Cyber-SHIP Lab

SECURING MARITIME

UNIVERSITY OF PLYMOUTH

Presented

by

Wesley Andrews

Avanthika Vineetha Harish

Rory Hopcraft

Juan Dorje Palbar Misas

On behalf of:

Professor Kevin Jones - Principal Investigator

Dr Kimberly Tam - Academic lead

Chloe Rowland - Project Manager

Wesley Andrews

Industrial Research Assistant
(Electronics/Hardware)/Project Engineer
Cyber-SHIP Lab

Cyber-SHIP Lab

SECURING MARITIME

Software
Hardware
Information
Protection

What is the Cyber-SHIP Lab?

- A Unique **£3.2 million hardware-based** platform
- Physical twin
- Real-world solutions to real-world problems
- Provide reports to OEMs

UNIVERSITY OF PLYMOUTH

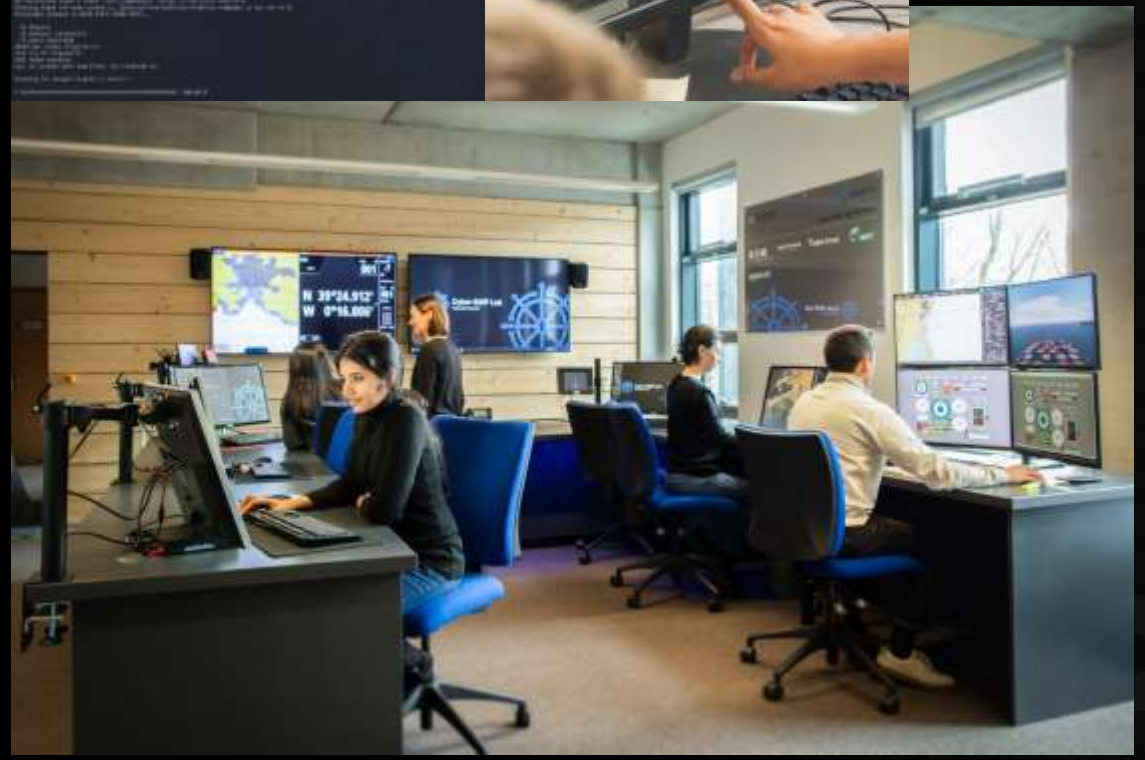
Cyber-SHIP Lab current status – Aug 2022

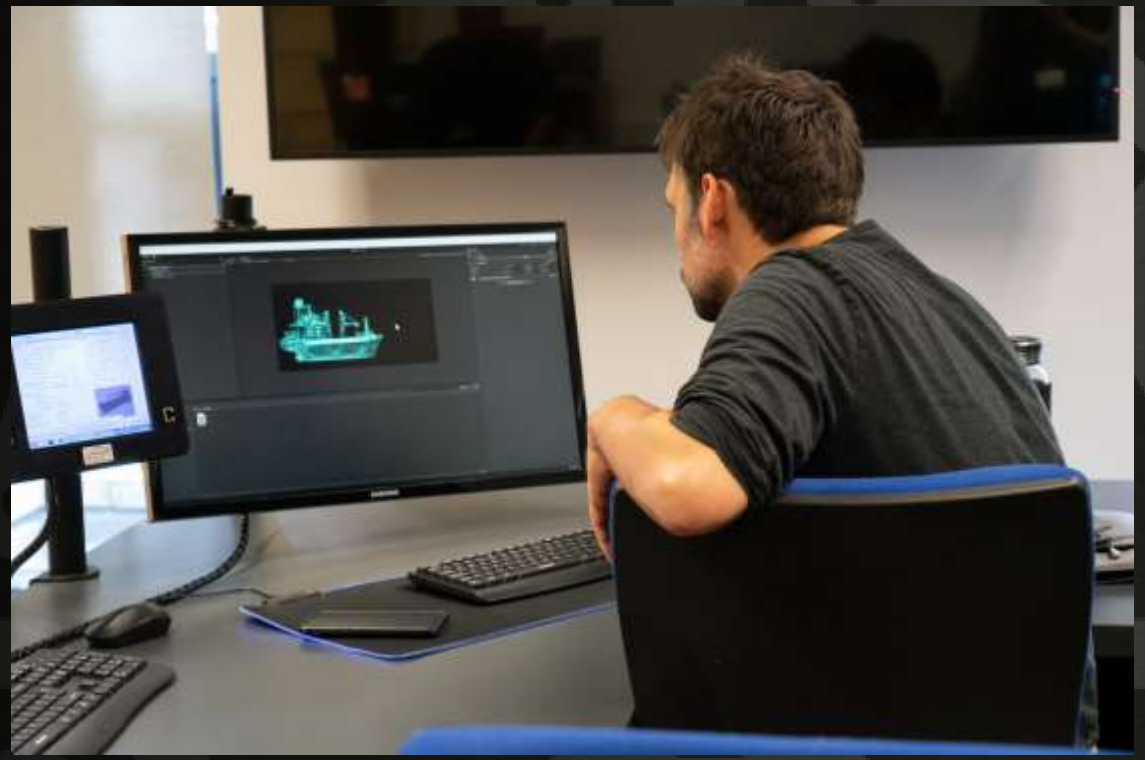
- Fully functioning lab with a growing number of bridge and control system configurations
- In-house custom built scale physical test rigs for steering and propulsion systems
- Set of standard tests providing basic vulnerability assessment
- Custom crafted malware
- Commercial consultancy to provide standard vulnerability reports
- *Still a work in progress, but progressing steadily…*

