV

Attack Surface: I.T – Identity theft through Deep Fake

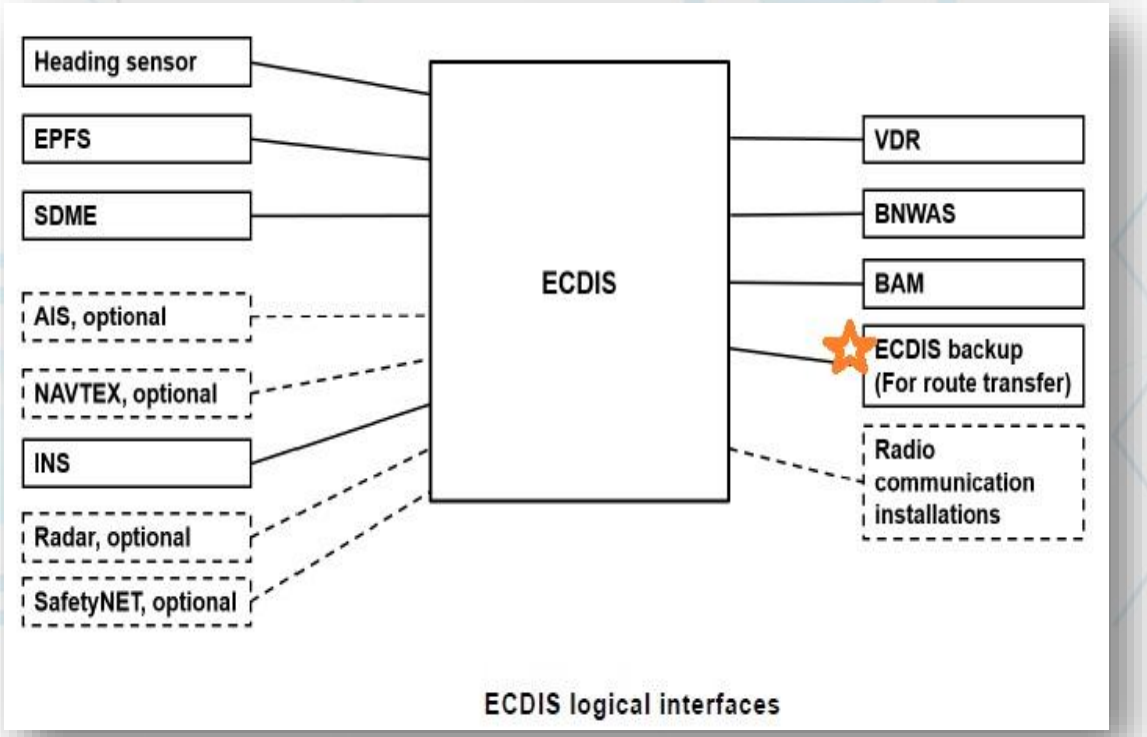
URL : https://training.fleetship.com/documents/CS_Seminar/Deepfake_Singularity.mp4

(Scanning this QR Code or Clicking on the URL will allow you to playback video, which was hosted on a secure site, when this document was created. The ownership of this video belongs / remains with DEIP NEP)

Source Credit : YouTube/DEIP NEP

Attack Surface: O.T - Nautical - ECDIS

It is a prerequisite that the **route plan** has been transferred to the back-up device **prior to the departure** and **after reassignment of the route plan** in order to enable a safe take-over when ECDIS fails.



ECDIS logical interfaces

Source Credit : I.E.C 80/1124/CD

ECDIS – Logical Interfaces

- There are **no IMO or IEC requirements** for a full-time wired interface between main and backup ECDIS.
- The logical interface *(wired or non-wired*) that IEC tests for, is **limited to Route Exchange only.**
- **Despite the above,** ENC *(IHO standards)* and AIO *(Non-IHO standards)* are imported in on a weekly basis, it is routed in from **'vendor/distributor systems'**, typically through the Back of Bridge Computer, through a non-standardized software.
- Typically, two or more ECDIS and the BoB Computer **are being kept in the wired interface**, and **weekly ENCs updates are being synchronized through the wire interface**, despite no requirement
- **Process of weekly updating** has no regulatory guideline – some vessels are updating it **simultaneously,** instead of **staggered** updating, increasing risk of **simultaneous failure of** all ECDIS
- Incase of malware, incompatibility or general errors due to a **large volume of data** being **simultaneously synched** on **aging** computers, **ECDIS machines** are at times hanging or entirely crashing, simultaneously!

