Cyber-SHIP Lab

SECURING MARITIME

Dr Kimberly Tam
Lecturer in Cyber-Security

56th EMPA General Meeting, 28th April 2022

UNIVERSITY OF PLYMOUTH

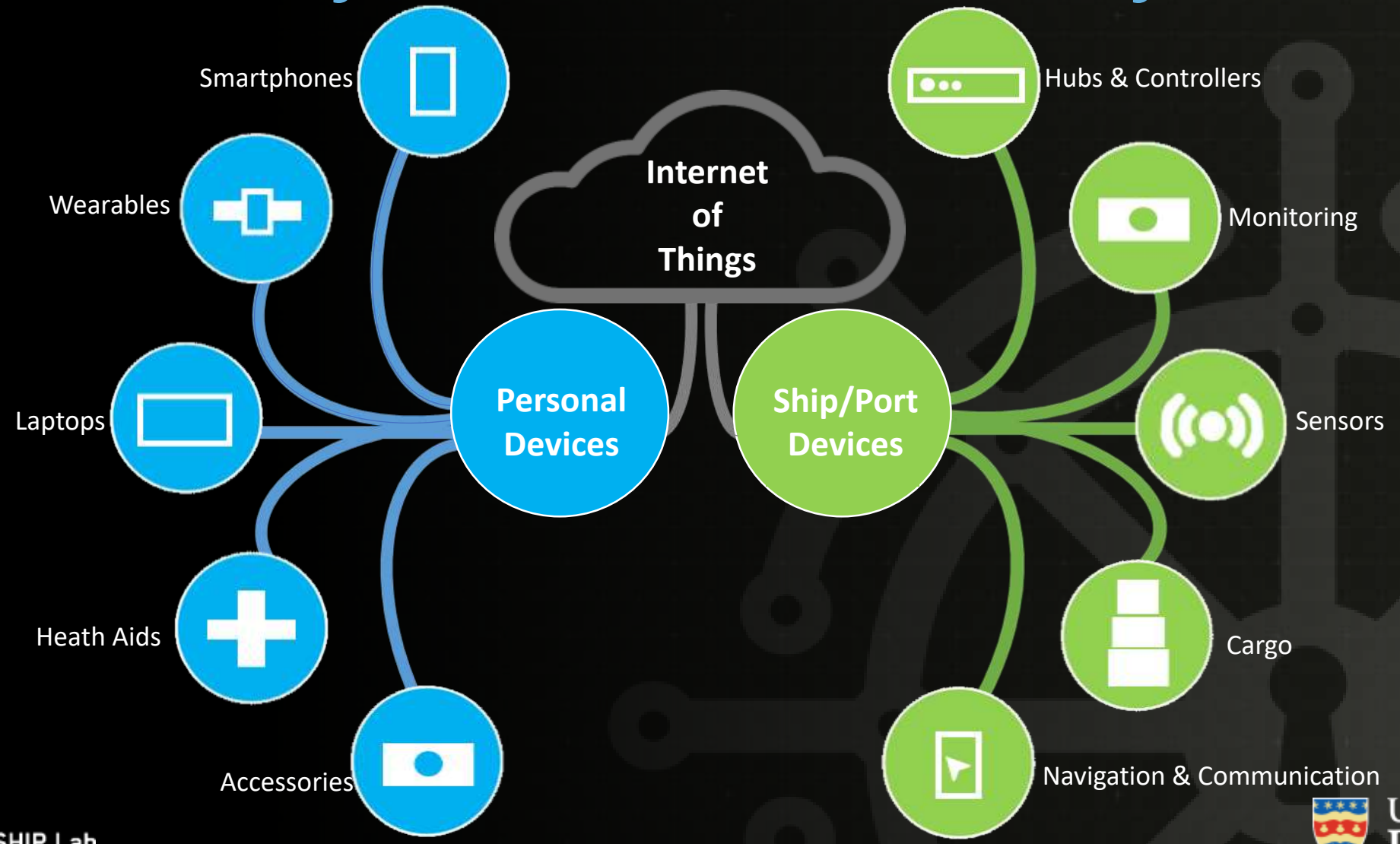
Maritime cyber attacks

UNIVERSITY OF PLYMOUTH

- **Growing exponentially**, with ports and ships
- Port of Barcelona in 2017, Maersk Not Petya in 2018, and CMA Ransomware in 2020 being recent high-profile examples
- Latest attack on CMA CGM means that all the Big-Four shipping lines, including MSC and COSCO, have suffered recent disruptive cyber events
- **90% of world-trade is moved by ship** and COVID has highlighted the fragility of supply chains
- Ships' complex and myriad system-of-systems present **many thousands of attack surfaces**