Two sides of the story…

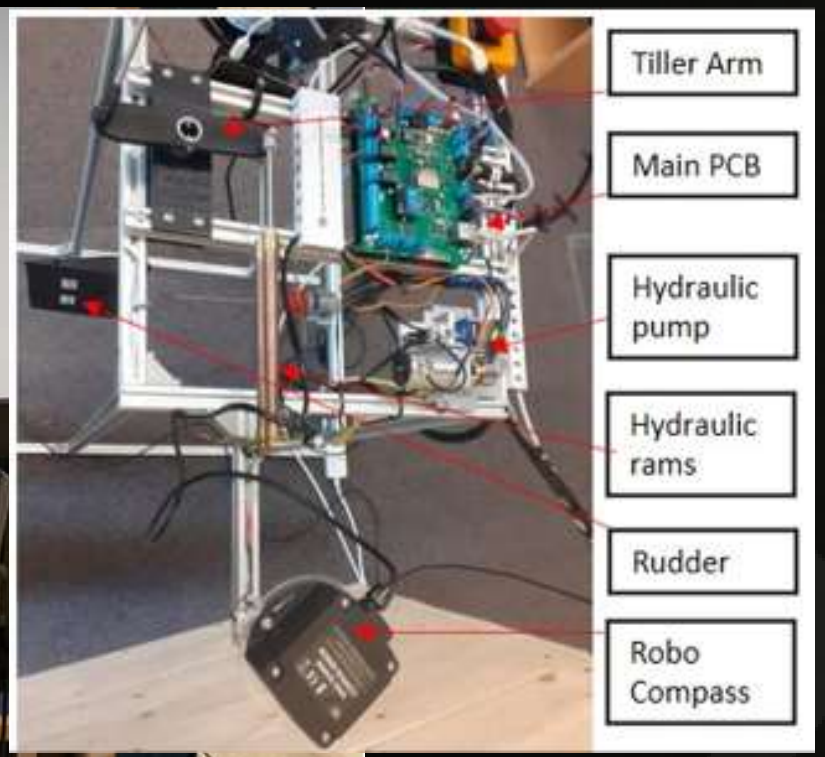
The Console Room

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



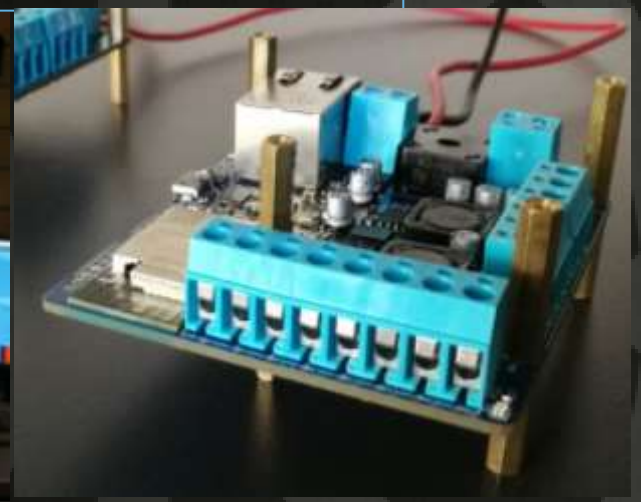


UNIVERSITY OF PLYMOUTH



Bespoke electronics design work

Custom built, in-house physical model of rudder and propulsion system simulator



The Vault

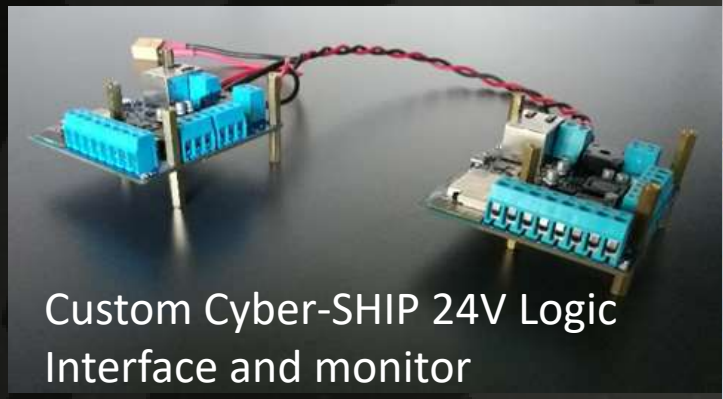

Drones and USVs


Radar equipment


Custom Power Distribution


VDRs and NAVTEX


AIS receivers


Custom Cyber-SHIP 24V Logic Interface and monitor


USV equipment

Cyber-SHIP Lab

UNIVERSITY OF PLYMOUTH


NMEA2000/0183
Devices


Serial- IP converters


Serial- IP converters


Data recovery from
ECDIS


AIS


Satcom


NAVTEX/AIS

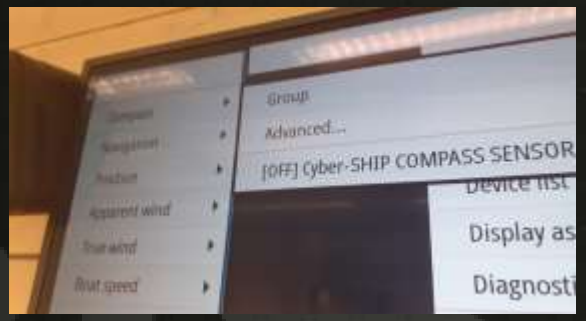
Now presenting…

Avanthika Vineetha Harish

Industrial Research Assistant (Pen-testing) -
Cyber-SHIP Lab

Testing

- Standard approach to device testing
- Testing at system level and entire configuration level
- Developing mariner-checked realistic scenarios
- Variety of attacks and vectors:
  - Denial of Service
  - Man in the Middle
  - Ransomware
  - Comms Channel
  - Supply Chain
  - NMEA 2000 injection (in house)



