Why Maritime Cyber-security?
Dr Kimberly Tam

CyberMAR: Cyber preparedness actions for a holistic approach and awareness raising in the MARitime logistics supply chain

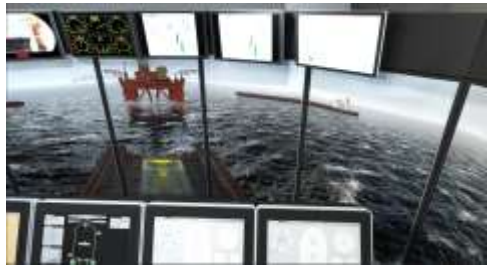
28th March 2023

The University of Plymouth

- The first and largest Marine Institute in UK, with over 3000 staff and students looking at the Ocean
- Three-time winner of the Queen's Anniversary Prize for Higher and Further Education, UK Top 25 for Teaching Quality & World Top 25 for Research Citations
- 1st in the world for research towards SDG 14 (Life Below Water), Times Higher Education 2021

Maritime, a key strength of the University

- More than 3,500 wind turbines off the Cornish coast by 2050
- Big increases in aquaculture
- Supported by a plethora of specialist support vessels
- Navigation Suite upgrade to a Nationally leading facility incorporating Class 3, full-mission DP Simulator (£600k investment)
- Growing fleet of marine autonomous assets and planned to Control Centre upgrade
- Leading on SDG 14 to ensure safe and efficient future for maritime operations
- Globally leading lab on Maritime Cyber Security (£3.2m investment in Cyber-SHIP)
- And then our lead on SDG 14, puts the University in a leading Thought Leadership position for all aspects of future Maritime operations in the Ocean Economy



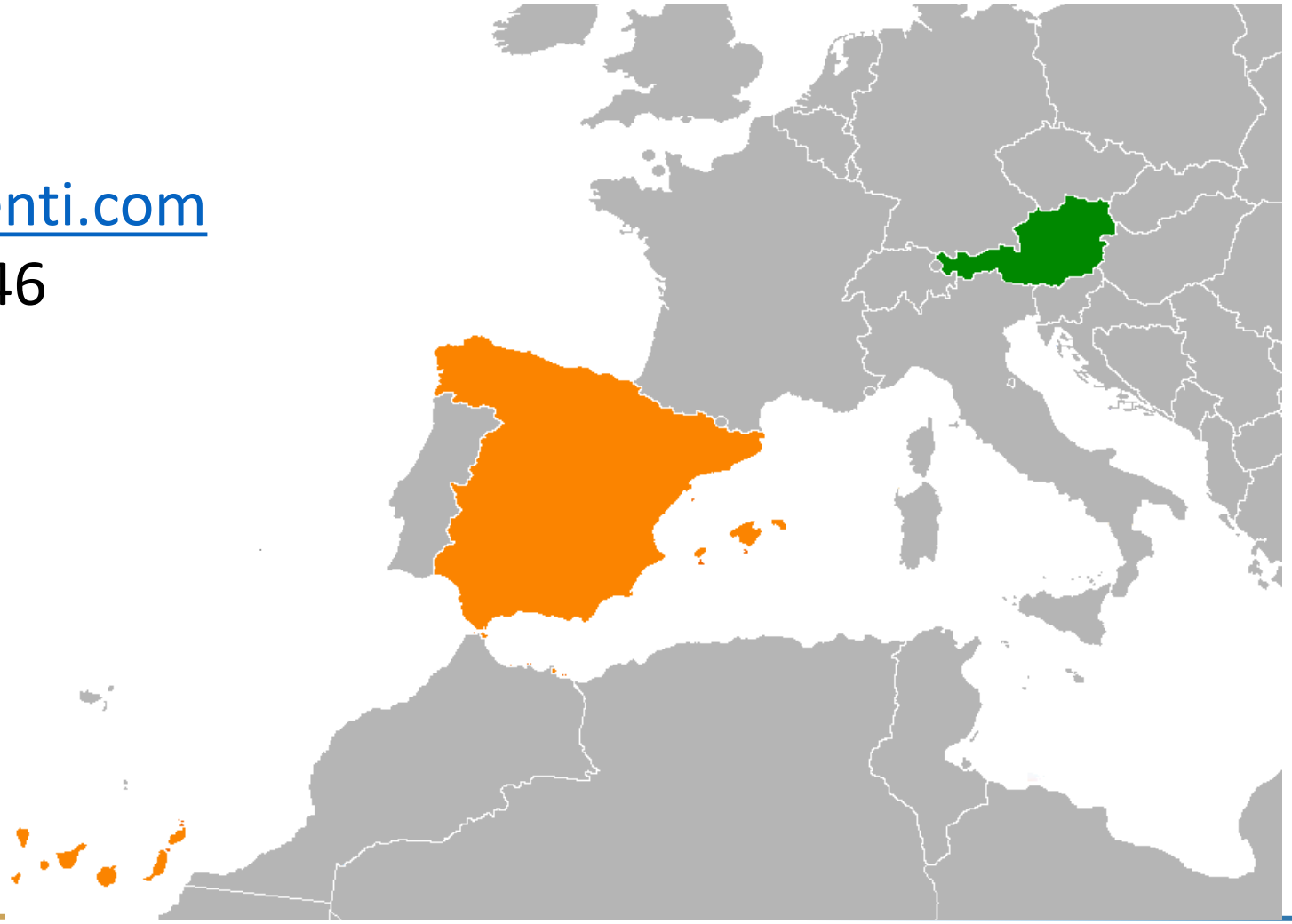
Cyber-SHIP Lab
SECURING MARITIME

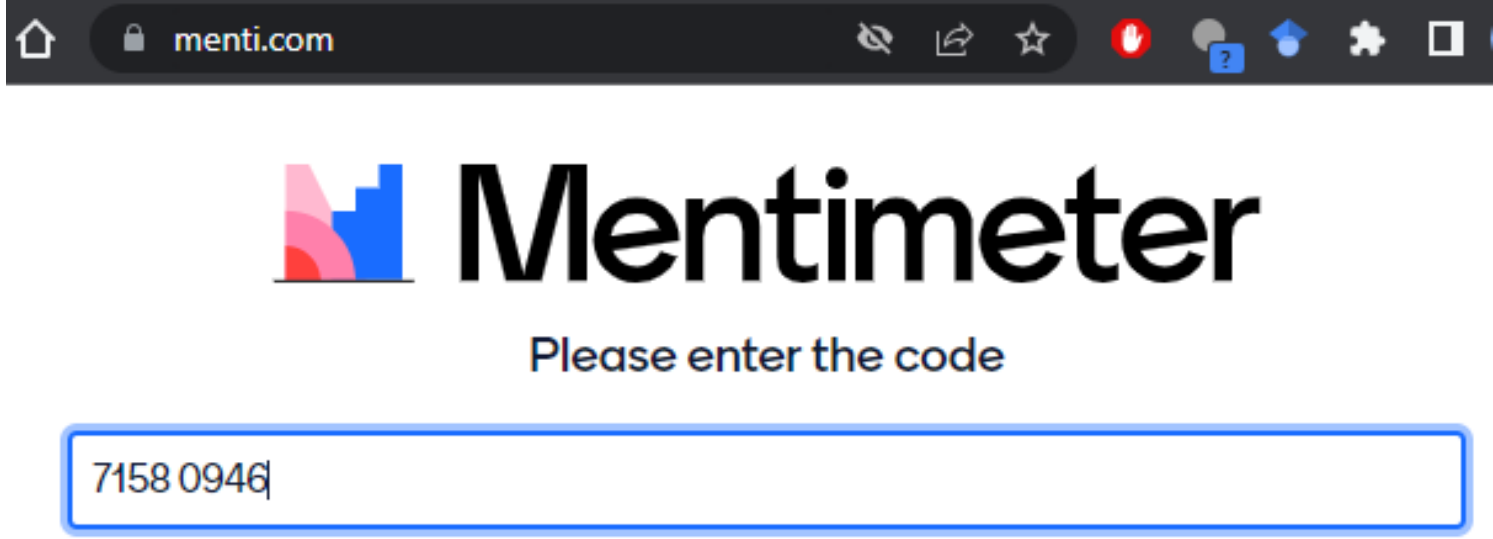
Does this matter to Austria?