Cyber-SHIP Lab

Cybersecurity: increased connectivity



Cyber-SHIP Lab

UNIVERSITY OF PLYMOUTH

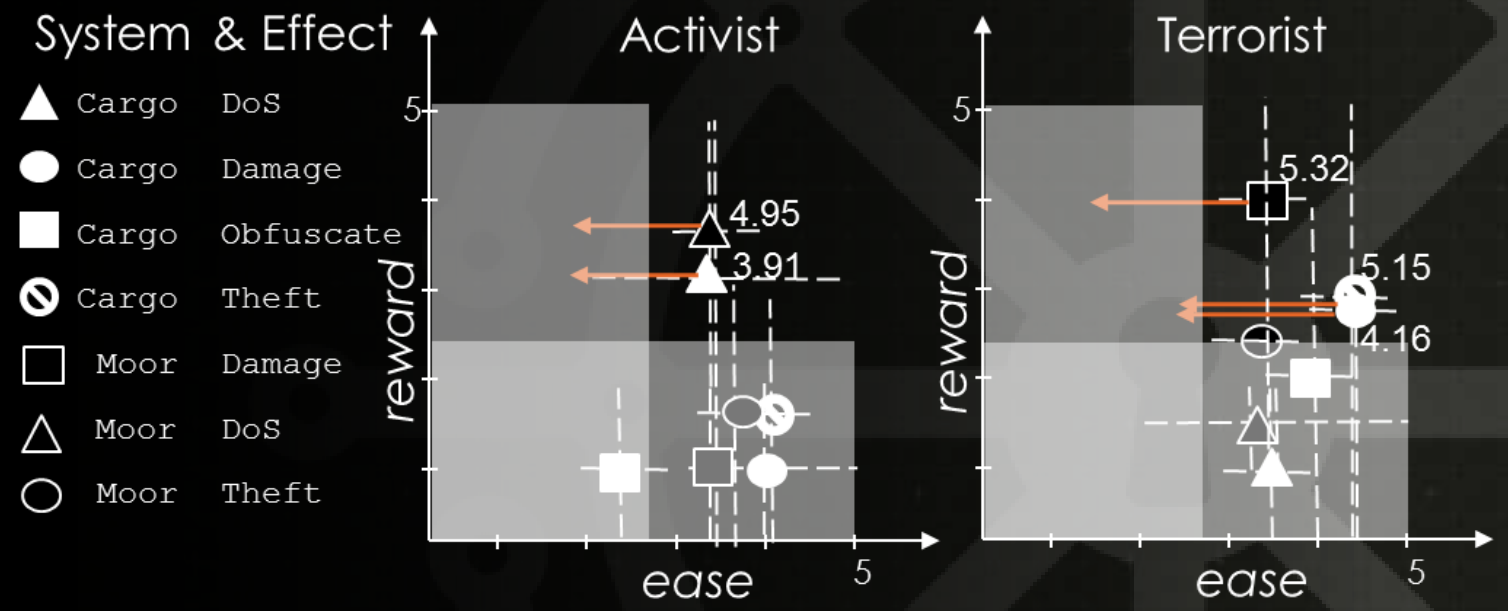
Ships and technology

- Ships have different functionalities
- Ships are equipped with different systems
- Ships travel through different locations
- Attackers have different interests
- Attackers have different resources levels

Each vessel has a dynamic risk profile that changes depending on circumstances

Maritime Cyber Threats Research Group

- The Maritime Cyber Threats Research Group at Plymouth is the largest of its kind globally – uniquely placed in the *understanding of risks to maritime vessels*, *port infrastructure* and national security
- Safeguarding the sector, this we are developing novel thinking around **Risk Assessment Frameworks**, and the new **Cyber-SHIP Lab** to deliver effective mitigation measures