Custom NMEA 2000 Injection attack

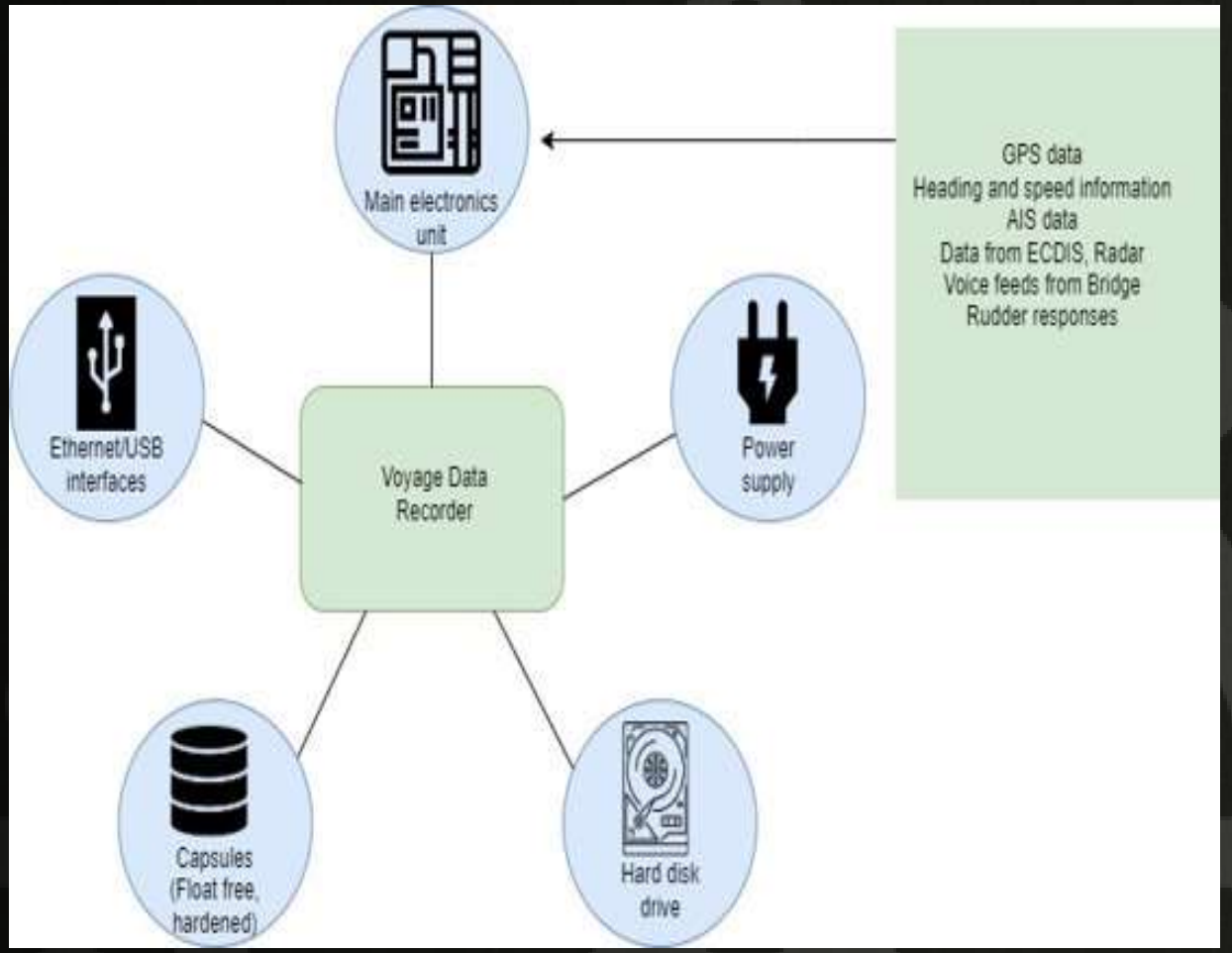
Software Defined Radio

Rubber Ducky

Cyber-SHIP Lab

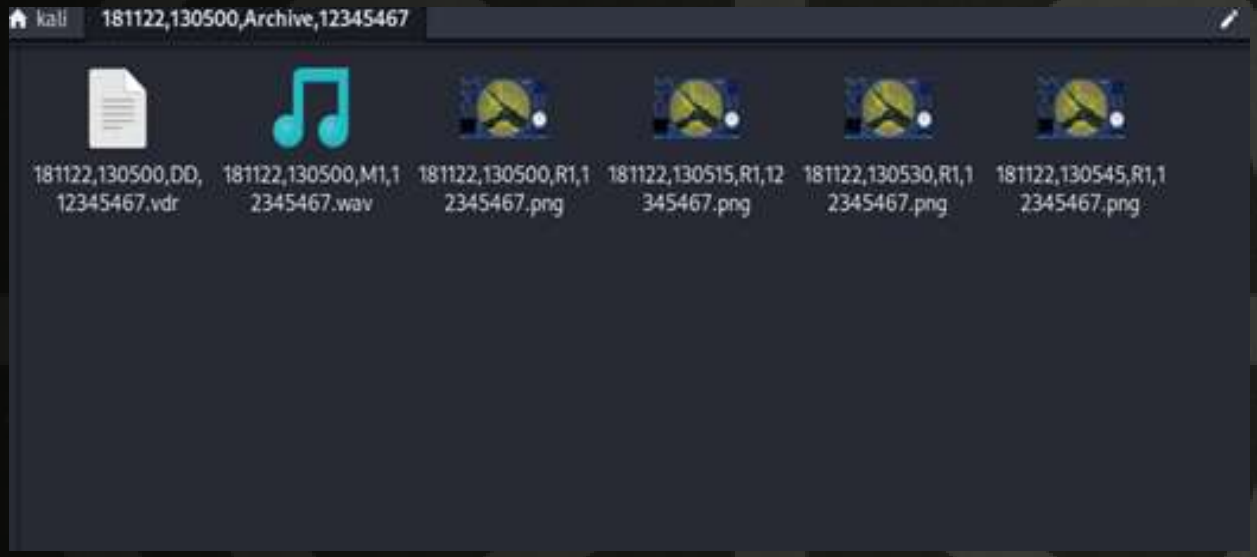
Voyage Data Recorders (VDRs)

- 'Black Box' for ships
- Running on old OSes and software
- Currently, VDRs do not have any mechanism to verify integrity and security of data stored.



Tested attacks

- Reverse shells
- Ransomware attacks
- Insider attacks
- Hard drive erasure
- USB based attacks
- Specific exploits
- Manipulating navigation data



Now presenting…

Rory Hopcraft

Industrial Researcher (Cyber-security/Governance)-
CyberMAR/Cyber-SHIP Lab

The Plymouth "ecosystem"

UNIVERSITY OF PLYMOUTH

Shipping operators (civil and defence), equipment manufacturers, regulators, insurers

Cyber-range labs

Exploits Tools

Cyber-SHIP Lab

Database

Ship simulators

Scenarios Training

Smart Sound

Autonomous/Remote control

Drones MAS

MaCRA

Profiles Reports Risk assessment

Shipping operators (civil and defence), equipment manufacturers, regulators, insurers