Let's look at Port of Valencia in Spain

www.menti.com

7158 0946





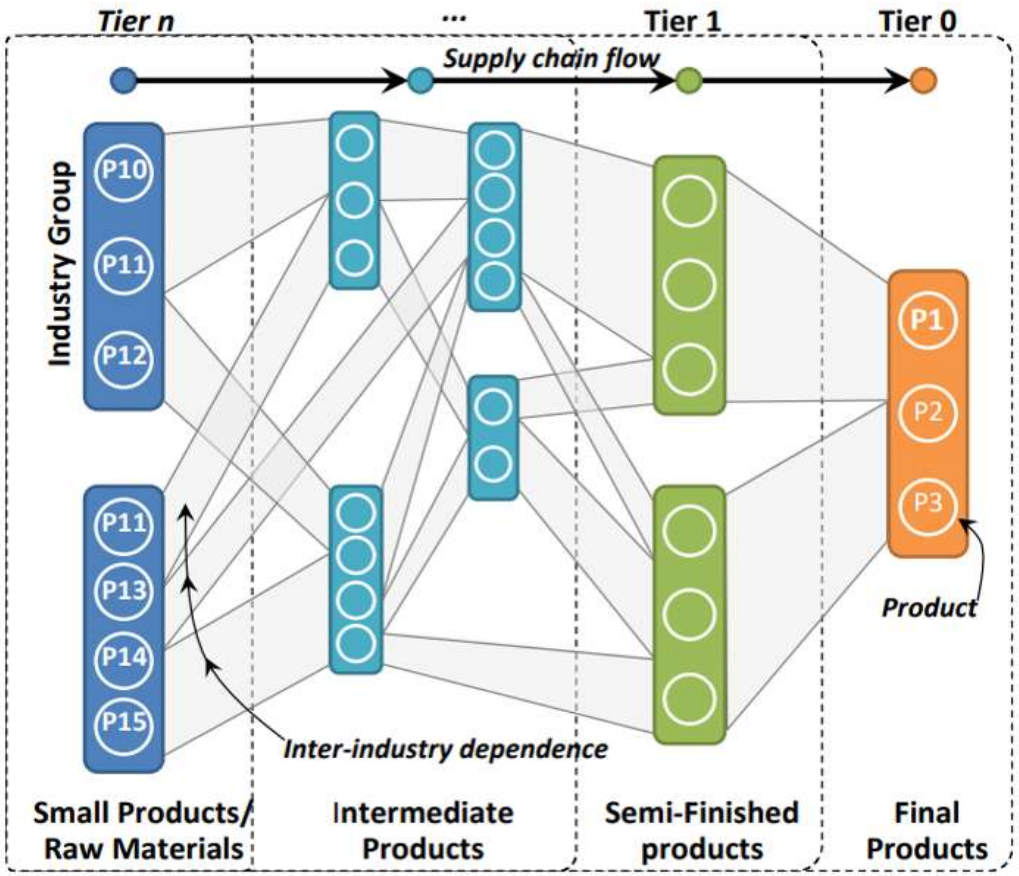
Calculating Econometric Loss

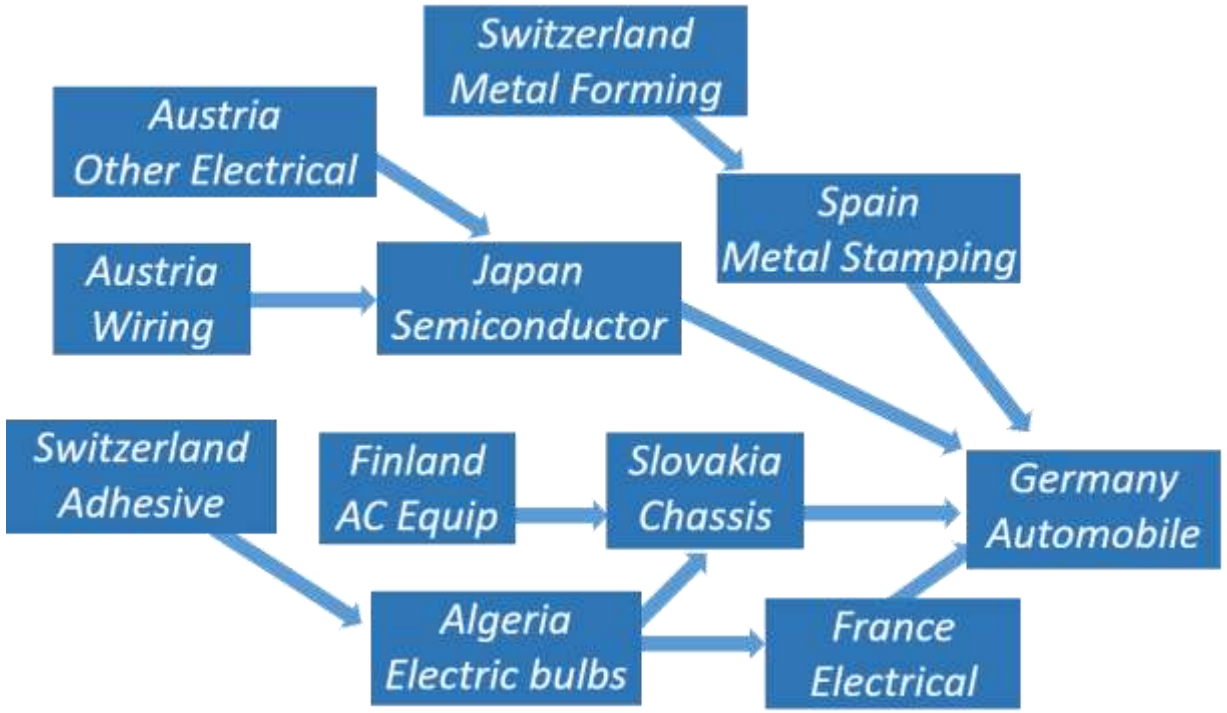
(from a seaport cyber-physical attack)

Study

- This study considers cyber-attacks as an external disruption to the supply chain, with attacks executed either by a third party or potentially executed by insider threats.
- The cyber-triggered disruptions can interrupt the production of raw materials or intermediate products depending on how and which system is compromised.
- Understand the disruption in the global supply network caused by a cyber-physical event by using a maritime-based case study with real data.
- Understand people's perception of maritime cyber threats using understanding of econometric loss

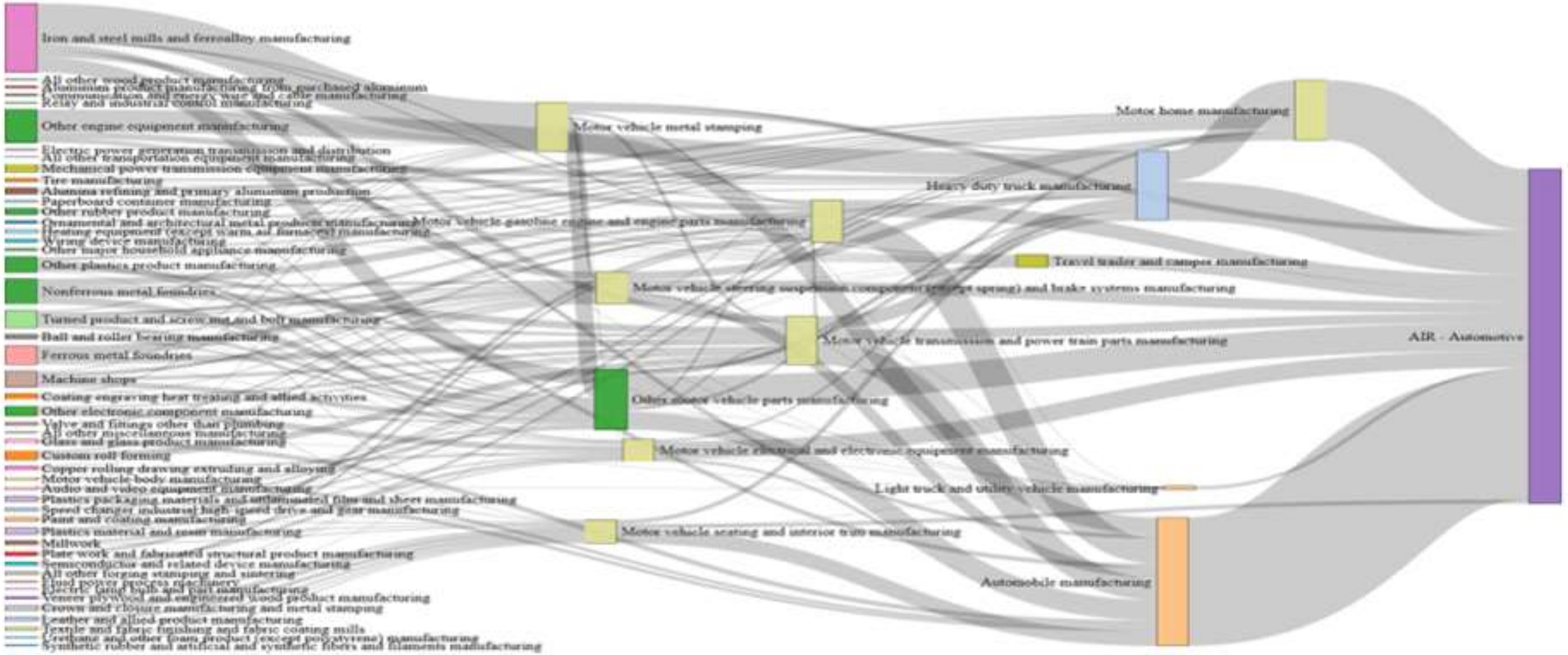
Modelling the Supply Chain





Examples of product dependencies [**(A)** on left] and trade networks [**(B)** on the right]

(product dependencies)



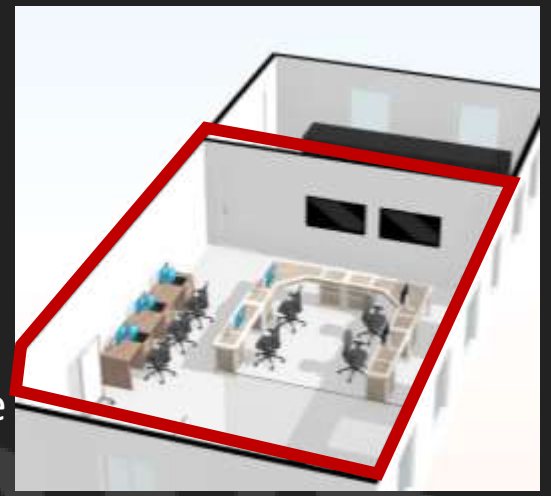
Introduction to Port of Valencia, Spain

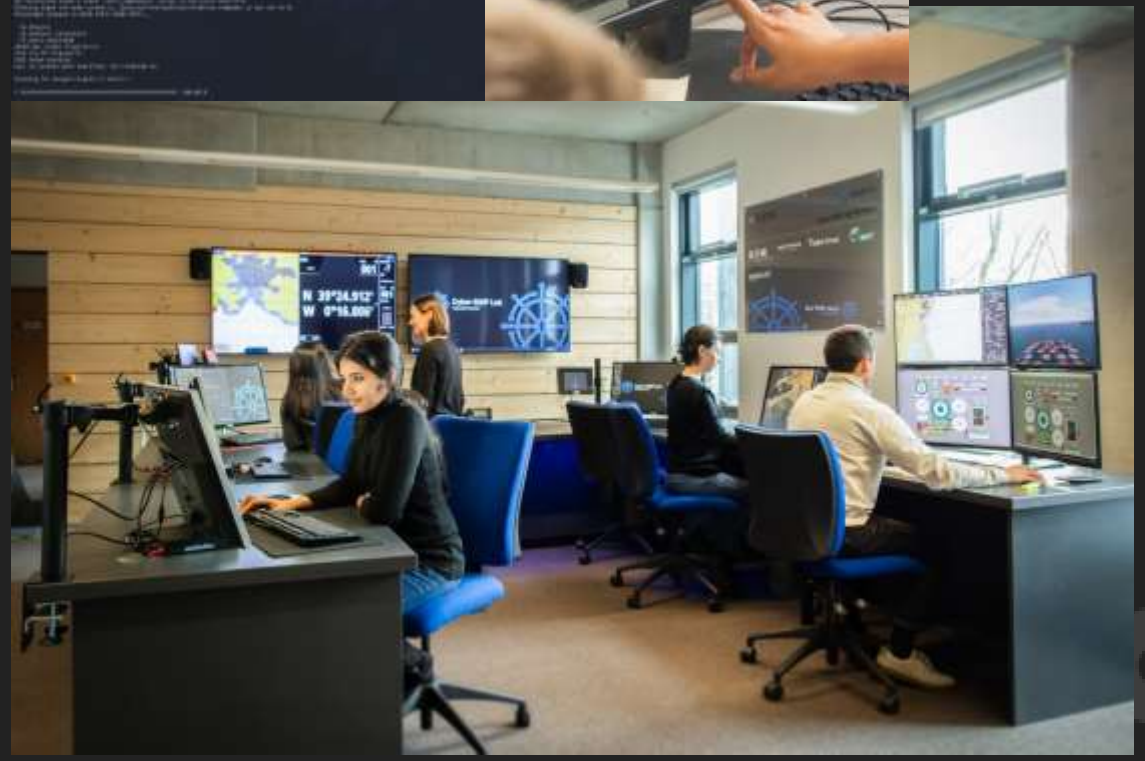
Testbed and cyber-rages

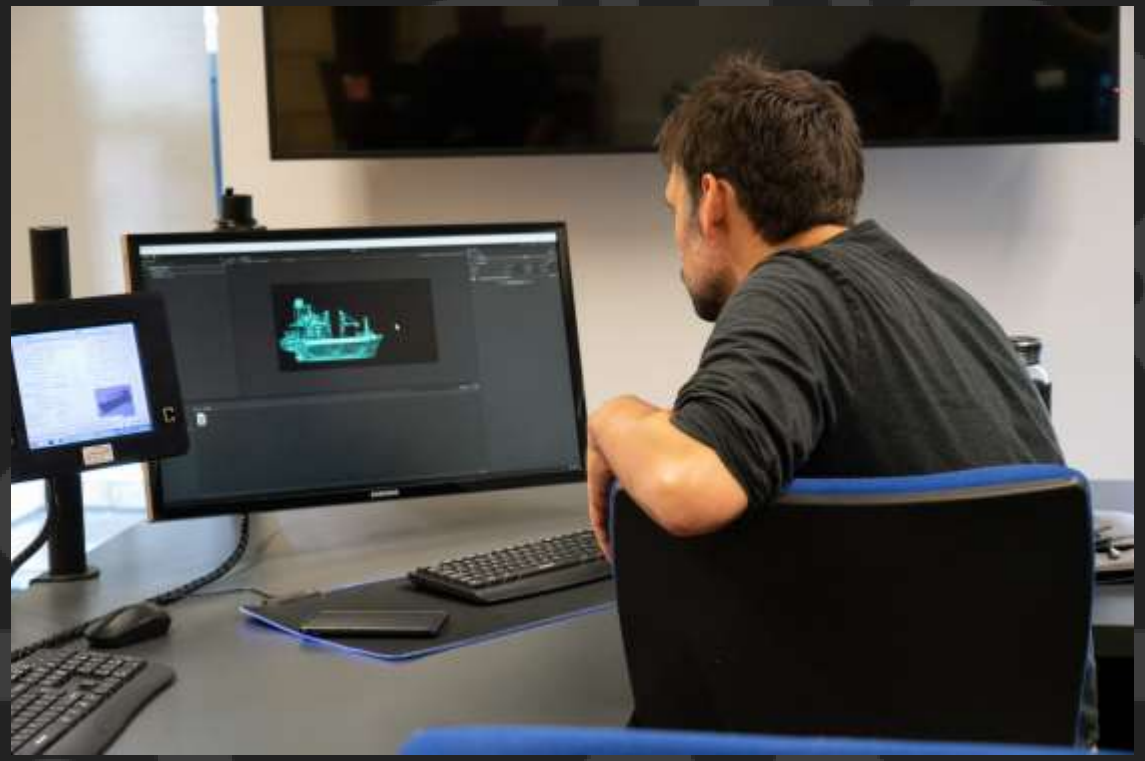
University of Plymouth

The Cyber-SHIP Console Room

Visualisation of data
Physical hardware visualisation of attacks
Pen-testing
Research Project development
Development of custom electronics and software
Teaching/training







