Cyber-SHIP Lab

SECURING MARITIME

Nor Shipping 2022

Prof Kevin D Jones
Dean of Science and Engineering
Head of Maritime Cyber Threats Research Group

UNIVERSITY OF PLYMOUTH

Cyber-SHIP Lab

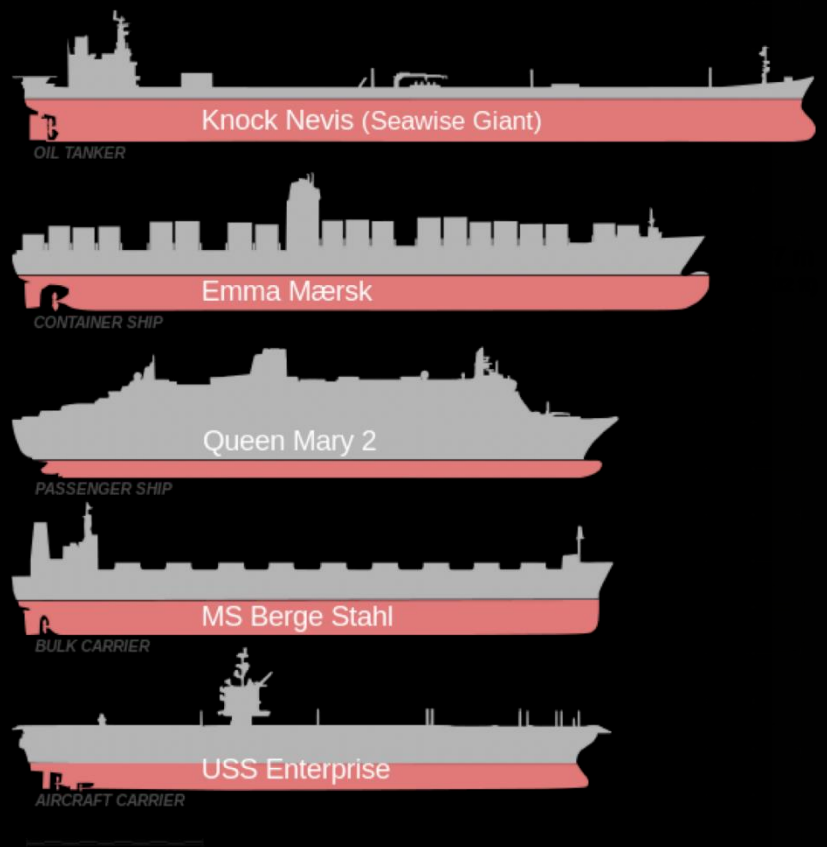
SECURING MARITIME

Software
Hardware
Information
Protection

- **Hardware-based** platform (or testbed) cyber risk-assesses and audit any ship's bridge
- **Endlessly configurable** 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

Ships and technology

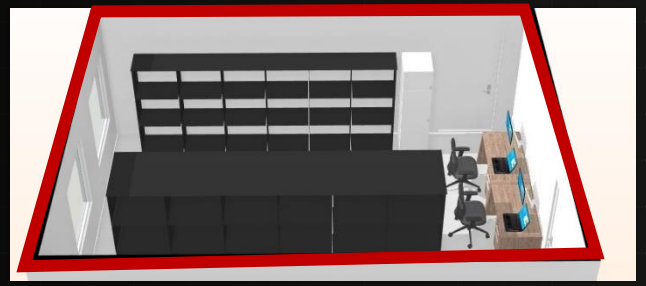


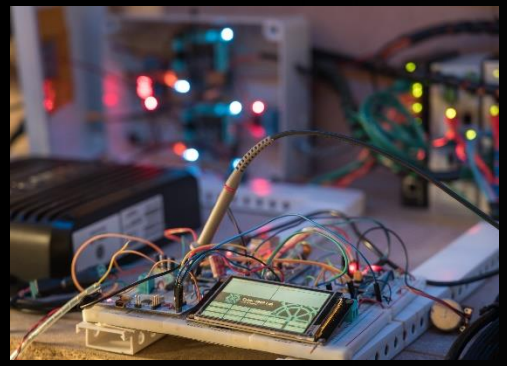
- Ships have different functionalities
- Ships are equipped with different systems
- Ships travel through different locations
- Attackers have different interests
- Attackers have different resources levels

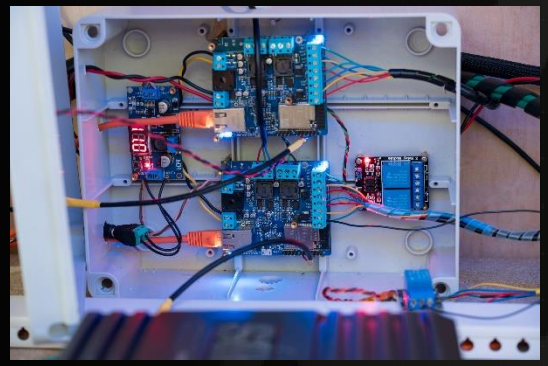
Each vessel has a dynamic risk profile that changes depending on circumstances and different vulnerabilities