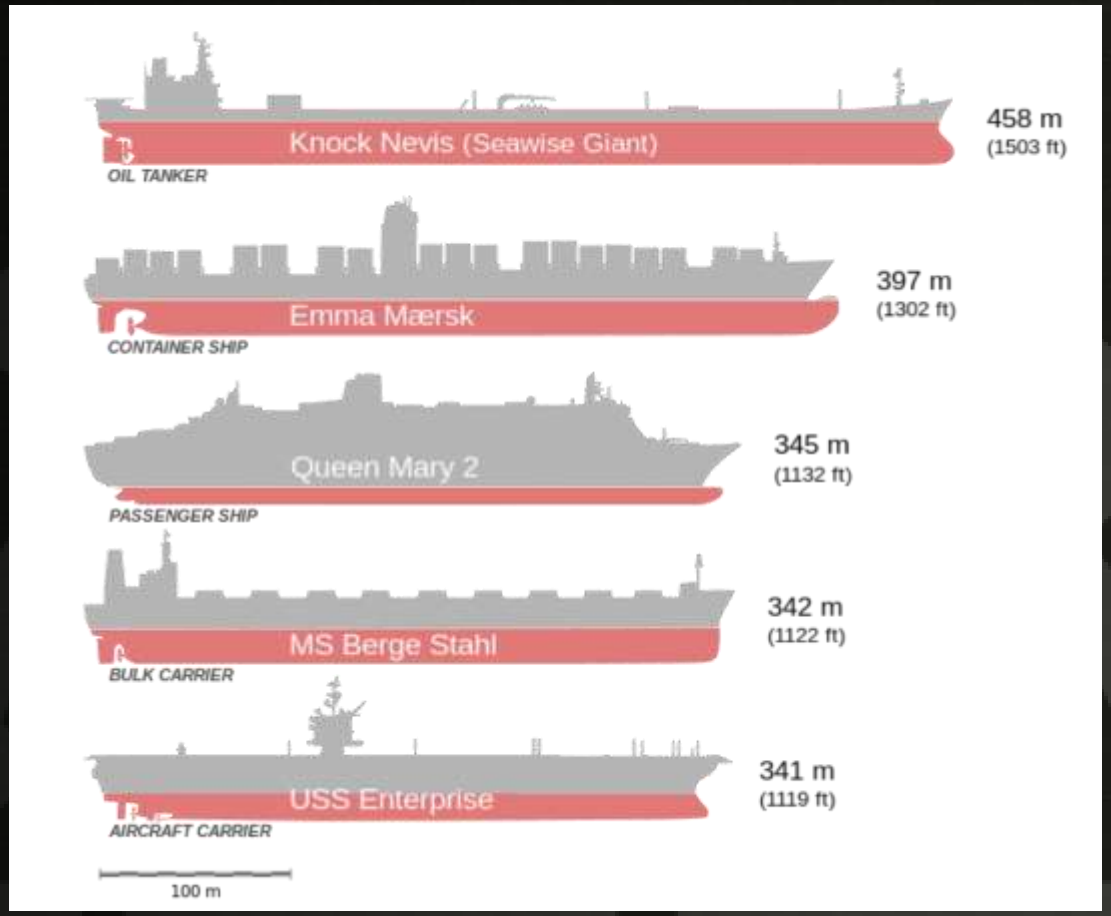
Cyber-SHIP Lab

UNIVERSITY OF PLYMOUTH

Research engagements and our partners

- Contract research, consultancy and PhDs
- Partnering for research
- Partnering with armed forces
- Partnering with industry