UNIVERSITY OF PLYMOUTH


NMEA2000/0183
Devices

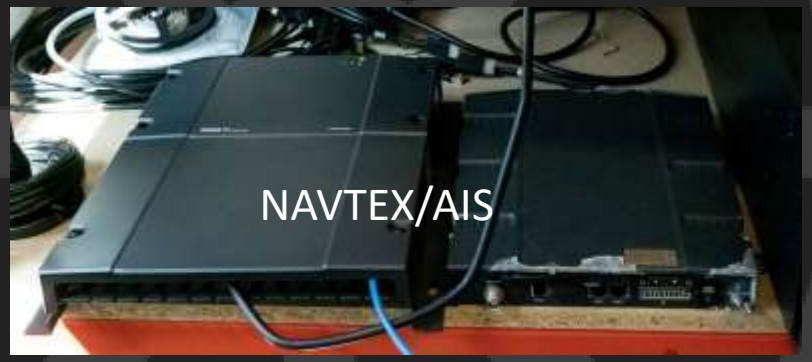

Serial- IP converters


Serial- IP converters
HENSOLDT

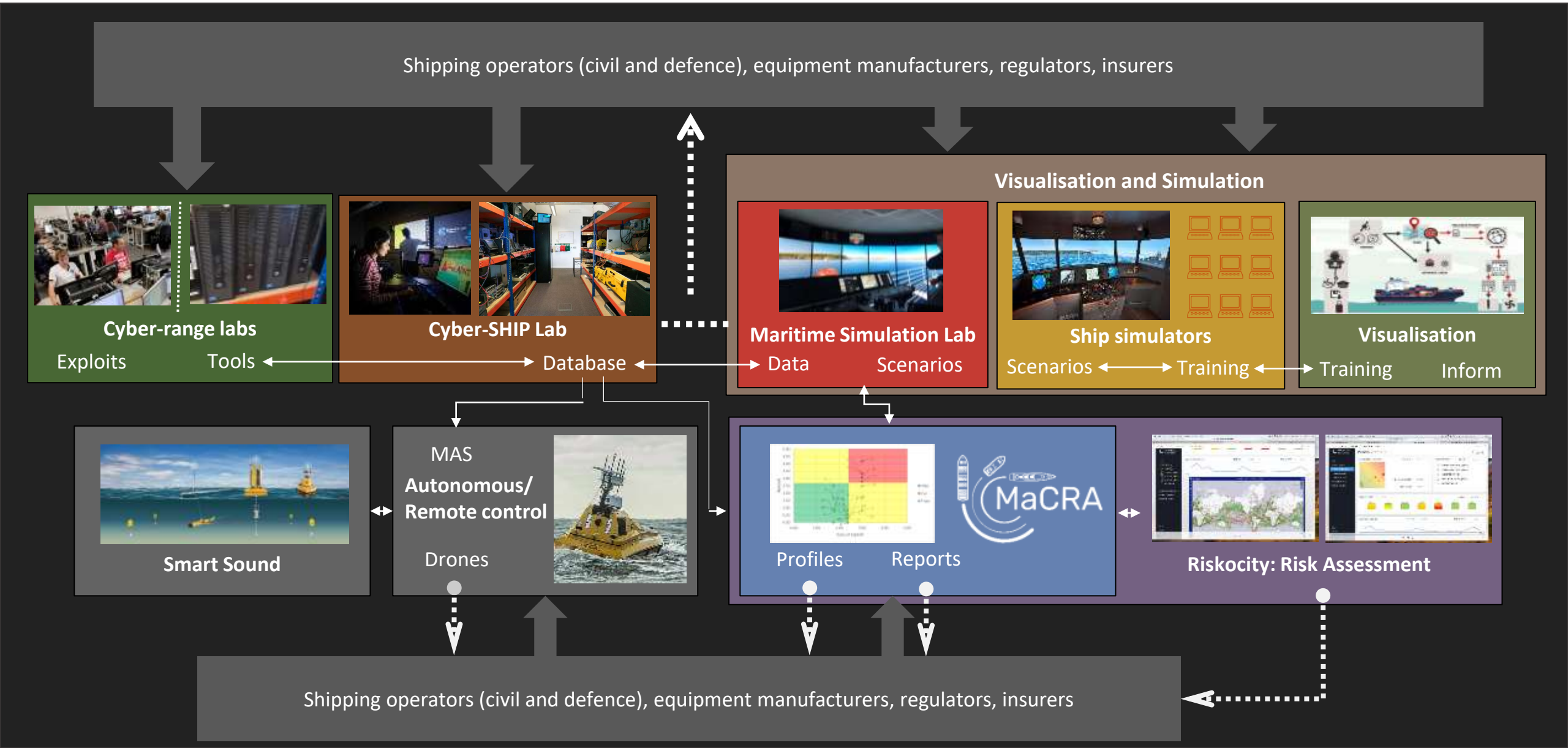

Data recovery from
ECDIS


AIS


SatCom


NAVTEX/AIS

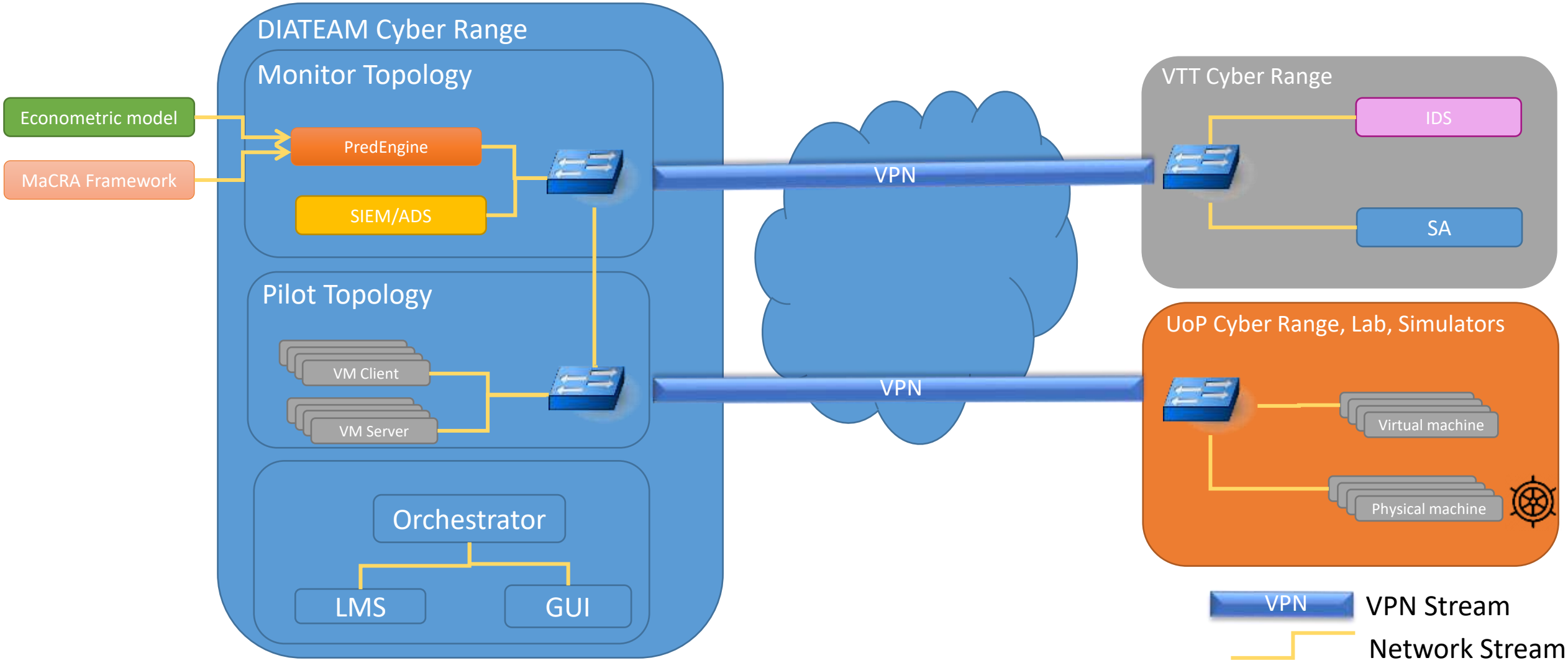
The Plymouth “ecosystem”



The Scenario for today’s discussion

Port of Valencia

Cyber Range Architecture – Connected Capabilities



Introduction to Port of Valencia

- Handling over 6 million tonnes of cargo a year
- Important regional hub for transhipment

- Handles a wide variety of cargo:
  - liquid bulk
  - dry bulk
  - containerised cargo and
  - vehicular traffic

Port Of Valencia

Overview Of Scenario

The vessel scenario that is considered in today's pilot constitutes a scenario where an attacker launches an attack that allows them to temporarily alter the course of a large container vessel and in so doing cause a blockage on the approach channel.

Progression of Attack can be broken down into a number of stages:

- Downloading and Propagation of Attack (Within IT Infrastructure)
- Installing and Initiating the Attack on Vessel Control Systems
- Attack realisation and crew response

Setting the Scene - Introduction of Ship Model

Large Container Vessel

Length	397 m (1,302 ft 6 in)
Beam	56 m (183 ft 9 in)
Draught	16.02 m (52 ft 7 in)
Depth	30 m (98 ft 5 in) (deck edge to keel)
Speed	25.5 knots (47.2 km/h; 29.3 mph)
Capacity	•14,770+ TEU