ECDIS Cyber Security – the Challenges!

- ***No Annual Service is required****. No software upgrade is required – if your software was good as* ***of 1st Sept 2017****, then you are considered 'good enough'*
- *Some ECDIS models* ***'meeting current requirements'*** *were OUT of MANUFACTURE in* ***2012 !***
- *No regulation compelling* ***'staggered updating of ENCs in multiple ECDIS'***
- No regulation requiring any standard for **the BoB – Back of Bridge Software.**
- **MIOS – third party** like SPOS and Guide to Port Entry can be overlaid and can cause glitches**.**
- **'AIR – GAPS' :** The Catch 22 Situation
- **IMO** is yet to develop guidance to establish a framework for **data distribution and global Internet Protocol (IP)-based** connectivity to realize the full potential **of S-100 capable ECDIS**

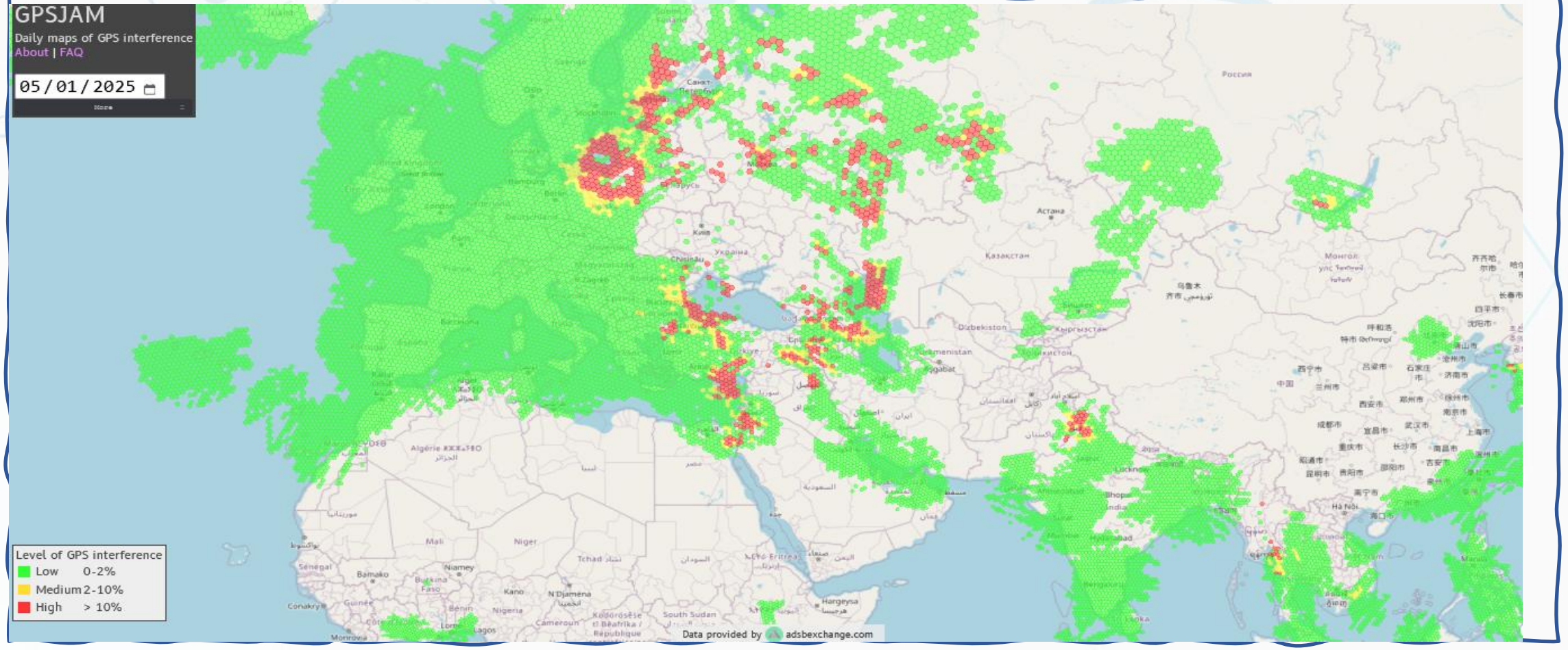
Attack Surface: O.T – Machinery: *A.I Based 'On-top' Propulsion Optimizer*

- An **A.I based 'on-top'** unit which controls **R.P.M** as well as **Pitch** of C.P.P propellors.
- Load on engine/propulsion is monitored, then fed through a cloud connection and via **IoT, adjustment commands** are given back to the system.
- Same is already being fitted on merchant vessels, to **improve emissions**.