A sister project…



Cyber-MAR: a real-world attack scenario

'Cyber-MAR project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 833389

Setting the scene
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

Cyber-SHIP Lab

UNIVERSITY OF PLYMOUTH

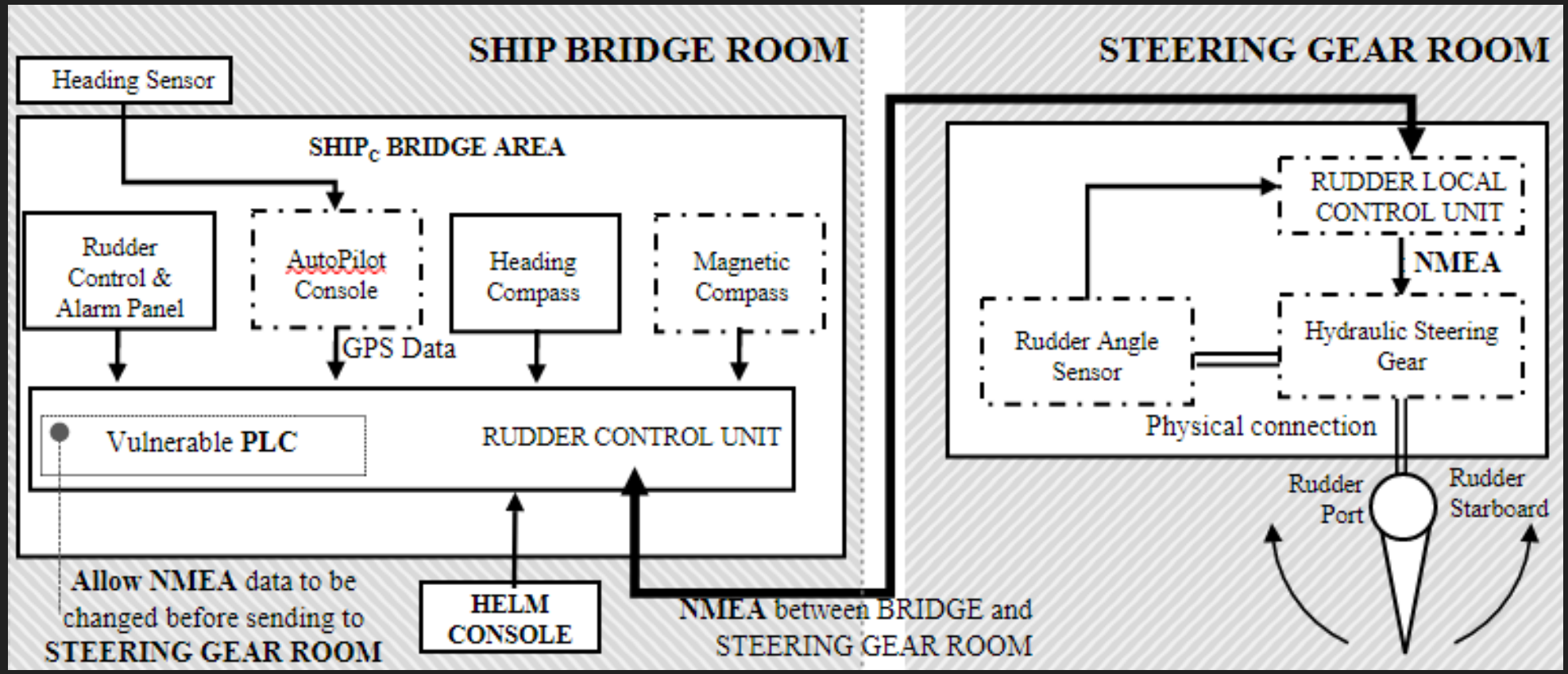
Setting the scene
Ship for the Scenario

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

Cyber-SHIP Lab

UNIVERSITY OF PLYMOUTH

Vessel navigation attack



Cyber-SHIP Lab

UNIVERSITY OF PLYMOUTH

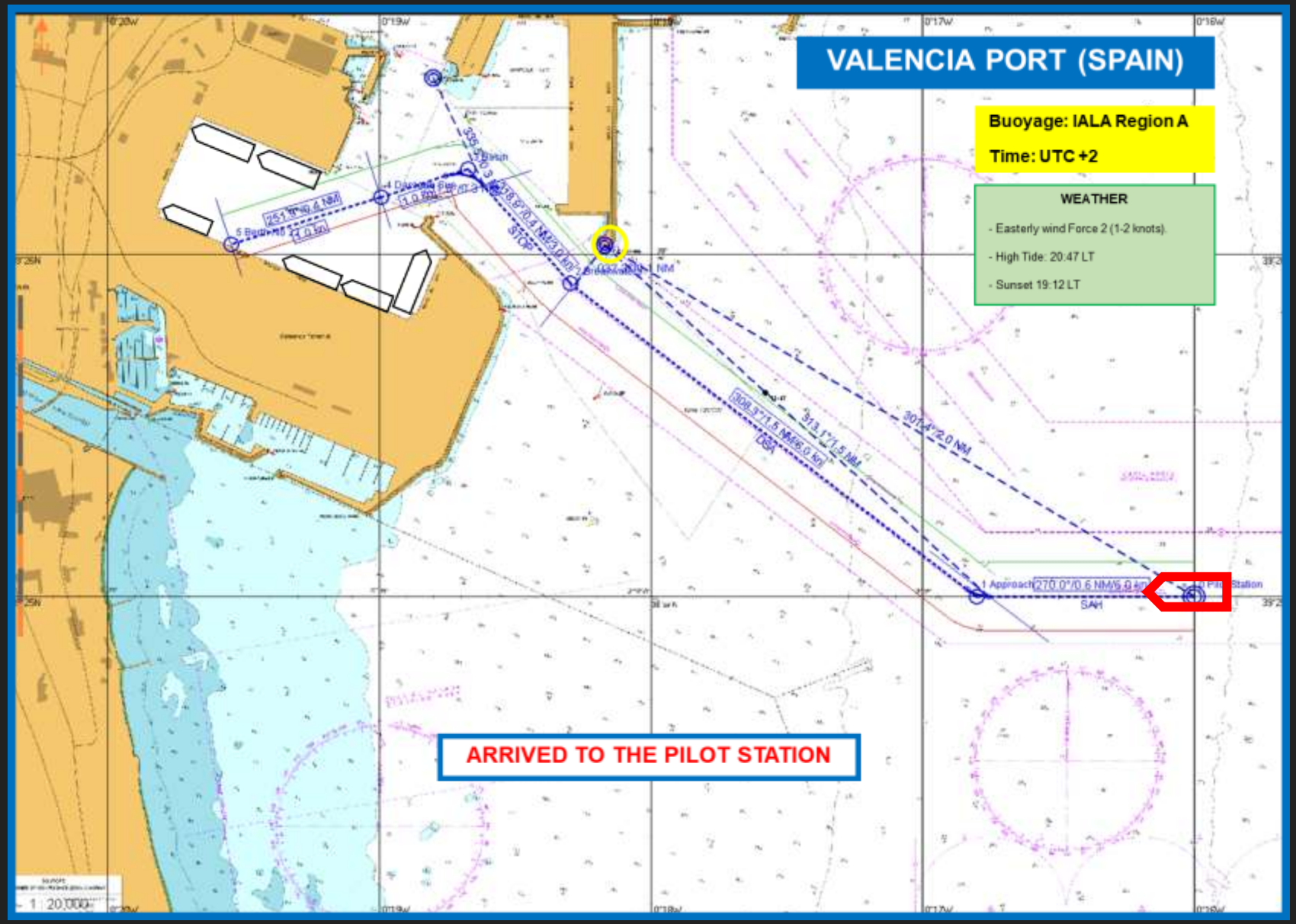