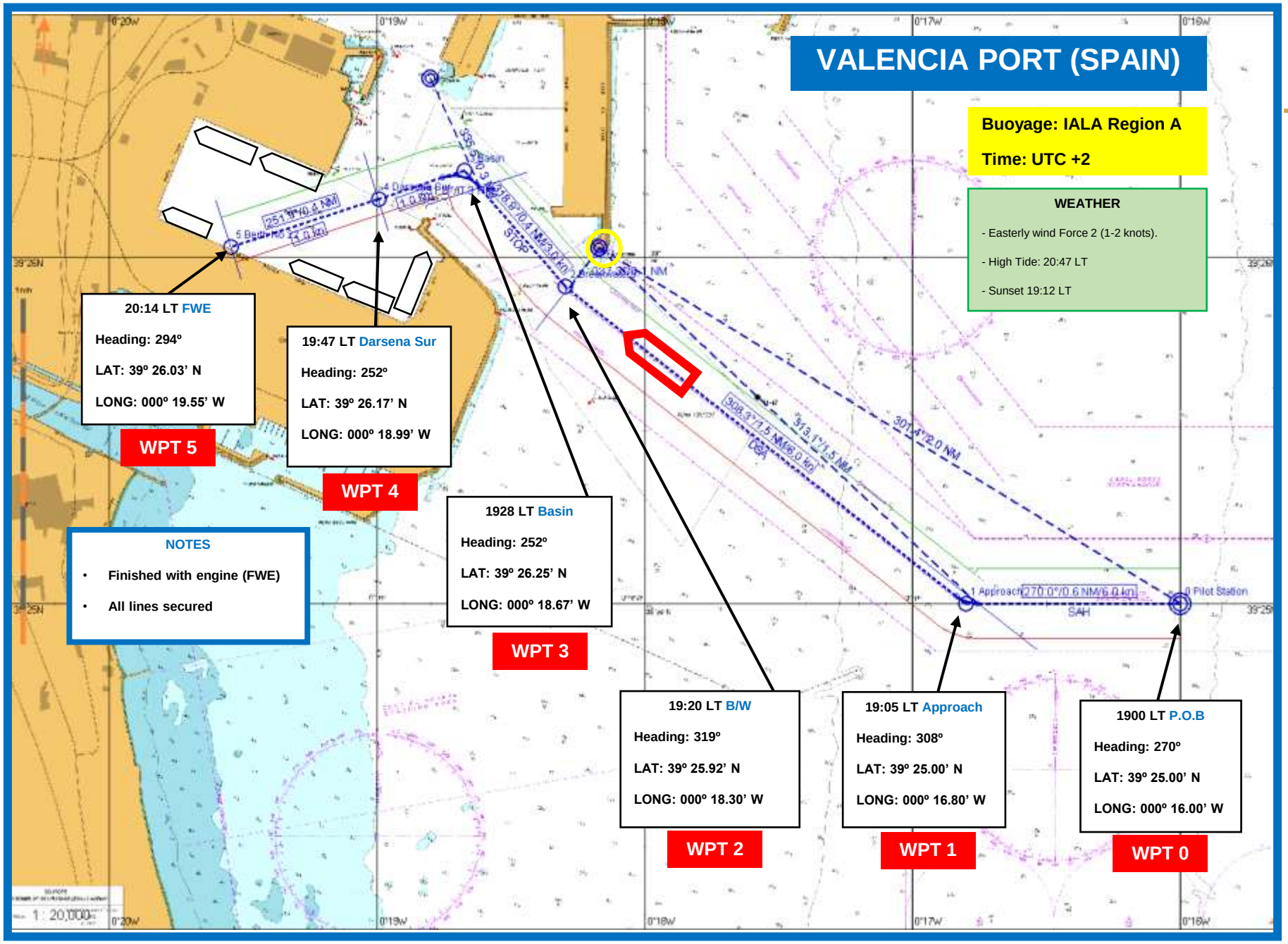
VALENCIA PORT (SPAIN)

Buoyage: IALA Region A

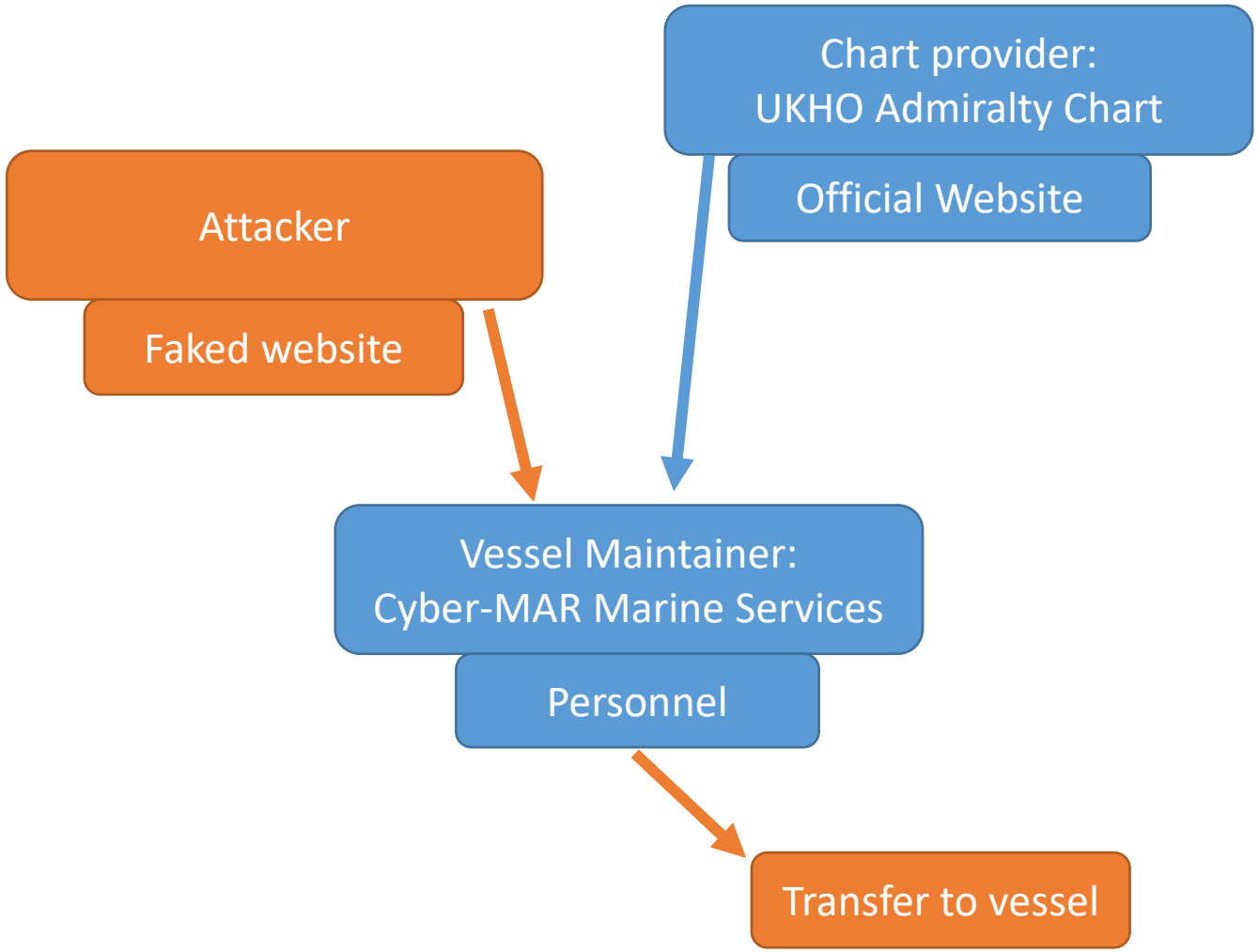
Time: UTC +2

WEATHER

- Easterly wind Force 2 (1-2 knots).
- High Tide: 20:47 LT
- Sunset 19:12 LT



Bridging the “Air-Gap”



Social Engineering – The Email

URGENT: Electronic Chart Update Inbox x

tech-support <tech-support-csl@protonmail.com>
to me

Hi Sir/Madam,

Please find below a forwarded email from UKHO regarding an urgent chart update. This update is mandatory to be installed before entering the port of New York. If any questions or concerns reply to this email.

Best regards,
Tech support team

——— Original Message ———
On Wednesday, September 13th, 2022 at 02:50 PM, ukho <customerservices@ukho.co.uk> wrote

UKHO

Electronic Chart Alert - URGENT

UKHO

Electronic Chart Alert - URGENT

Date: 13/09/2022
Subject: Critical update to Electronic Charts

Dear user,

This is to advise you that there is an important chart update available for the following ENCs.

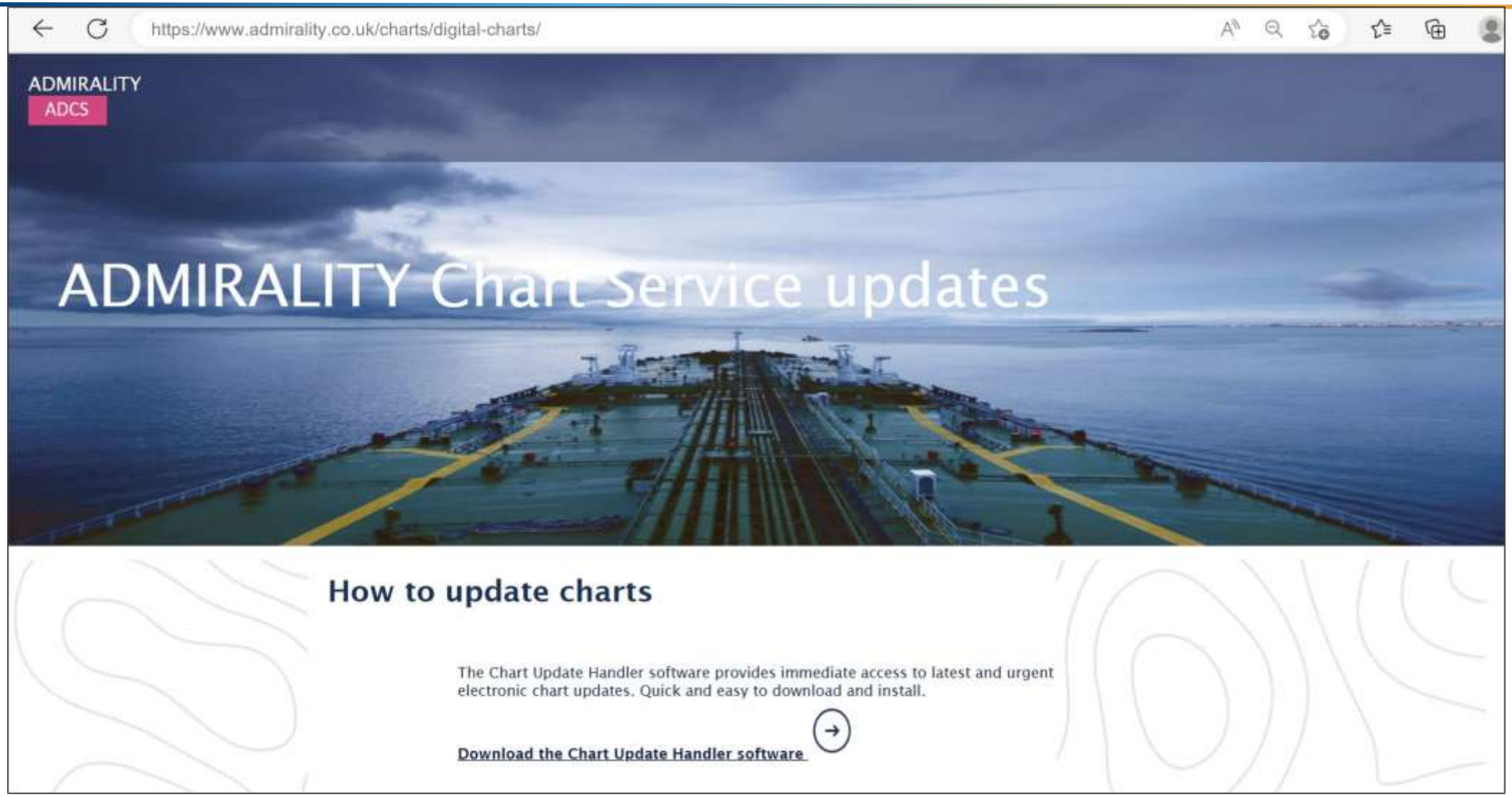
- US5NYCCE - Kill Van Kull
- US5NYCCF - New York Lower B. Northern Part
- US5NYCDE - Passaic and Hackensack Rivers
- US5NYCDF - Hudson R. Hackensack Rivers
- ES504811 - Valencia Harbour
- GB503028 - Harwich and Felixstowe
- GB403024 - Appr Felixstowe, Harwich and Ipswich

We strongly urge you to notify all customers to update the charts before entering the areas covered by the updates. Please note Authority of Port of New York and New Jersey has published an alert notifying the updates. Find the download and update instructions below:

Download and update information:

- Go to chart update website
- Download the chart update handler zip file
- Extract the zip file and transfer to the ECDIS
- Open the Chart Handler software and start updating
- Wait till the update is finished and close the window

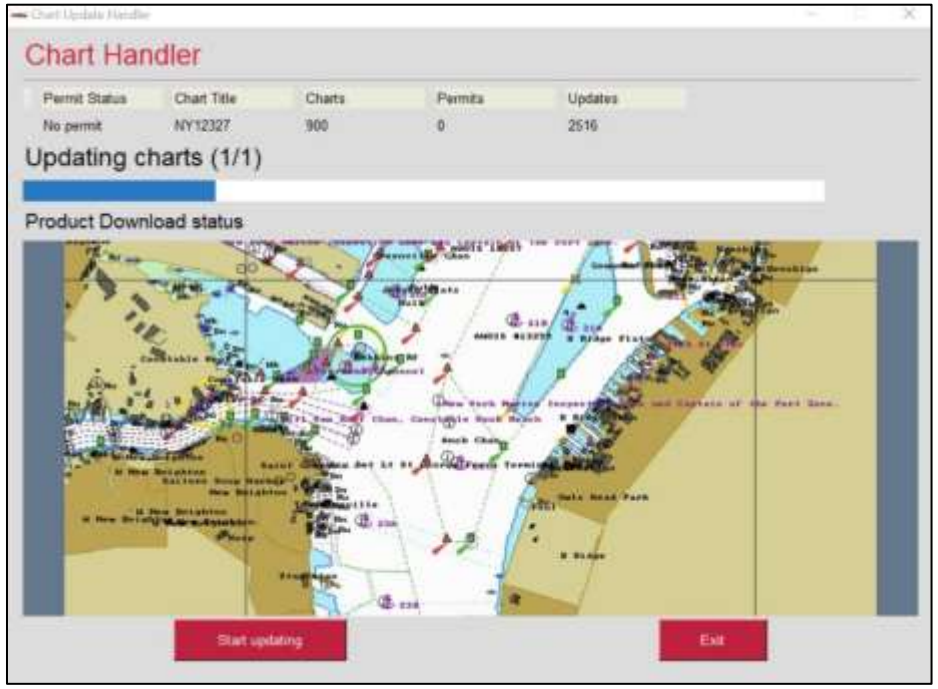
Social Engineering – The Website



The Attack - Overview

- On extraction, and running of software malware is installed on the device constantly looking for the geolocation trigger

- On location the malware sends a command to send the rudder to a set angle and increase speed before jamming them



Packet Flow

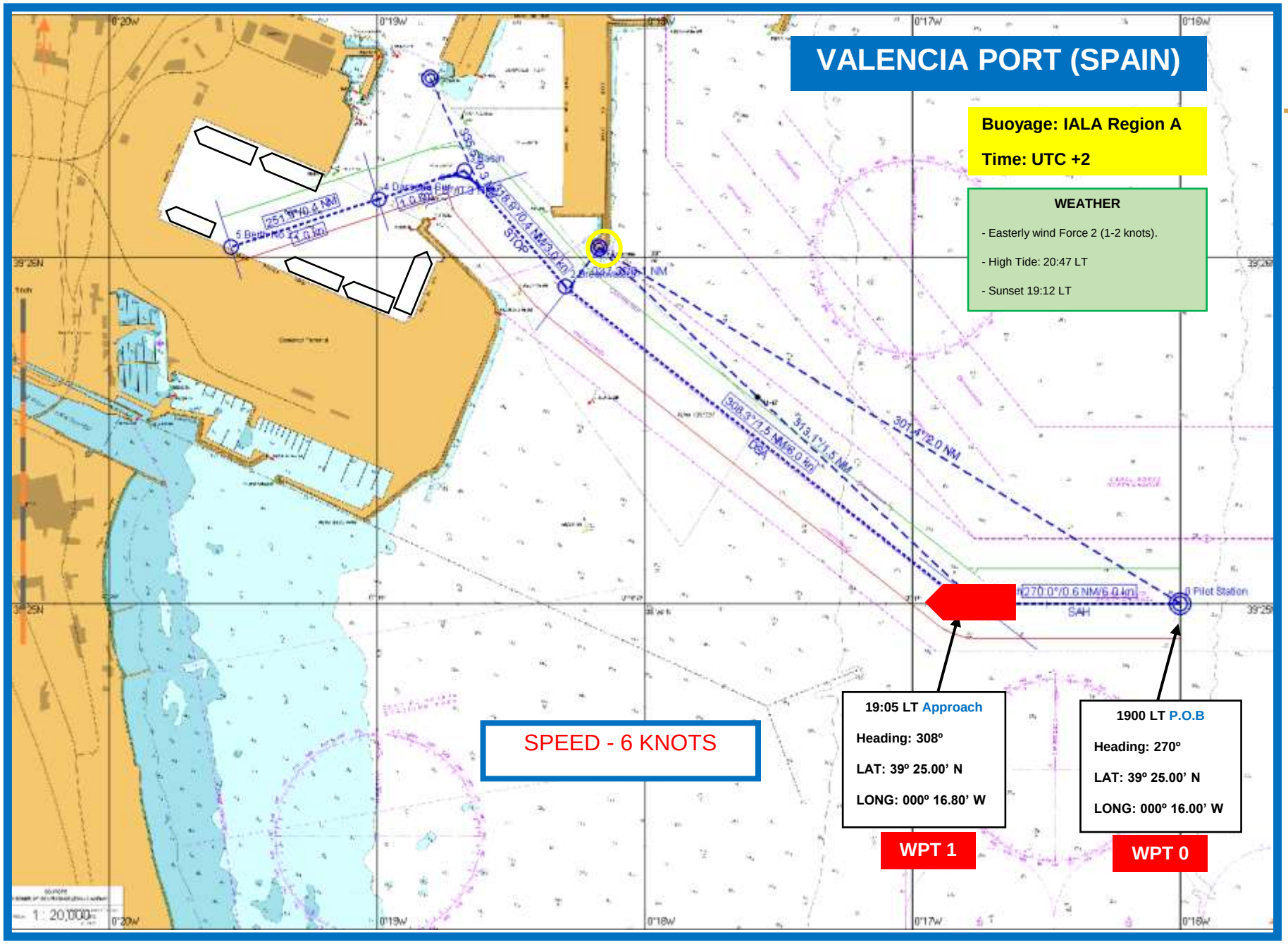
VALENCIA PORT (SPAIN)

Buoyage: IALA Region A

Time: UTC +2

WEATHER

- Easterly wind Force 2 (1-2 knots).
- High Tide: 20:47 LT
- Sunset 19:12 LT



SPEED - 6 KNOTS

19:05 LT Approach

Heading: 308º

LAT: 39º 25.00' N

LONG: 000º 16.80' W

WPT 1

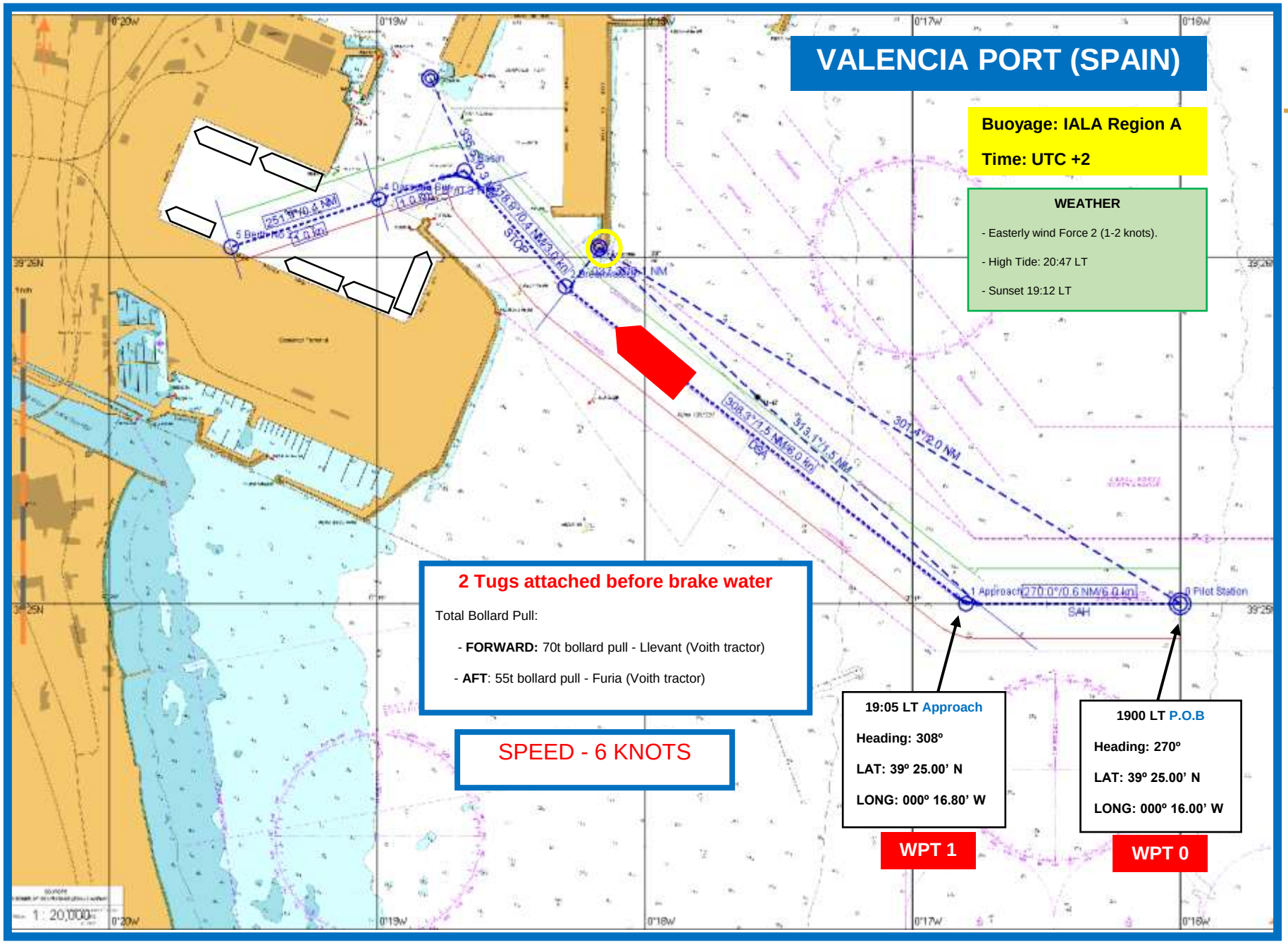
1900 LT P.O.B

Heading: 270º

LAT: 39º 25.00' N

LONG: 000º 16.00' W

WPT 0


VALENCIA PORT (SPAIN)
Buoyage: IALA Region A
Time: UTC +2
WEATHER
- Easterly wind Force 2 (1-2 knots).
- High Tide: 20:47 LT
- Sunset 19:12 LT
2 Tugs attached before brake water
Total Bollard Pull:
- FORWARD: 70t bollard pull - Llevant (Voith tractor)
- AFT: 55t bollard pull - Furia (Voith tractor)
SPEED - 6 KNOTS
19:05 LT Approach
Heading: 308º
LAT: 39º 25.00' N
LONG: 000º 16.80' W
WPT 1
1900 LT P.O.B
Heading: 270º
LAT: 39º 25.00' N
LONG: 000º 16.00' W
WPT 0
1 Approach
0 Pilot Station
SAH
1 : 20,000