Concerns:

- No **quality or regulatory standards** are available on maker's website or over email query.
- While services are marketed by a Scandinavian company**, servers could be elsewhere.**
- No information **on Cybersecurity standards is available** on website or over email query.
- Fitment was done with minimal MoC. The above certification status was unknown.
- No **S.O.P drafted** to monitor, control or specific situations or contingency procedures as to when and how to override commands.
- Essentially, **propulsion control is provided external to the vessel**, and MoC / RA is done retrospectively.

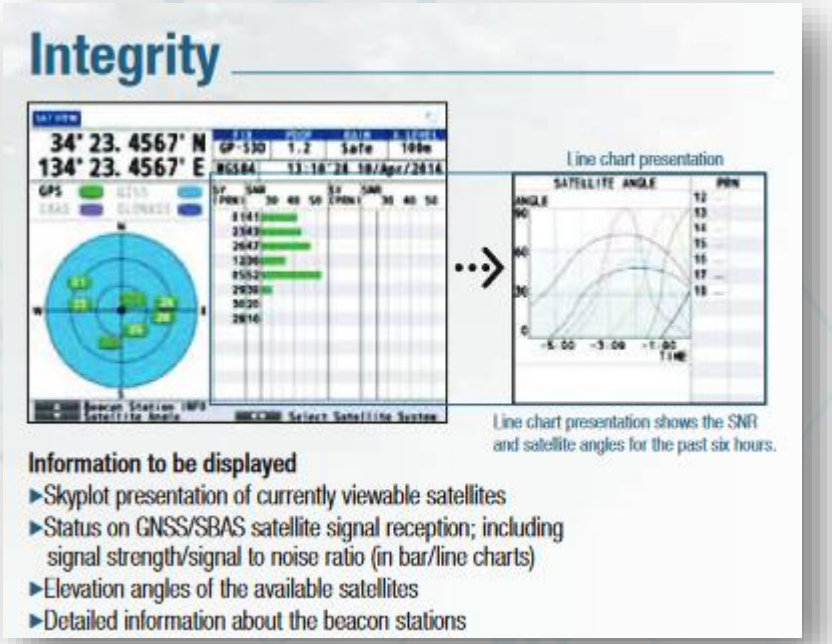
Attack Surface: External systems– GPS SPOOFING AND JAMMING



Source Credit :www.gpsjam.org

Attack Surface: External systems– GPS SPOOFING AND JAMMING

- **Jamming causes the GPS receiver to DIE,**
- **Spoofing causes the GPS receiver to LIE!**



Mitigating measures available:

1) **Anti-Spoofing / Anti-Jamming equipment on the ship.**
2) **Using Multi-Frequency / Multi- constellation receivers.**
3) **Traditional methods of GPS position verification – terrestrial fixes.**