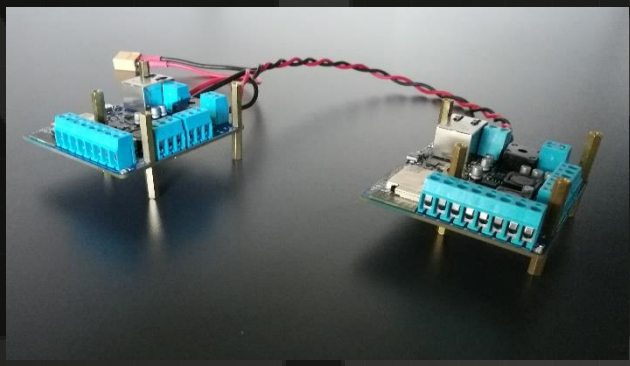
Cyber-SHIP Lab

SECURING MARITIME









UNIVERSITY OF PLYMOUTH

New Equipment here/arriving very soon

- 3 different **ECDIS** systems (WECDIS WAIS)
- Integrated Wartsila portable simulation
- Networking gear
- Secure storage (physical and digital)
- **Autonomous drones** (1 aquatic, 1 aerial)
- **Satellite connection** (Iridium)
- **AIS** (Automatic identification system) systems
- **VHF** (Very high frequency) Radios
- **PLCs** (programmable logic controller)
- Dedicated industrial Computers
- Reconfigurable **firewall** (different OS)
- New serial to Ethernet converters
- Custom designed electronics interfaces
- Visual and Audio devices for human-machine interactions
- USB Rubber ducky

Pen-testing Audit Suite

- Mostly manual but with **some automation**
- Currently testing on devices in the lab and **finding published vulnerabilities**
- A GUI to **scan the network**, **detect open ports** and generate html report as well as writing to a database
- **Executing exploits** for possible vulnerabilities to check if the execution is successful and how the system deals with it
- **Predicting attack paths**, finding vulnerabilities and obtaining a cyber security maturity level for the ship configuration (Future research)

Configuration System

- Currently researching into **electronically controlled communication links**
- Attempting to **physically switch communication** links through multiplexing techniques.
- Protocols to be switched include (but not limited to) Ethernet, HDMI, USB, RS232, RS485 and CAN bus.
- **Eventually leading to a fully configurable system at the touch of a button**, dynamically and physically linking ship/bridge equipment to create any bridge configuration over the network.
- Looking to expand this research to other sectors such as Aerospace

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).

This 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.

Scenario Demo

- Combination project with **Cyber-MAR** project
- Pulled in expertise in **cargo ship** and **container port operations**

Cyber MAR

Research aims

UNIVERSITY OF PLYMOUTH

Cyber attacks are going unnoticed

- Harden systems from tampering
- Collect forensics to detect attacks
- Use data to create investigation and 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 **and** 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

Cyber-SHIP Lab

The Plymouth "ecosystem"

UNIVERSITY OF PLYMOUTH

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

Cyber-range labs

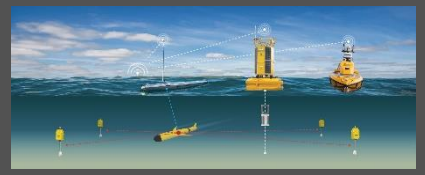
Exploits Tools

Cyber-SHIP Lab

Database

Ship simulators

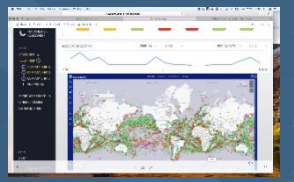
Scenarios Training



Smart Sound

Autonomous/Remote control

Drones MAS



Profiles Reports

MaCRA

Risk assessment

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

Cyber-SHIP Lab

SECURING MARITIME

Professor Kevin Jones

Executive Dean, Faculty of Science and Engineering and Cyber-SHIP Lab Principal Investigator

Dr Kimberly Tam

Lecturer in Cyber Security and Cyber-SHIP Lab Academic Lead

Kevin Forshaw

Director of Industrial and Strategic Partnerships, Faculty of Science and Engineering

Chloe Rowland

Project and Knowledge Exchange Manager, Cyber-SHIP Lab

Thank you

plymouth.ac.uk/research/cyber-ship-lab
cyber-ship-lab@plmymouth.ac.uk

UNIVERSITY OF PLYMOUTH