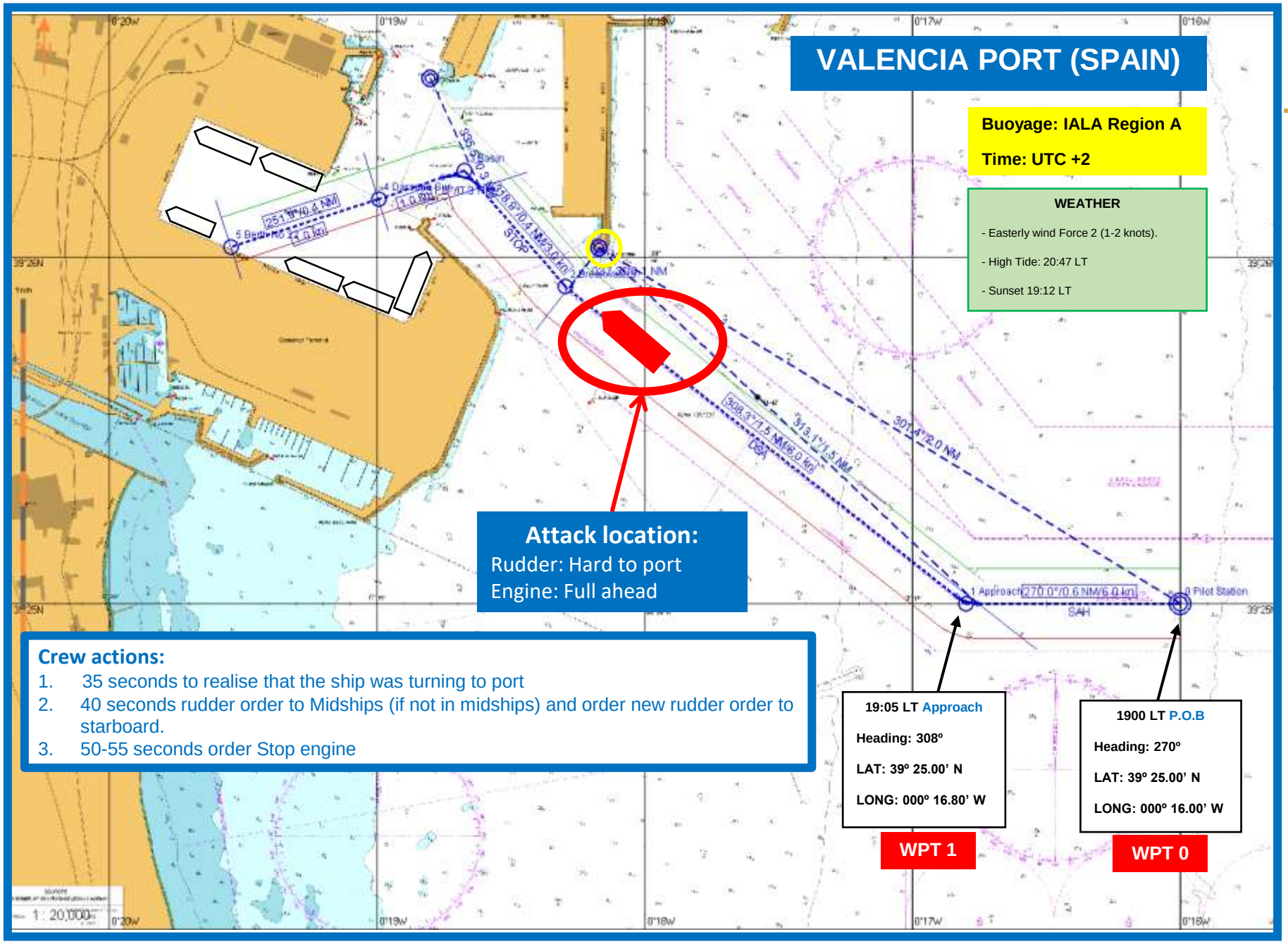
VALENCIA PORT (SPAIN)

Buoyage: IALA Region A

Time: UTC +2

WEATHER

- Easterly wind Force 2 (1-2 knots).
- High Tide: 20:47 LT
- Sunset 19:12 LT



Attack location:
Rudder: Hard to port
Engine: Full ahead

Crew actions:

1. 35 seconds to realise that the ship was turning to port
2. 40 seconds rudder order to Midships (if not in midships) and order new rudder order to starboard.
3. 50-55 seconds order Stop engine

19:05 LT Approach

Heading: 308º

LAT: 39º 25.00' N

LONG: 000º 16.80' W

WPT 1

1900 LT P.O.B

Heading: 270º

LAT: 39º 25.00' N

LONG: 000º 16.00' W

WPT 0

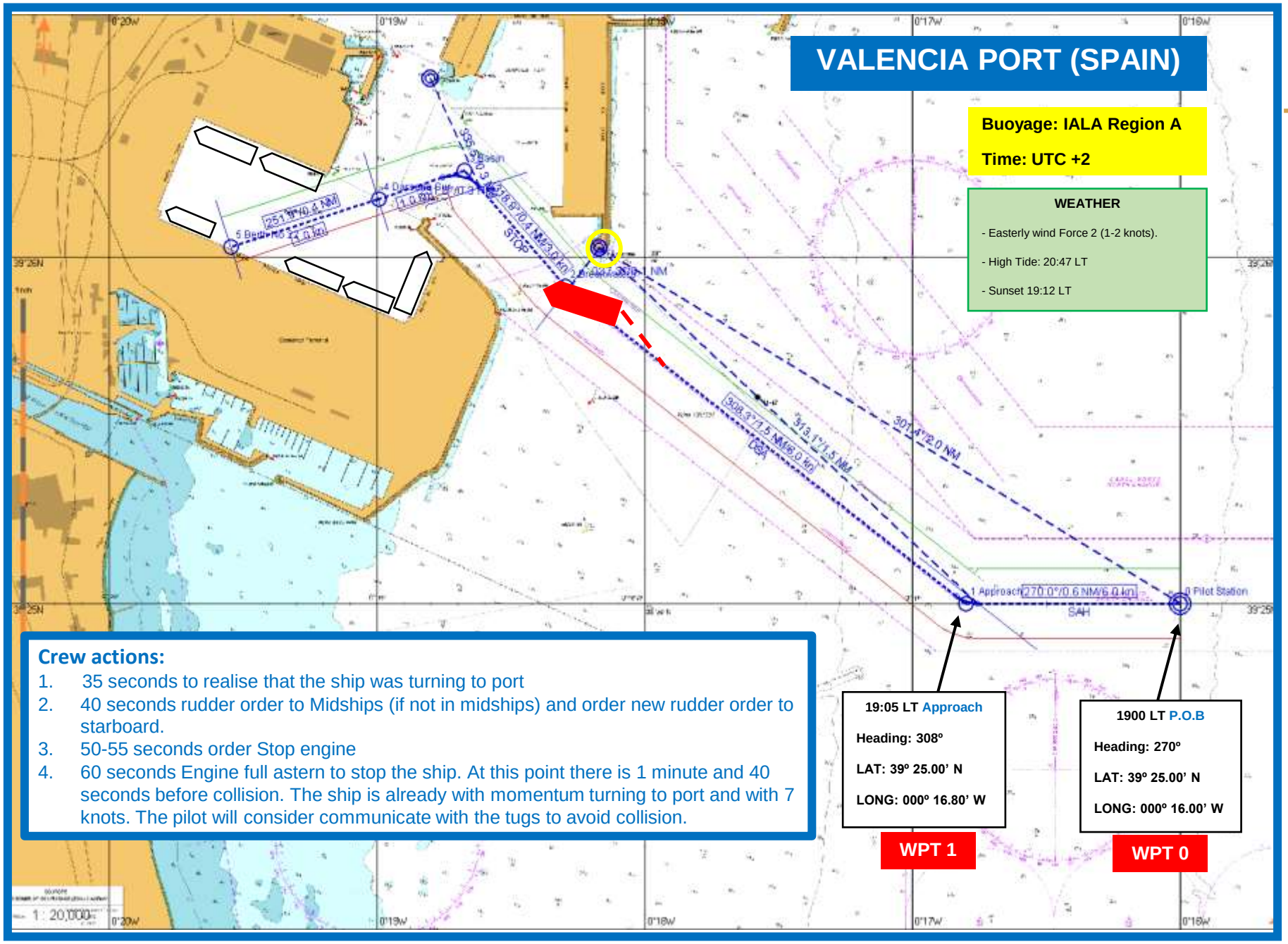
VALENCIA PORT (SPAIN)

Buoyage: IALA Region A

Time: UTC +2

WEATHER

- Easterly wind Force 2 (1-2 knots).
- High Tide: 20:47 LT
- Sunset 19:12 LT



Crew actions:

1. 35 seconds to realise that the ship was turning to port
2. 40 seconds rudder order to Midships (if not in midships) and order new rudder order to starboard.
3. 50-55 seconds order Stop engine
4. 60 seconds Engine full astern to stop the ship. At this point there is 1 minute and 40 seconds before collision. The ship is already with momentum turning to port and with 7 knots. The pilot will consider communicate with the tugs to avoid collision.

19:05 LT Approach

Heading: 308º

LAT: 39º 25.00' N

LONG: 000º 16.80' W

WPT 1

1900 LT P.O.B

Heading: 270º

LAT: 39º 25.00' N

LONG: 000º 16.00' W

WPT 0

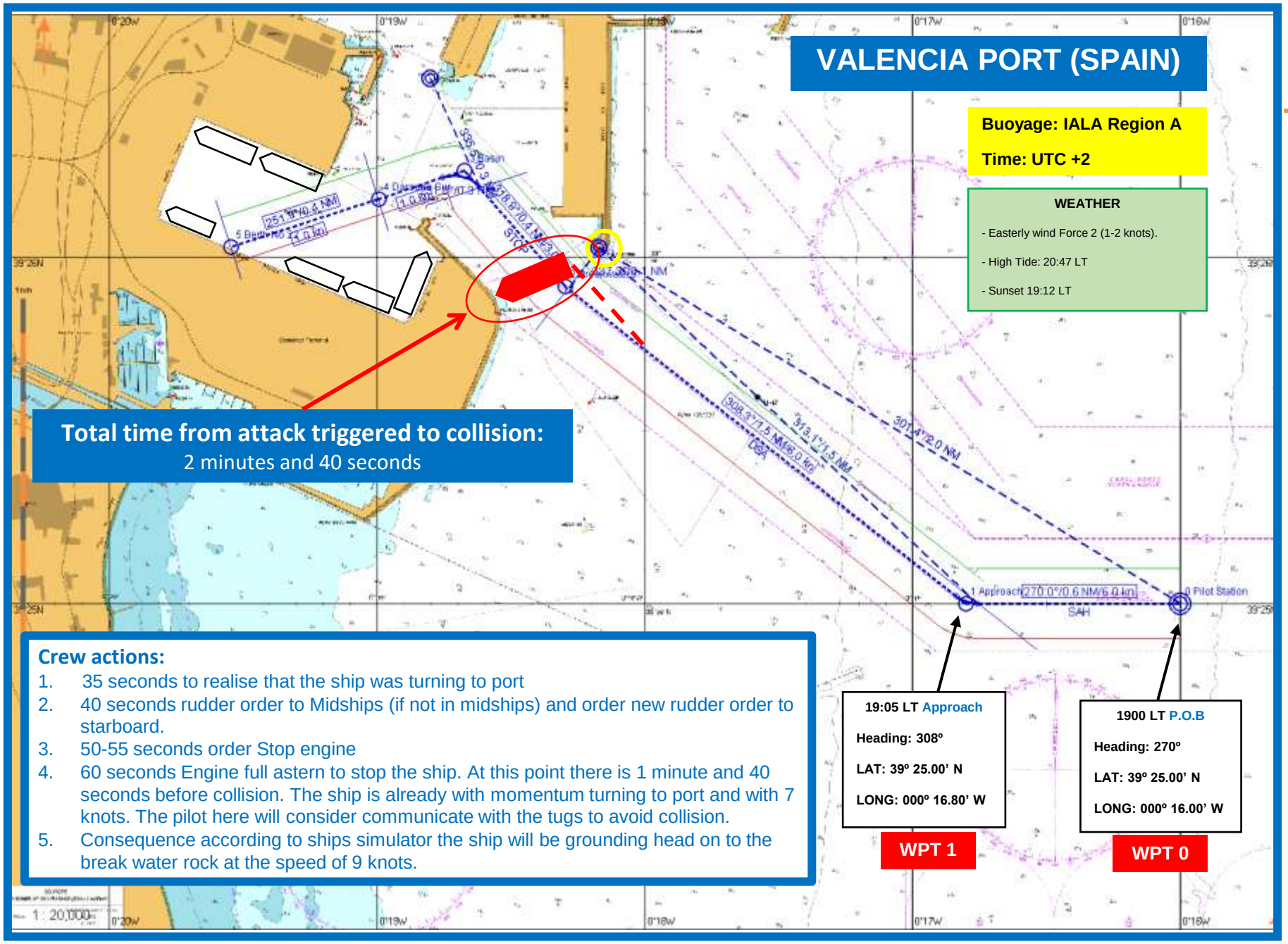
VALENCIA PORT (SPAIN)