Source Credit : Screenshot from www.furuno.com

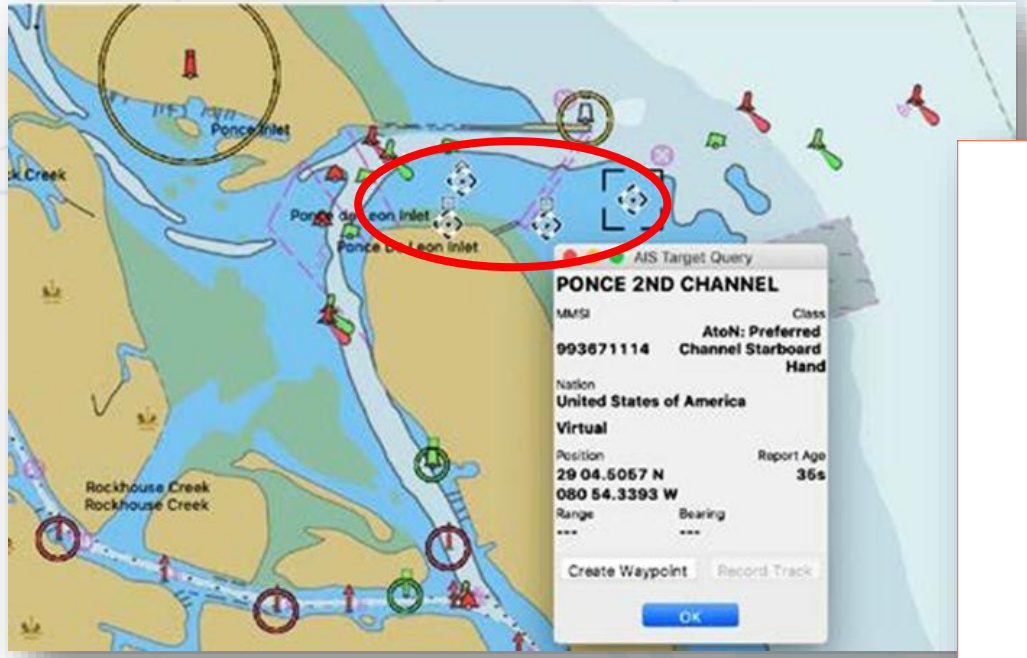
Attack Surface: External - AIS SPOOFING

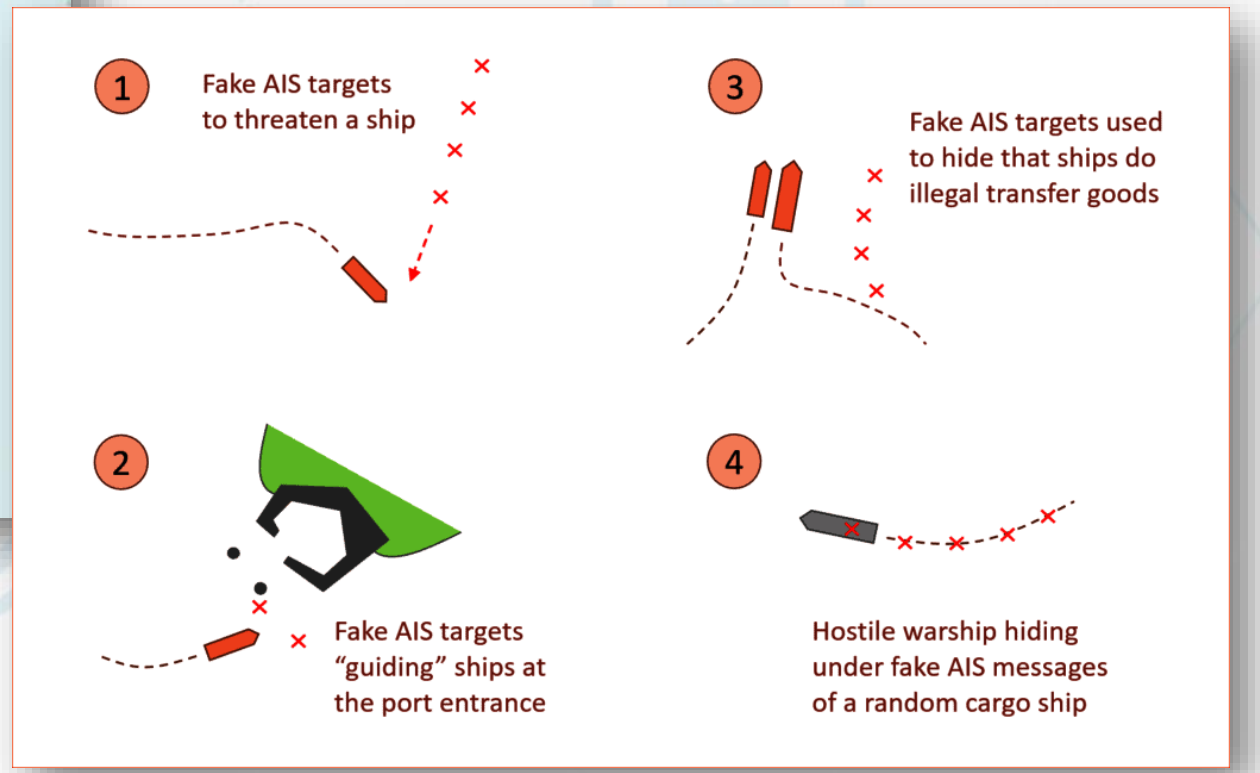
Challenges with AIS

- Lack of validity checks: No geographic validation information meaning that it is possible for a bad actor to send an AIS message from any location while purporting to be in another location.
- Lack of timing checks: AIS messages contain no time stamp verification information meaning that a cyber-attacker can replay valid AIS information at a later time of their choosing.
- Lack of authentication: The AIS protocol provides no mechanism to authenticate the sender, thus anyone with the ability transmit an AIS packet can impersonate any other AIS device.
- Lack of integrity checks: AIS messages are transmitted in an unencrypted and unsigned form; this makes it simple for an interloper to intercept and/or modify transmissions

Source Credit : Gary Kessler Associates

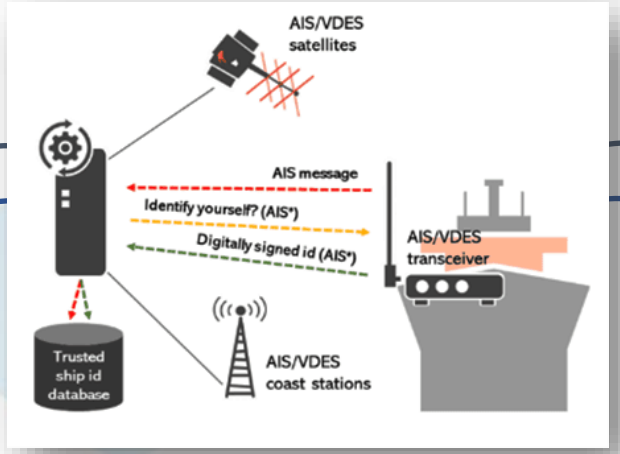