Cyber-SHIP Lab

Cyber-SHIP Lab

SECURING MARITIME

Software
Hardware
Information
Protection

- Unique £3.2 million *hardware-based* testbed to cyber risk-assesses any ship's bridge
- *A configurable bridge* for research, software development and training facility
- Combines maritime tech with leading-edge cyber security research and practice
- Enhances understanding of maritime systems' cyber vulnerabilities
- *Actionable outputs*: knowledge and tools

UNIVERSITY OF PLYMOUTH

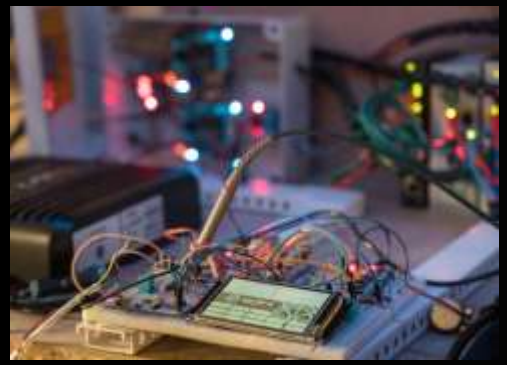
Cyber-SHIP Lab

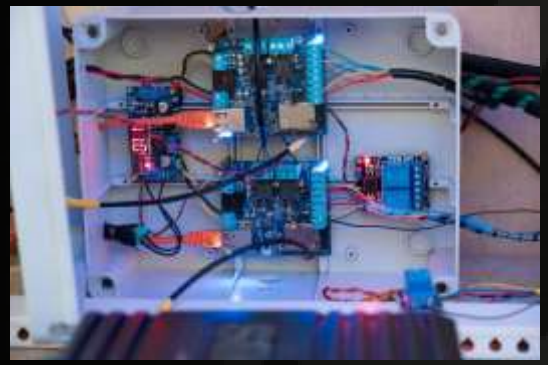
SECURING MARITIME

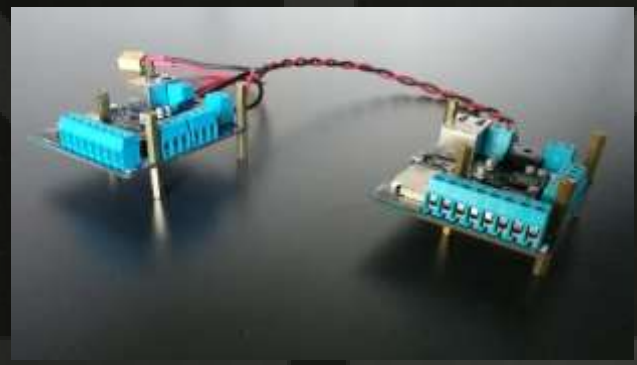
UNIVERSITY OF PLYMOUTH

Cyber-SHIP Lab

SECURING MARITIME







UNIVERSITY OF PLYMOUTH

Projects – EC H2020 Cyber-MAR

- Proposal Title: Cyber preparedness actions for a holistic approach and awareness raising in the maritime logistics supply chain {Cyber-MAR}
- Cyber-MAR is developing an innovate simulation environment for maritime logistics, combining a knowledge-based platform and decision support tool, incorporating novel risk analysis and econometric models.
- 13 Maritime logistics organisations will increase cyber awareness and validate their business continuity management in a six-million Euro Project
- Why ports? A recent hypothetical cyber attack on 15 major ports across Asia Pacific, estimate losses up to £90 billion (see; https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/shen-attack-cyber-risk-in-asia-pacific-ports).