Now presenting…

Juan Dorje Palbar Misas

Research Assistant in Navigation and Maritime Cyber - CyberMAR/Cyber-SHIP Lab

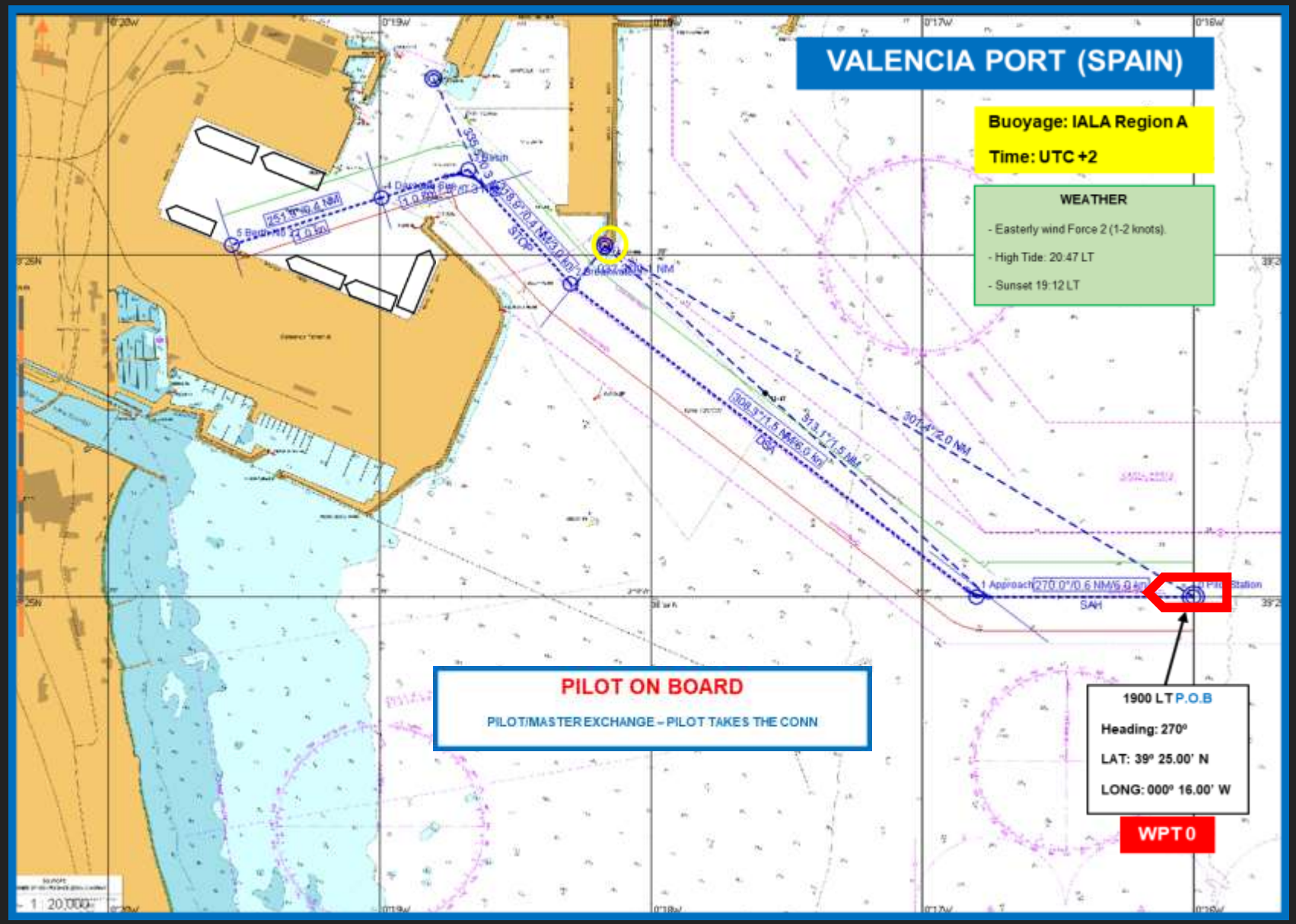
Cyber-SHIP Lab

UNIVERSITY OF PLYMOUTH



Cyber-SHIP Lab

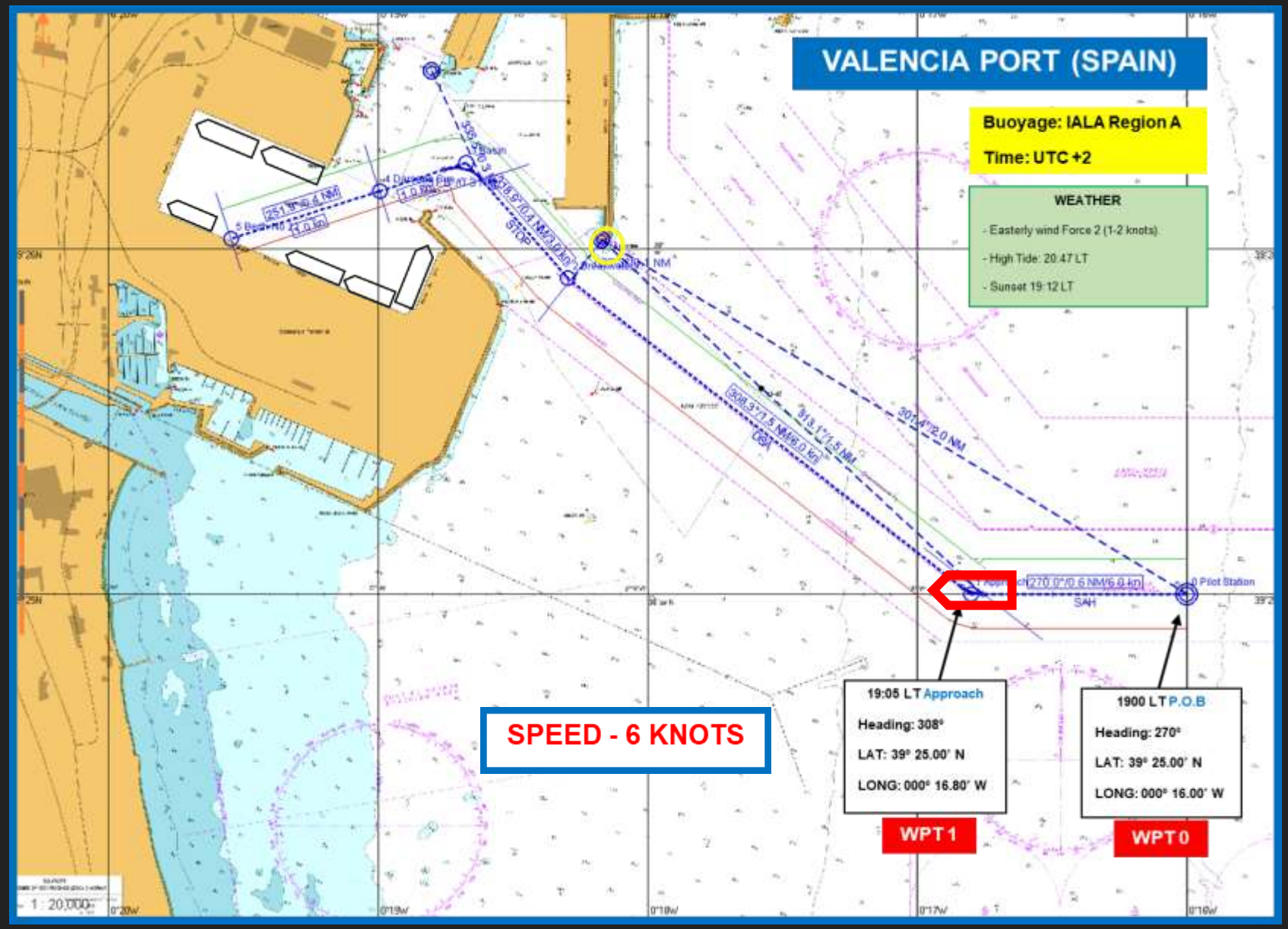
UNIVERSITY OF PLYMOUTH



Cyber-SHIP Lab

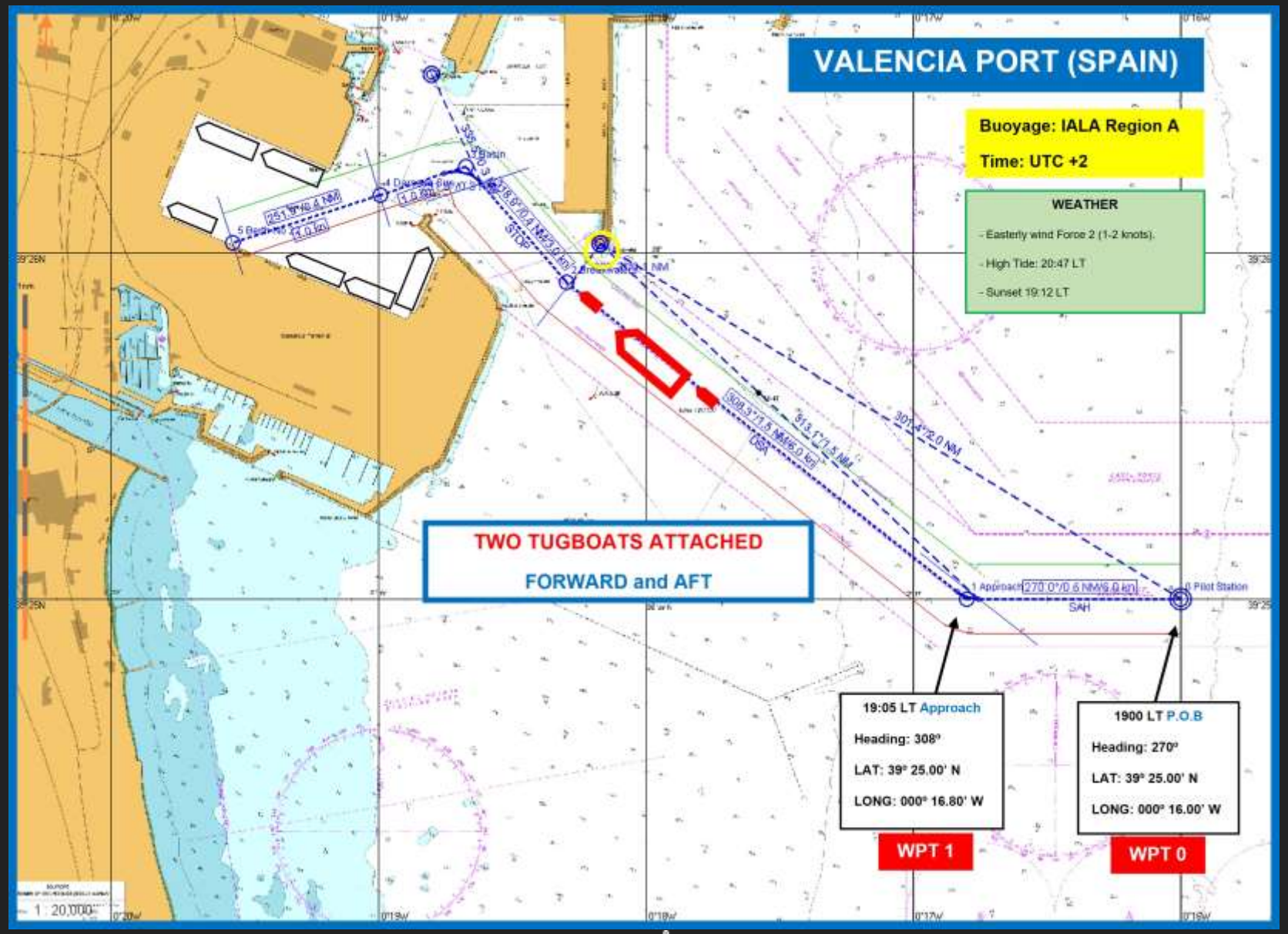
UNIVERSITY OF PLYMOUTH

CyberMAR



Cyber-SHIP Lab

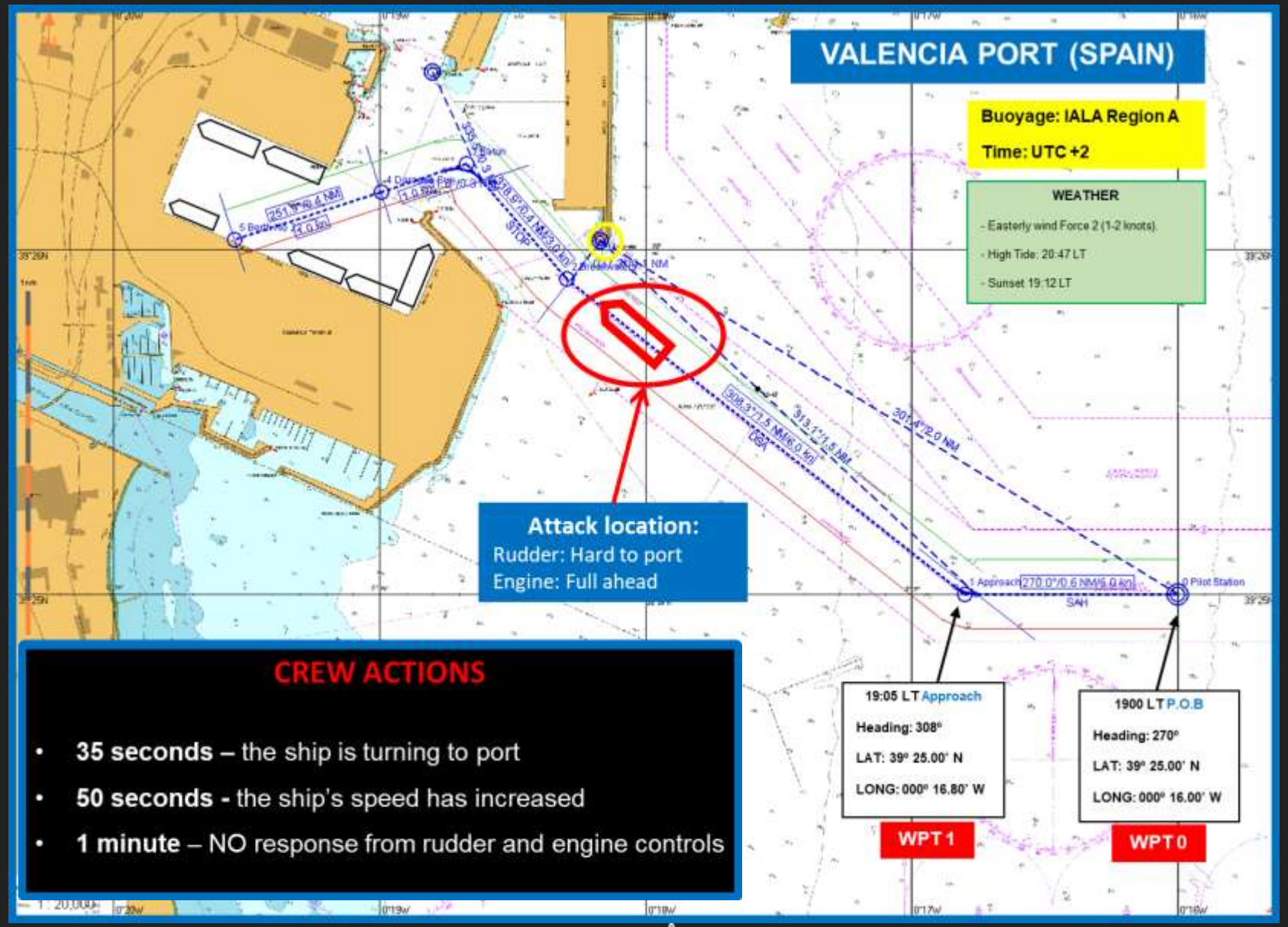
UNIVERSITY OF PLYMOUTH



Cyber-SHIP Lab

UNIVERSITY OF PLYMOUTH

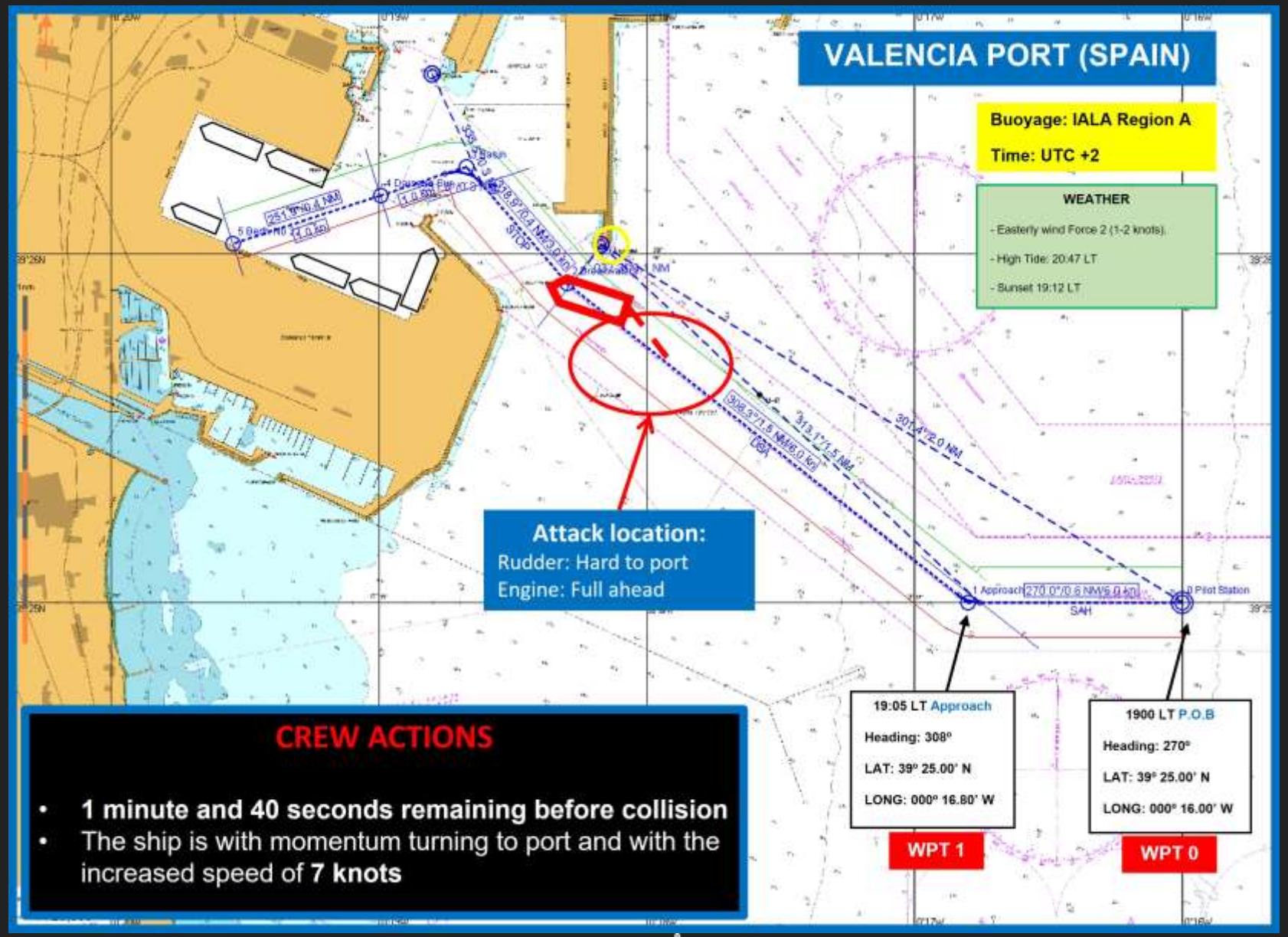