AIS SPOOFFED: FALSE – TARGET & AtoN CHANNEL





Source Credit : STERNULA AS/ Gary Kessler Associates

AIS Spoofing – Mitigating Measures

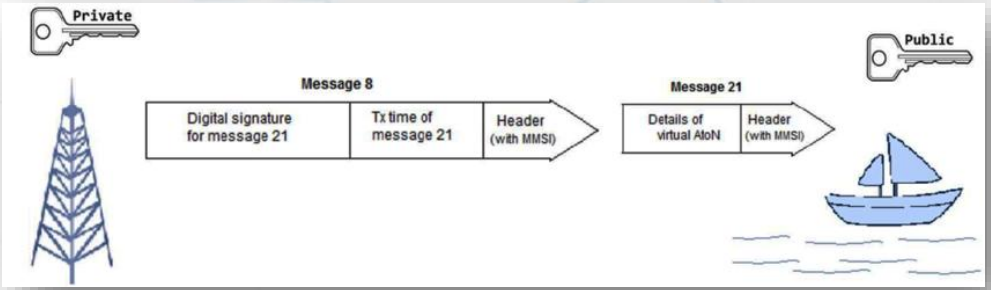


Mitigating measures planned:

- MSC 109 approved a revision of the performance standards (AIS) (Resolution MSC.74(69)) to prevent tampering of a ship's information.
- IMO's Sub-Committee on Navigation, Communications, Search and Rescue are proposing amendments to Chapter V/19.2.4 and finalizing of performance standards for VDES will in NCSR 12 in May 2025
- VDES is a digital communication system that operates over the very high frequency (VHF) band to provide secure and reliable data exchange. *(IALA is also working on Guidelines for VDES).*

- **VDES – VHF Data Exchange Scheme** includes 4 components:

1. Automatic identification system (AIS)
2. Application specific message (ASM)
3. Terrestrial component for VHF data exchange (VDE-TER)
4. Satellite component for VHF data exchange (VDE-SAT)