Buoyage: IALA Region A

Time: UTC +2

WEATHER

- Easterly wind Force 2 (1-2 knots).
- High Tide: 20:47 LT
- Sunset 19:12 LT



Total time from attack triggered to collision:
2 minutes and 40 seconds

Crew actions:

1. 35 seconds to realise that the ship was turning to port
2. 40 seconds rudder order to Midships (if not in midships) and order new rudder order to starboard.
3. 50-55 seconds order Stop engine
4. 60 seconds Engine full astern to stop the ship. At this point there is 1 minute and 40 seconds before collision. The ship is already with momentum turning to port and with 7 knots. The pilot here will consider communicate with the tugs to avoid collision.
5. Consequence according to ships simulator the ship will be grounding head on to the break water rock at the speed of 9 knots.

19:05 LT Approach

Heading: 308º

LAT: 39º 25.00' N

LONG: 000º 16.80' W

WPT 1

1900 LT P.O.B

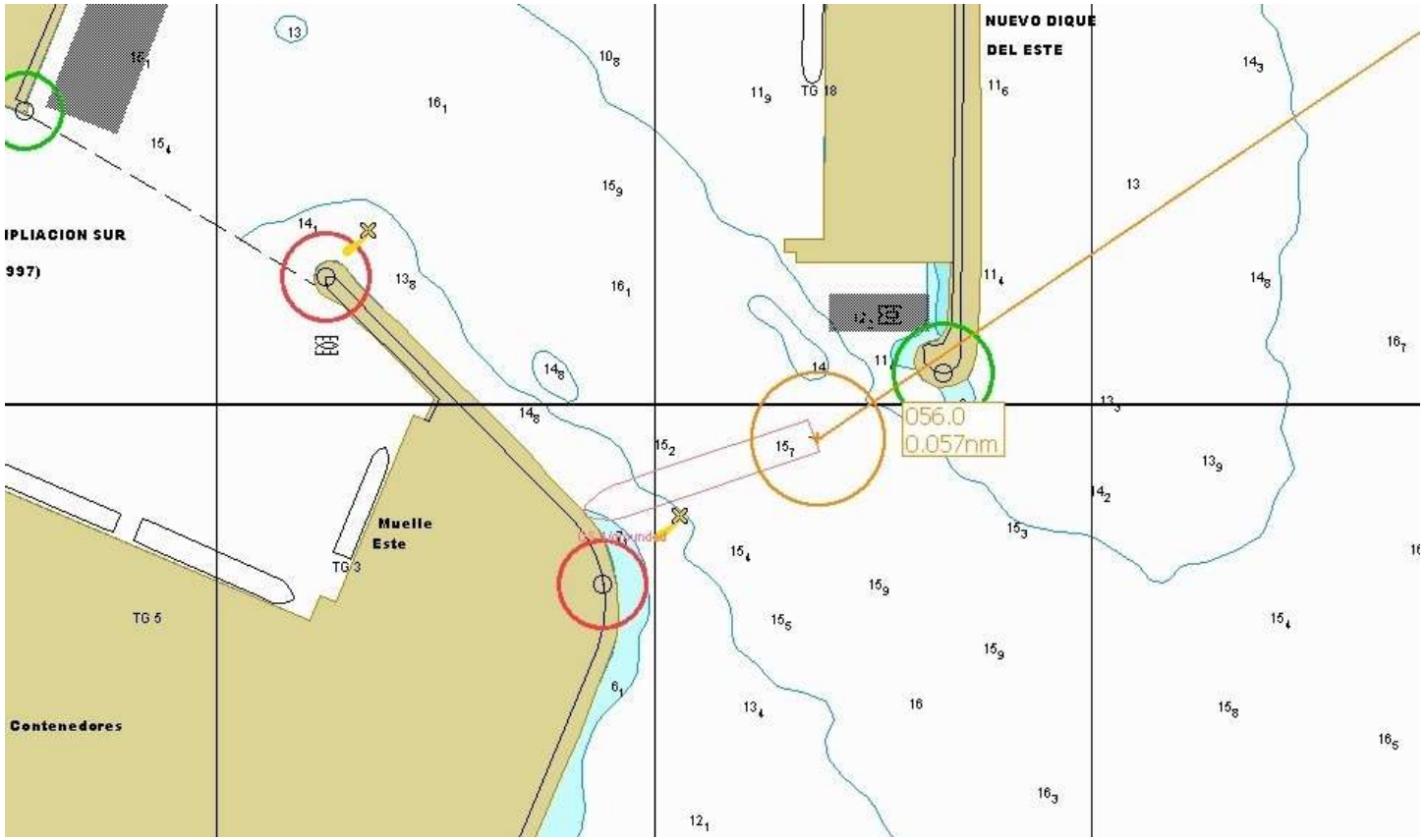
Heading: 270º

LAT: 39º 25.00' N

LONG: 000º 16.00' W

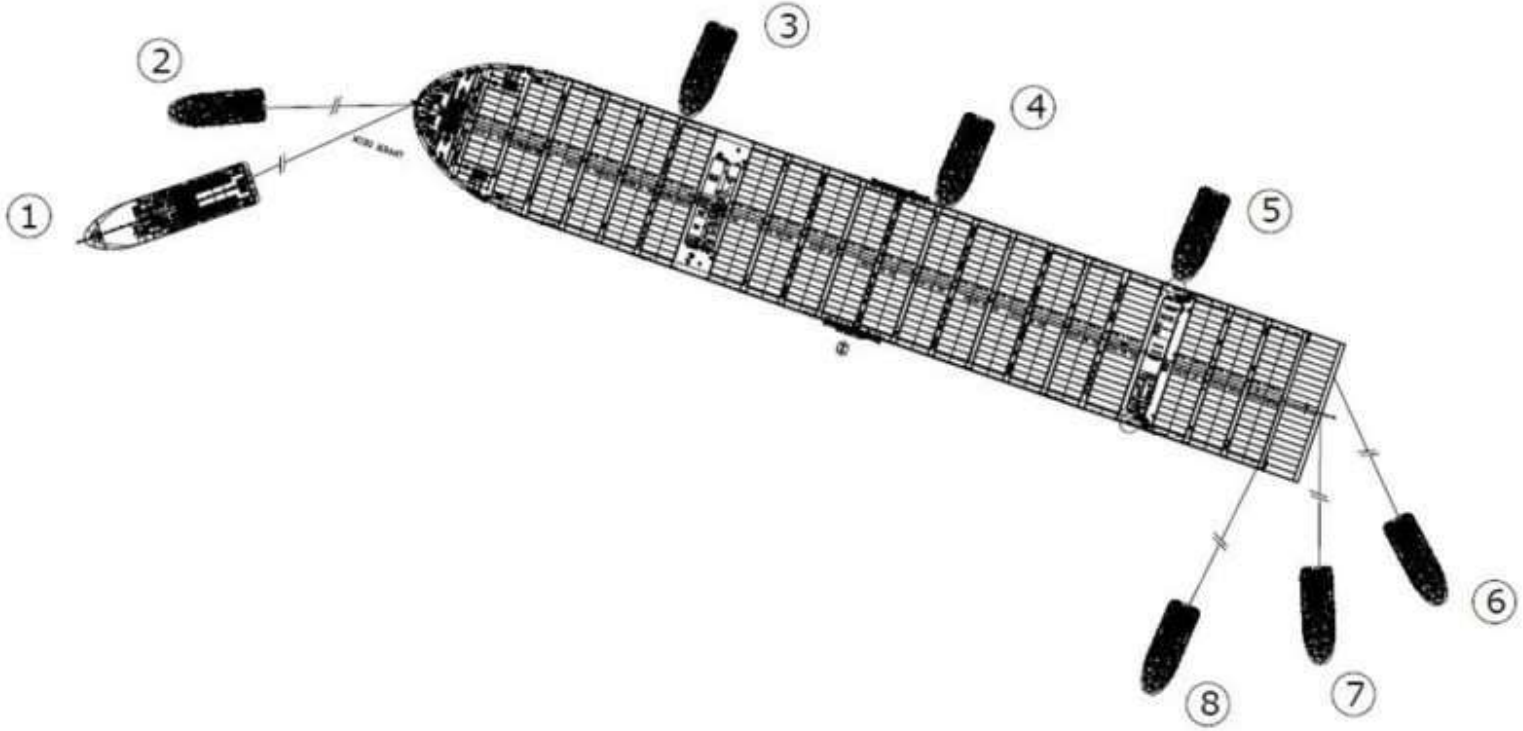
WPT 0

Experiencing the Attack



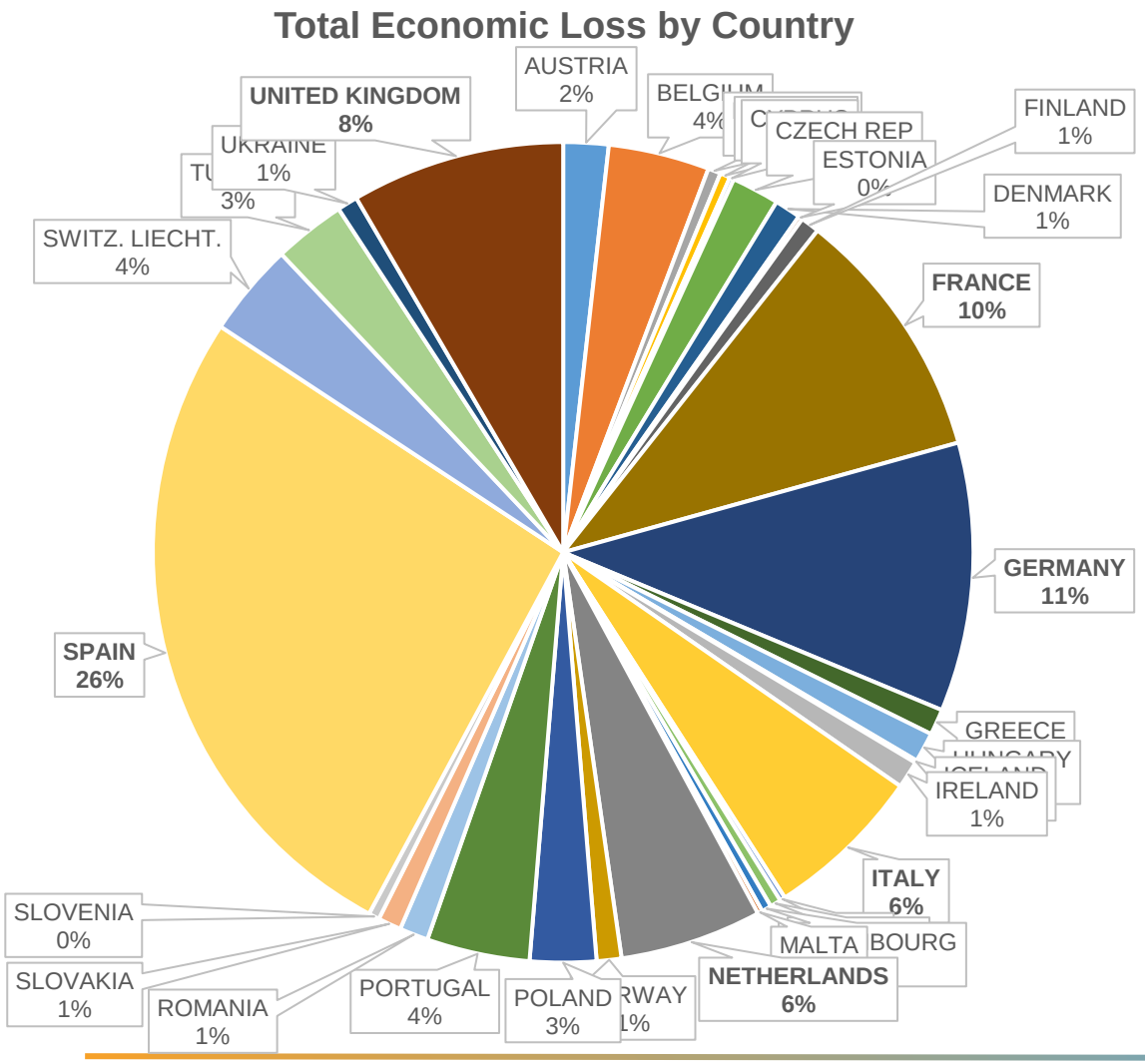
- **What tugs could do to avoid collision with break water?**
- **Vessel blocking the Port of Valencia entrance (100 metres gap)**