Cyber MAR



POINT OF NO RETURN

Cyber-SHIP Lab

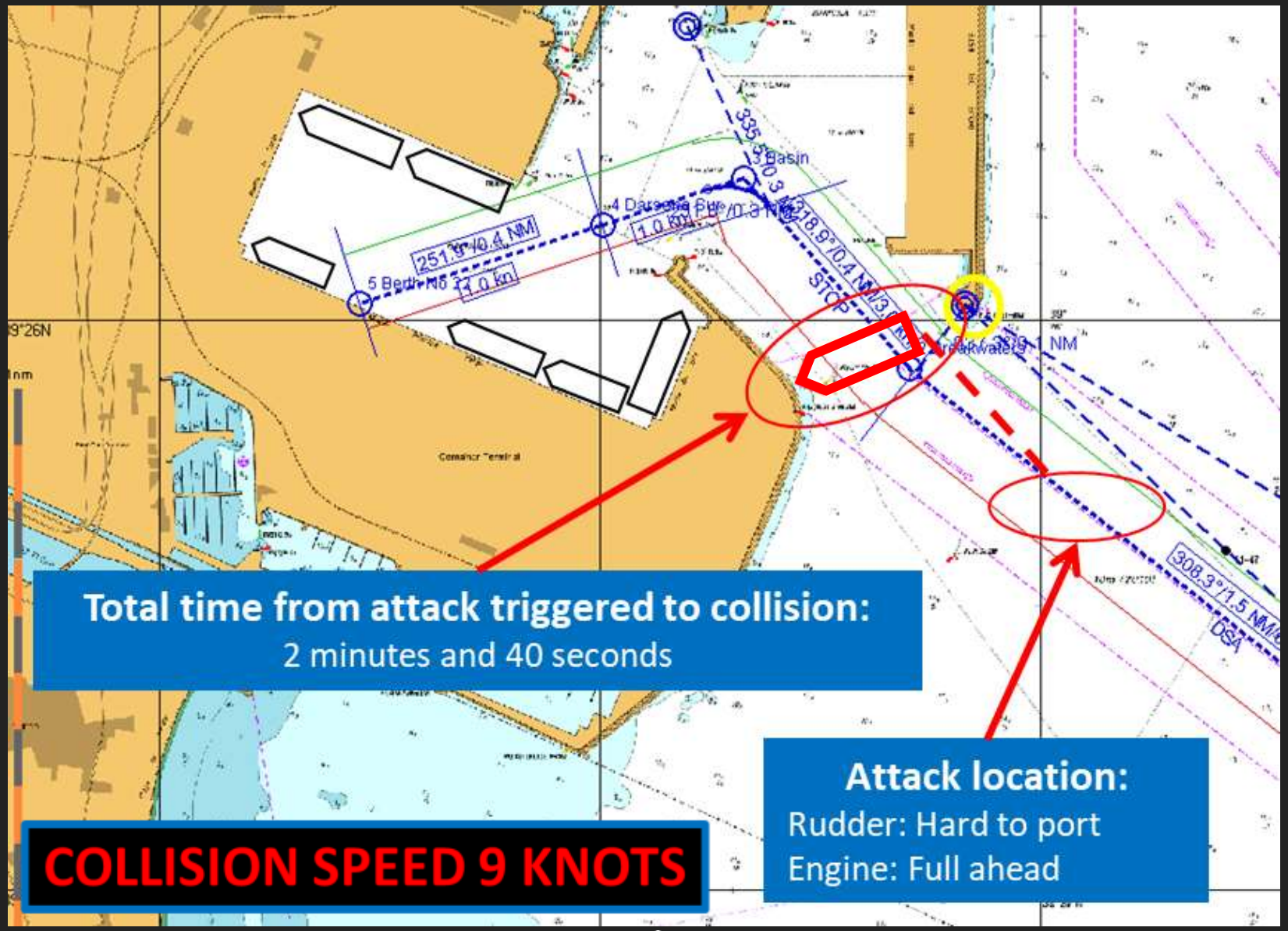
UNIVERSITY OF PLYMOUTH



Cyber-SHIP Lab

UNIVERSITY OF PLYMOUTH

Cyber MAR



Cyber-SHIP Lab

UNIVERSITY OF PLYMOUTH

Reference of tugboats salvage operation as per following case:
"Mumbai Maersk, which ran aground outside Bremerhaven, Germany on 2 February, 2022"

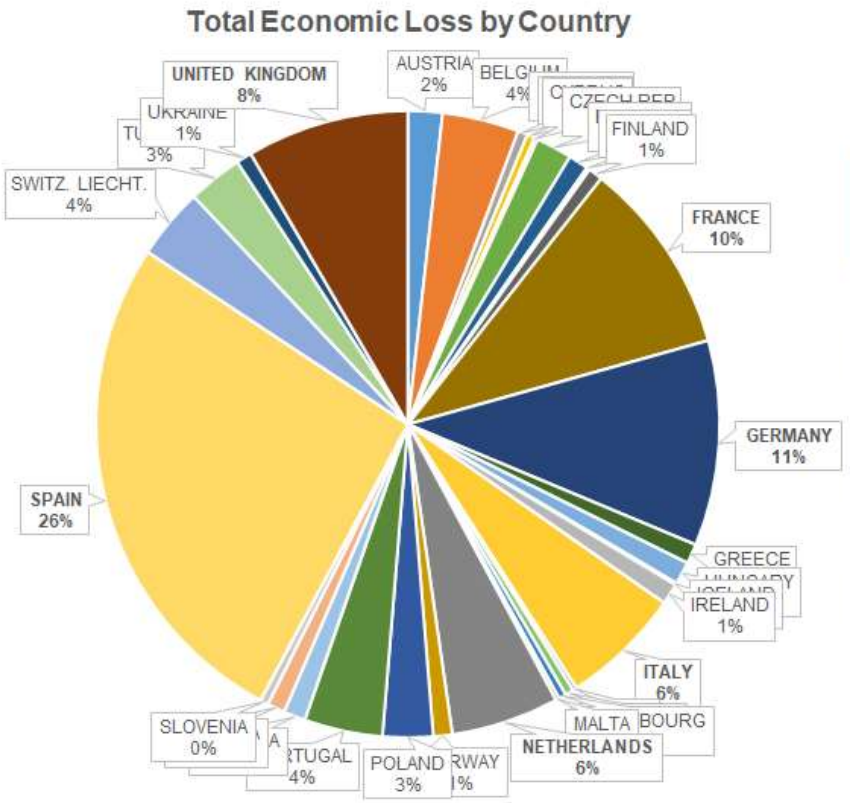
Conclusion and consequences

1. Unavoidable collision with rock pier
2. Blockage of Port entrance 3-7 days
3. Depending on Salvage operations:
   - Possible damage to the ship and environment
   - Substrate removal operations
   - Available tugboats

Cyber-SHIP Lab

UNIVERSITY OF PLYMOUTH

Economic consequences



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

Cyber-SHIP Lab

UNIVERSITY OF PLYMOUTH

Demo time

Q & A

Cyber-SHIP Lab

SECURING MARITIME

Thank you from the Cyber-SHIP Lab team!

For more information please contact:

Chloe Rowland

Cyber-SHIP Lab Project and Knowledge Exchange Manager

chloe.rowland@plymouth.ac.uk

UNIVERSITY OF PLYMOUTH