Source Credit : IALA / IMO – MSC & NCSR / STERNULA AS

Challenges for the Industry..... *01*

- **Aging assets / Aging OT - never designed to work without Air Gaps. Equipment was not designed to be coupled with internet and software is almost never upgraded.**
- **Cyber Security is a newer concept for ships; it's expensive and there is lack of investment.**
- **Cyber Experts are good at IT protection; are not that familiar with ship OT protection.**
- **IT used in shore-based PMS and Accounting system is antiquated.**
- **Internet provided onboard is the 'cheapest' and may not be the most secure.**

Challenges for the Industry……. *02*

- **Navigation / communication / cargo /ballast / propulsion / steering / emission control all are poorly protected OT, in current standards**
- **State-sponsored IT attackers and Hacktivist have increased.**
- **Russia-Ukraine conflict, Iran, Taiwan, China and similar geo-political tensions have raised the ante for cyber-terrorism.**
- **Ransomware is not just profitable but easier to execute, thanks to Bitcoin and Cryptocurrencies.**
- **Cyber awareness and Cyber Security Training are insufficient and not mandatory.**

Challenges for the Industry……. *03*

- **While cyber risk insurers MAY now provide cover for business, interruption arising from an IT system failure, policies, generally exclude bodily injury and property damage – even loss of use in some instances.**

- **Clause CL380, which has been inserted into the majority of marine policies since 2003, removes cover for the use of IT systems as a means of inflicting harm. This exclusion removes all cover for a cyber-attack leaving a client completely uninsured, including any associated business interruption loss.**

Insurance Coverage

	Coverage										
Participant	CL380 buyback	Hull Physical Damage	Vessel Loss of Hire	Hull War **	Ports & Terminals	Defence & Remediation	Data Loss & Recovery	Crime	Business Interruption	Terrorism	Comment
A		-	-	-	-	-	Y	-		-	No take up, coverage too narrow
B		-	-	-	-	Y	-	Y		-	No take up too narrow
C	Y										Low take up; Aggregate limit across all insureds
D				Y							Limited to "war" only
E								Y			$1m only as part of their War K&R product
F	Y			Y		Y	Y	Y	Y	Y	Cover available, but not together. (SME focused)
G		Y	Y			Y	Y	Y			The leading credible proposition
H	Y			Y		Y	Y	Y		Y	Cover available, but not together. (SME focused)
ASTAARA	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	

** Limited to capture seizure arrest restraint or detainment, and the consequences thereof or any attempt thereat and / or confiscation or expropriation.

Source Credit : WEST – PandI

Reference material for today's session.

https://training.fleetship.com/documents/CS_Seminar/Reference_Documents.zip

(Scanning this QR Code or Clicking on the URL will allow you to download a zipped folder which contains PDF files with reference documents which was hosted on a secure site, when this document was created. The source credit / ownership for these documents are indicated in individual documents and may be redundant or replaced by individual owner, in the future)

Index Reference regulations, documents and regulations:

1. IACS UR-E26-Rev.1-Nov-2023-Cyber Resilience of Ships
2. IACS UR-E27-Rev.1-Sep-2023-Cyber Resilience of Onboard Systems and equipment
3. IACS Recomm. 171-1 Incorporating Cyber Risk Management into SMS
4. IACS UR-E26 / E27 – Summary by INMARSAT and CLASS NK
5. Class NK Cyber Security Management System for Ships
6. IR Class Guidelines on Maritime Cyber Security
7. DNV Maritime Cybersecurity Priority 2024/25
8. International Association of Ports and Harbours - Cybersecurity-Guidelines
9. MSC 98 Resolution (428) Maritime Cyber Security in SMS

Reference regulations, documents and regulations:

10. MSC 104-FAL.1-Circ.3-Rev.2 - Guidelines on Maritime Cyber Risk Management
11. MSC 108-06-FAL.1 Circ. 3- Proposed Revision to Rev.2 Guidelines on Maritime Cyber Risk-Management
12. MSC 108-100 Proposed modifications to the draft amendments to the STCW Code
13. MSC 109-19-3 Proposal for a new output to realize the full potential of the S-100 ECDIS
14. FAL 47 Circ.42-Rev.3 Guidelines for setting up Maritime Single Window
15. FAL 49 Agenda for Meeting of 100325
16. IALA Guidance 1117-Ed3.0-VHF-Data-Exchange-System-VDES.
17. State of AI in Cyber Security – by Dark Trace
18. The Guideline on Cyber Security on board ships – Ver.5.0 (Industry)

Tools that may help

- **IMO, IACS, CLASS, BIMCO, OCIMF, INTERTANKO, INTERTANKO, IALA, IAPH.**

  IEC, ISO , NIST – all provide a lot of guidance on the subject.