Example of similar vessel with tug operations to recover a ship that run's aground *"Mumbai Maersk, which ran aground outside Bremerhaven, Germany on 2 February, 2022"*



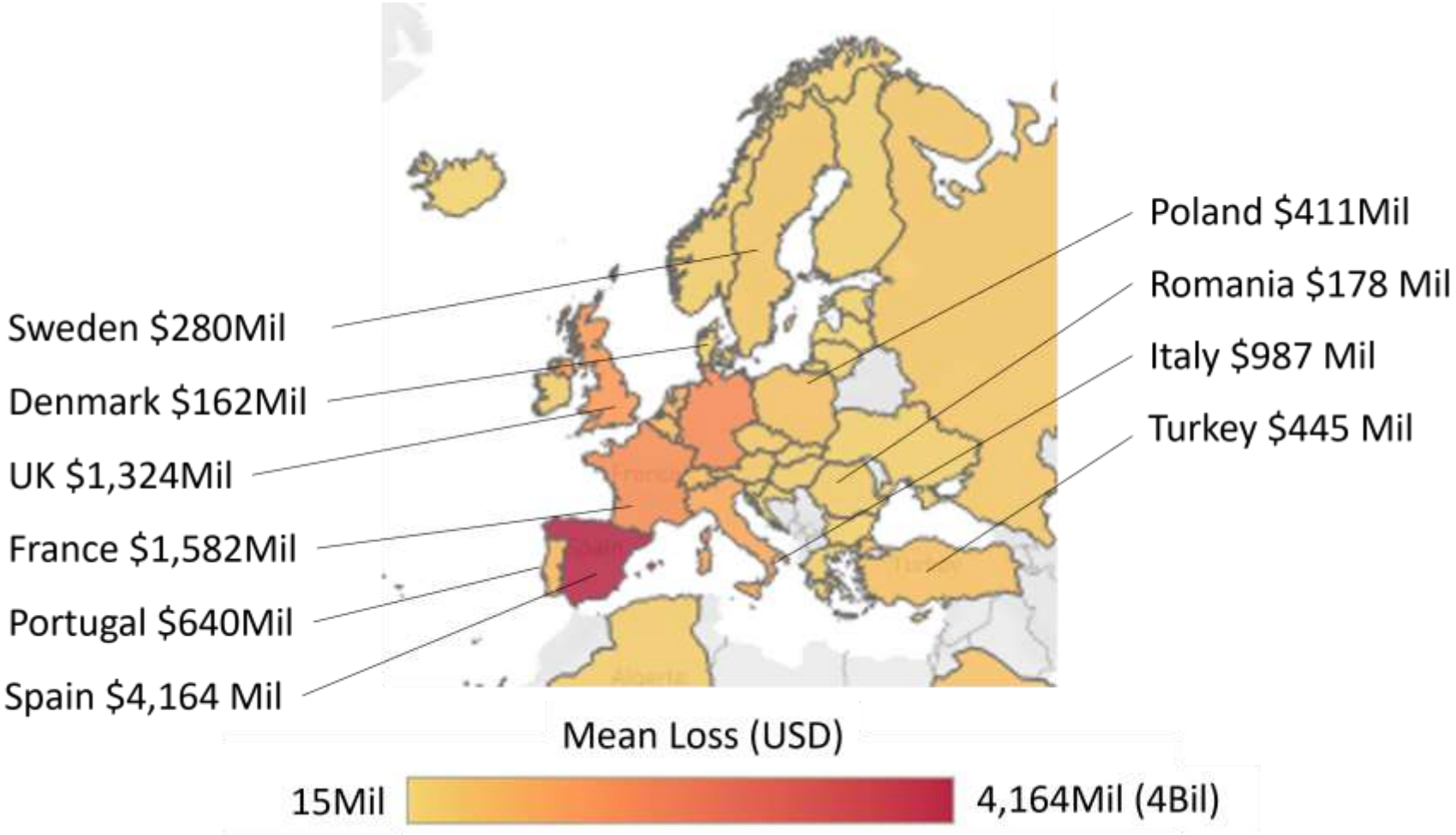
- **Salvage operations estimated duration 3-7 days**
- **Impact on berthing and unberthing operations**

Economic Impact on EU Region

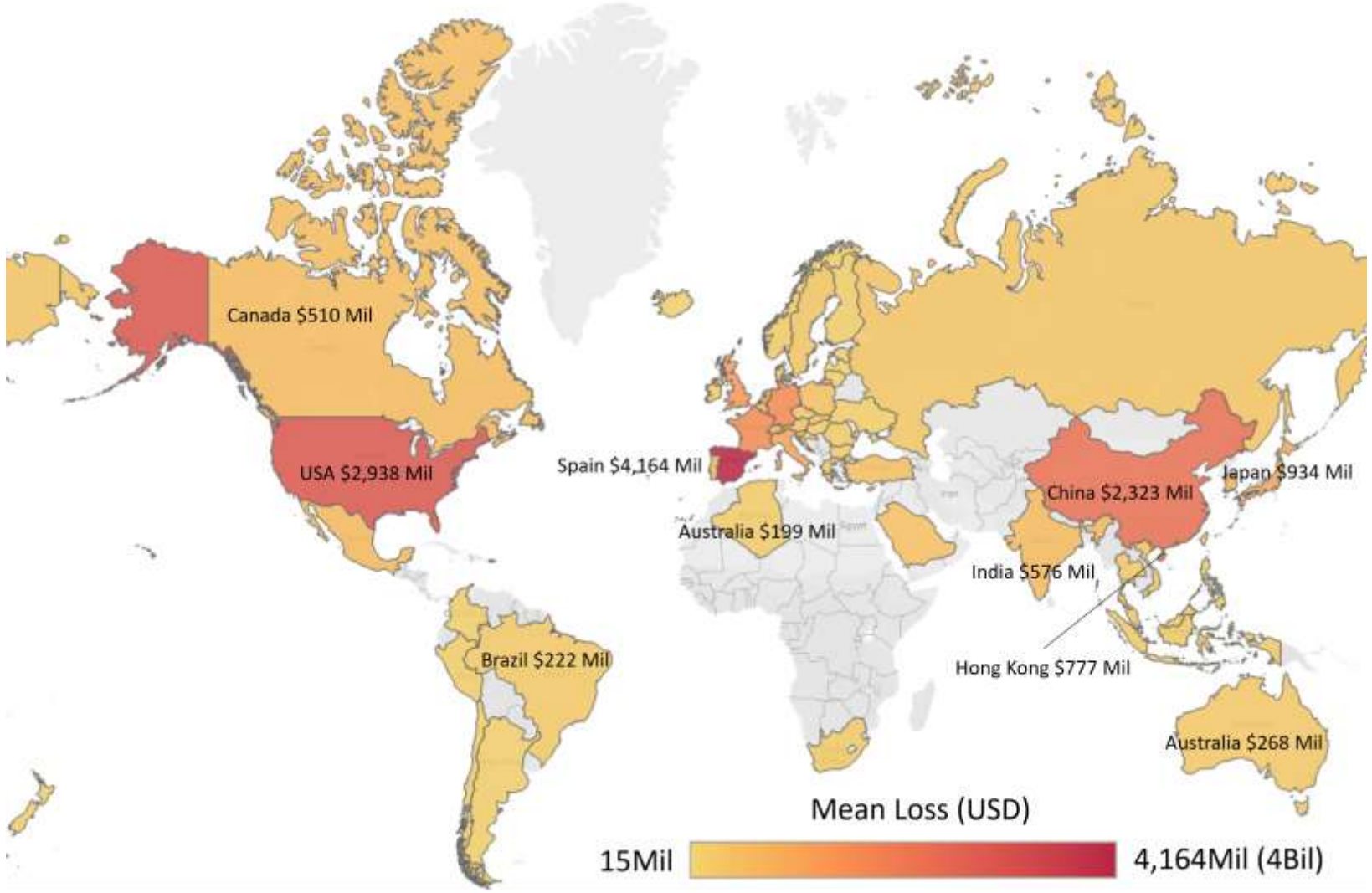


Losses (EUR M)	Initial Port Disruption		
	3 days	5 days	7 days
France	950	1,600	2,200
Germany	1,000	1,700	2,400
Italy	600	1,000	1,400
Netherlands	550	900	1,300
Spain	2,500	4,200	5,900
UK	800	1,300	1,900
…	…	…	…
Austria	**190**	**320**	**440**

5 Day Econometric Impact - EU



5 Day Econometric Impact – Global



Mitigating the Risk

Dormant period

Email arrives → Visits fake website → Downloads to USB → Installs on ECDIS → Geo trigger

- Whitelisting
- Policy
- Sender verification
- Email scan

- Blacklisting
- Whitelisting
- URL verification
- Secure certificates

- Scan USB devices
- Scan the download
- Use secure/verified USBs

- Policy
- Secure ports (USB)
- Scan software
- Anti-malware
- Asset management
- Locking OS

- IDS/IDP
- AI based Firewalls
- Incident response policy
- Preparation, drills and training

Training
Policy
Technology

frontiers About us All journals All articles Submit your research

Frontiers in Computer Science Sections Articles Research Topics Editorial Board

ORIGINAL RESEARCH article

Front. Comput. Sci., 23 January 2023
Sec. Computer Security
Volume 4 - 2022 |
https://doi.org/10.3389/fcomp.2022.1057507

This article is part of the Research Topic
The Impacts of Cyber Threat in the Maritime Ecosystem
View all Articles >

Quantifying the econometric loss of a cyber-physical attack on a seaport

Kimberly Tam[1*], Barbara Chang[2], Rory Hopcraft[1], Kemedi Moara-Nkwe[3] and Kevin Jones[1]

[1] Maritime Cyber Threats Research Group, University of Plymouth, Plymouth, United Kingdom
[2] Verisk EES (AIR Worldwide), San Francisco, CA, United States
[3] Warwash Solent University, Southampton, United Kingdom

Thank you

Kimberly Tam
Kimberly.tam@plymouth.ac.uk

This presentation is partly funded by the research efforts under Cyber-MAR. Cyber-MAR project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 833389. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.