Cyber MAR

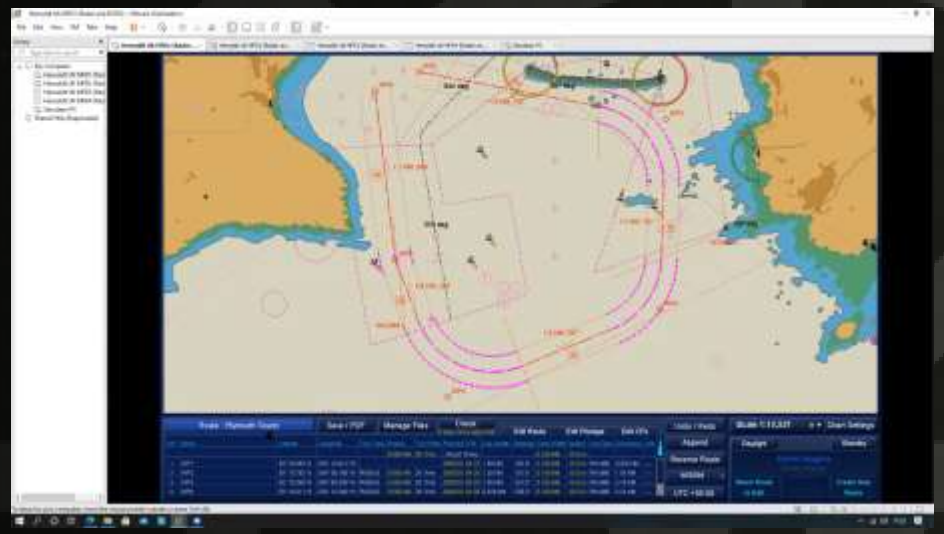
Cyber-MAR project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 833389. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

Rudder Control in Port of Valencia

This is a project cross-over with EU2020 Cyber-MAR

- Applying this to a specific scenario/pilot involving the port of Valencia
- Working closely with UoP Navigation for realistic approach / crew reactions

Portable ship simulator – Valencia charts

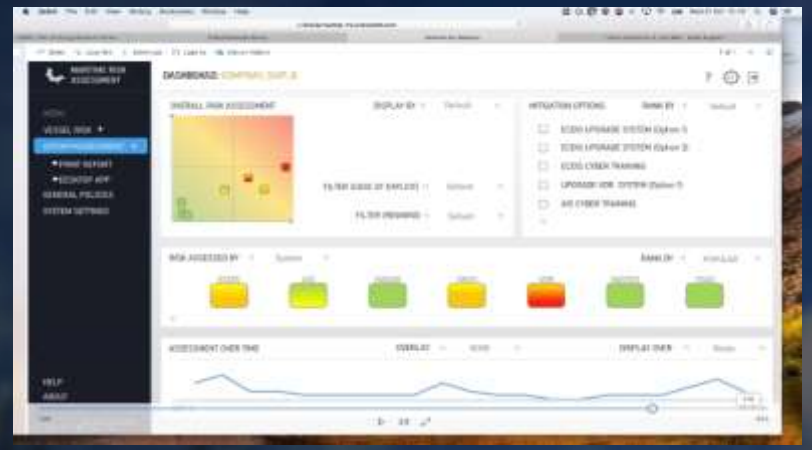


Kelvin Hughes / Hensoldt simulation - Plymouth

MaCRA®

MaCRA® uniquely provides **dynamic, multi-dimensional risk assessment tooling,** that uniquely addresses both **IT** and **OT (Operational Technology)** elements of a specific vessel **System**

Taking known **System** vulnerabilities and then cross-referencing them with threats associated with **Cargo transported,** and **Route** operated



Prototype Screenshots

The Plymouth “ecosystem”

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

Cyber-range lab

Exploits Tools

Cyber-SHIP Lab

Database

Ship simulators

Scenarios Training

Smart Sound

Autonomous/Remote control

Drones MAS

MaCRA
Risk assessment

Profiles Reports

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

Research Aims

- Cyber attacks are going unnoticed
  - Harden systems from tampering
  - Collect forensics to detect attacks
  - Use data to create investigation tools
  - Use data to create AI-based intrusion tools
  - Assess risks to prioritise vulnerabilities
  - Compliance/audit suite—regulator and insurance-ready tools
- IT/OT **convergence** significantly increases risks
  - Holistic understanding of connected *systems-of-systems*
  - Examine OT, not just IT
  - Examine security across hardware, software and people
- Cyber attacks encroaching into maritime sector
  - Smart ports / smart port cities
  - Autonomous ships
  - Internet-of-things; BYO-devices
  - Ship-to-shore and ship-to-ship interactions

Dr Kimberly Tam
Lecturer in Cyber security

Kimberly.tam@plymtouth.ac.uk
plymouth.ac.uk/research/cyber-ship-lab

Thank you