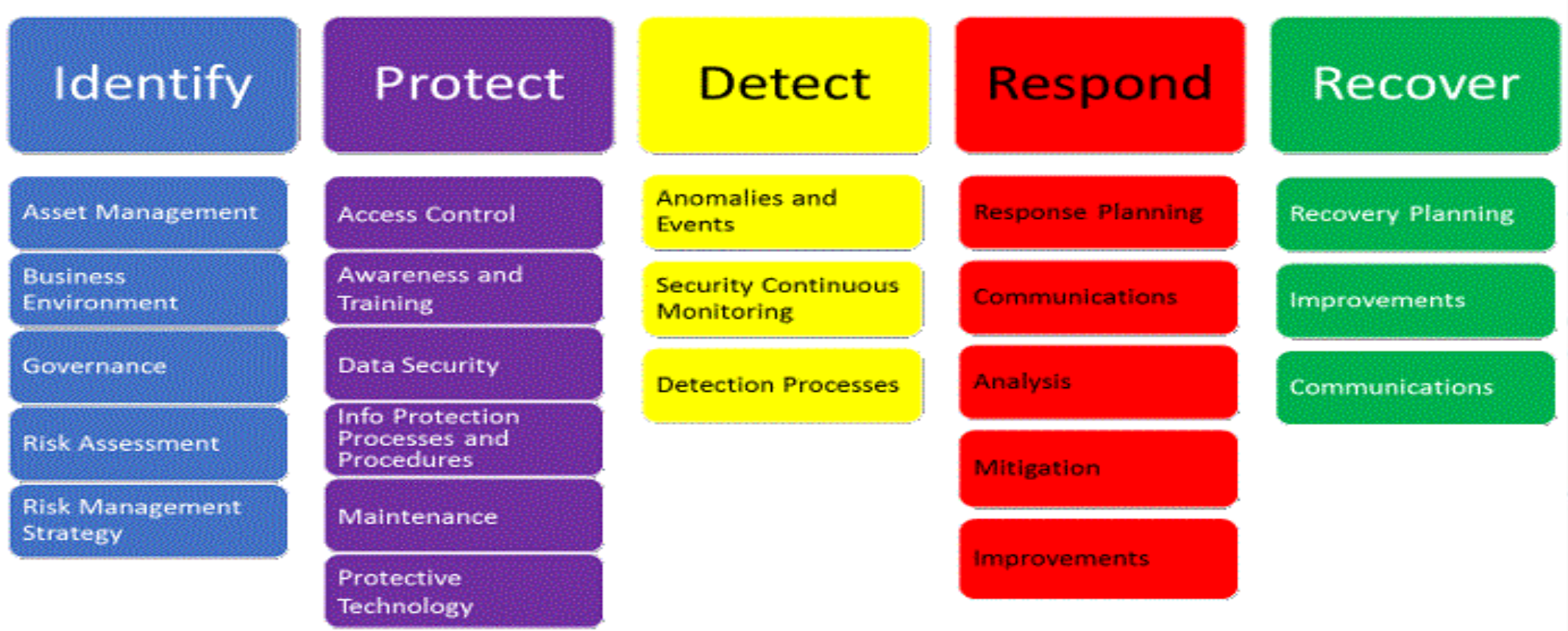
- **Strong shore-based IT team, focussed on both IT and OT.**
- **Regular updates to OT and IT software.**
- **Investing in strong cybersecurity tools / software.**
- **AI based software to strengthen Cyber Resilience *(like Darktrace)***
- **Having IT /OT System Audits by qualified third party – C.I.S.A or by Class**

Tools that may help

- **Keeping proper/safe back-ups and recovery systems.**
- **Considering double-redundancy with lesser automated back-ups.**
- **Having a strong Cyber Resilience policy and culture in your organisation.**
- **Have regular cyber-awareness and training programmes.**
- **Insist on a large budget allocation towards Cybersecurity–**

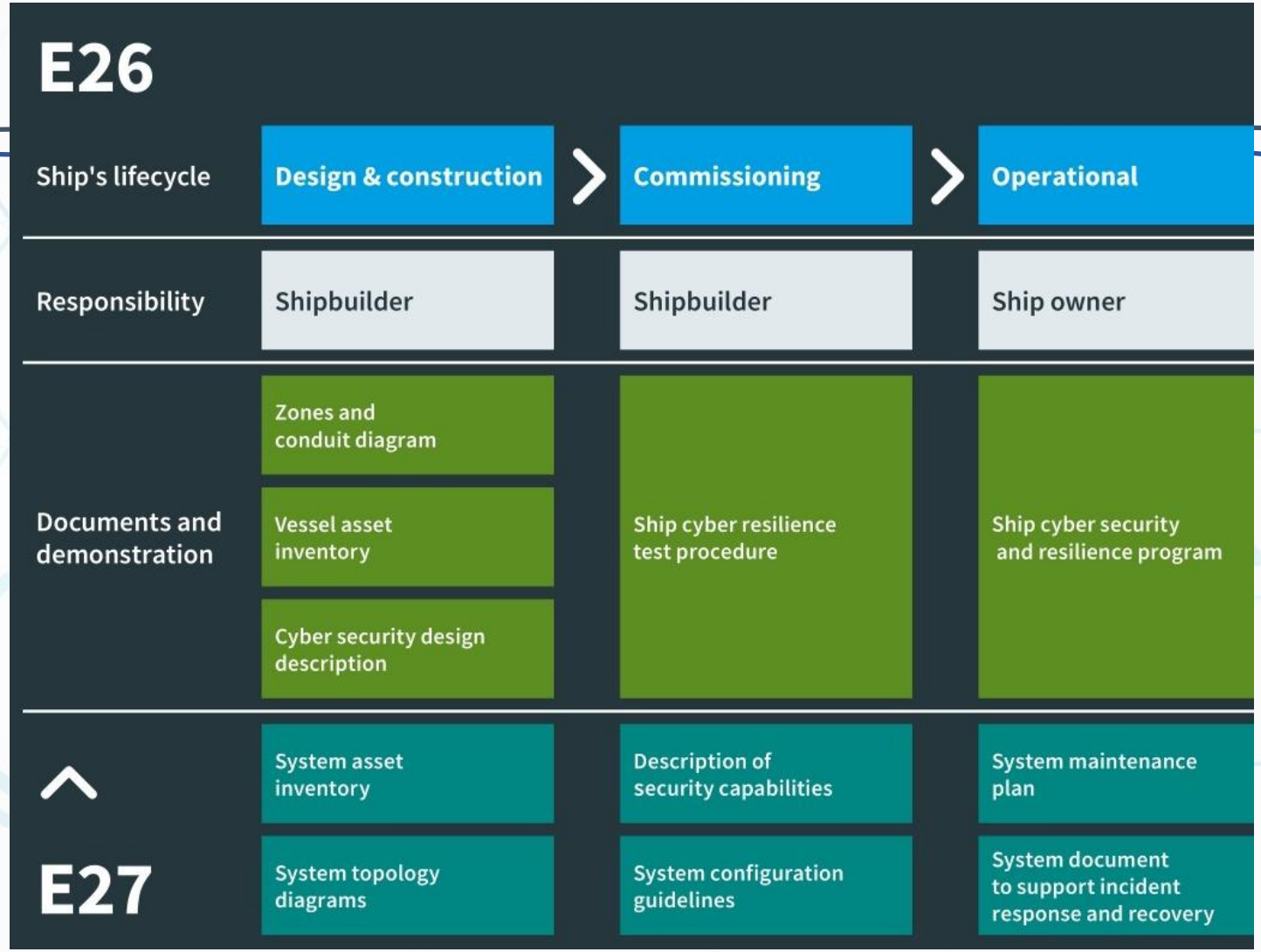
  it's a NECESSARY AND UNAVOIDABLE INVESTMENT

5 Sub Goals of Cyber Security



Source Credit : National Institute of Standards of Technology

Typical Class Survey responsibilities



Source Credit : INMARSAT / Class NK

And if you feel safe, please remember that these establishments got hacked by a 15-year-old!!