Cyber-SHIP Lab

SECURING MARITIME

UNIVERSITY OF PLYMOUTH

Dr Kimberly Tam

Lecturer in Cyber Security, Lead Academic – Cyber-SHIP Lab

Avanthika Vineetha Harish

Industrial Research Assistant – Penetration Testing

Chloe Rowland

Cyber-SHIP Lab Project and Knowledge Exchange Manager

University of Plymouth

Our roots go back over 150 years, but it is our contemporary relevance that gives us our energy and direction.

Our research is committed to addressing the multidisciplinary challenges of today and tomorrow - and informs an educational experience that places emphasis on practical, real-world experiential learning.

Over **145,000** alumni in 135 countries

Over **18,000** students

134 different nationalities

Over **2,500** staff

Maritime cyber attacks

UNIVERSITY OF PLYMOUTH

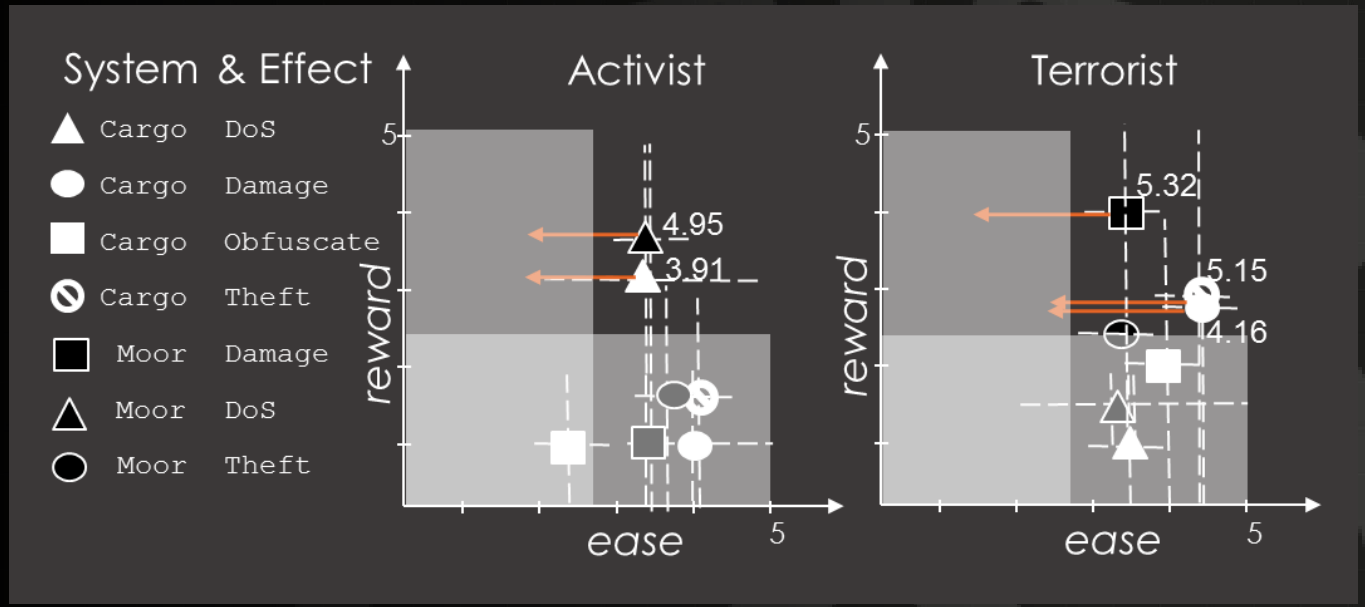
- **Growing exponentially**, with ports and ships experiencing costly attacks now on a monthly basis
- Port of Barcelona 2017; Maersk NotPetya 2018; Port Authority of London 2022
- All “Big-Four” shipping lines, including MSC, COSCO, CMA and CGM hit by recent disruptive cyber events
- **Ransomware** now a household word and becoming common in the sector
- **90% of world-trade moved by ship**—COVID highlighted the fragility of supply chains
- Ships’ complex system-of-systems present **a broad attack surface**

Cyber Skill Lab

Maritime Cyber Threats Research Group

UNIVERSITY OF PLYMOUTH

- **The Maritime Cyber Threats Research Group** at University of Plymouth is the largest of its kind globally
- Uniquely placed in the ***understanding of risks to maritime vessels, port infrastructure*** **and national security**
- Novel thinking around **Risk Assessment Frameworks**, and the **Cyber-SHIP Lab** to deliver effective mitigation measures to safeguard the sector



Cyber-SHIP Lab

General Research Aims

Founded in 1862 as the School of Navigation, UoP is one of the UK's largest universities

We combine cyber strengths with our Maritime heritage to:

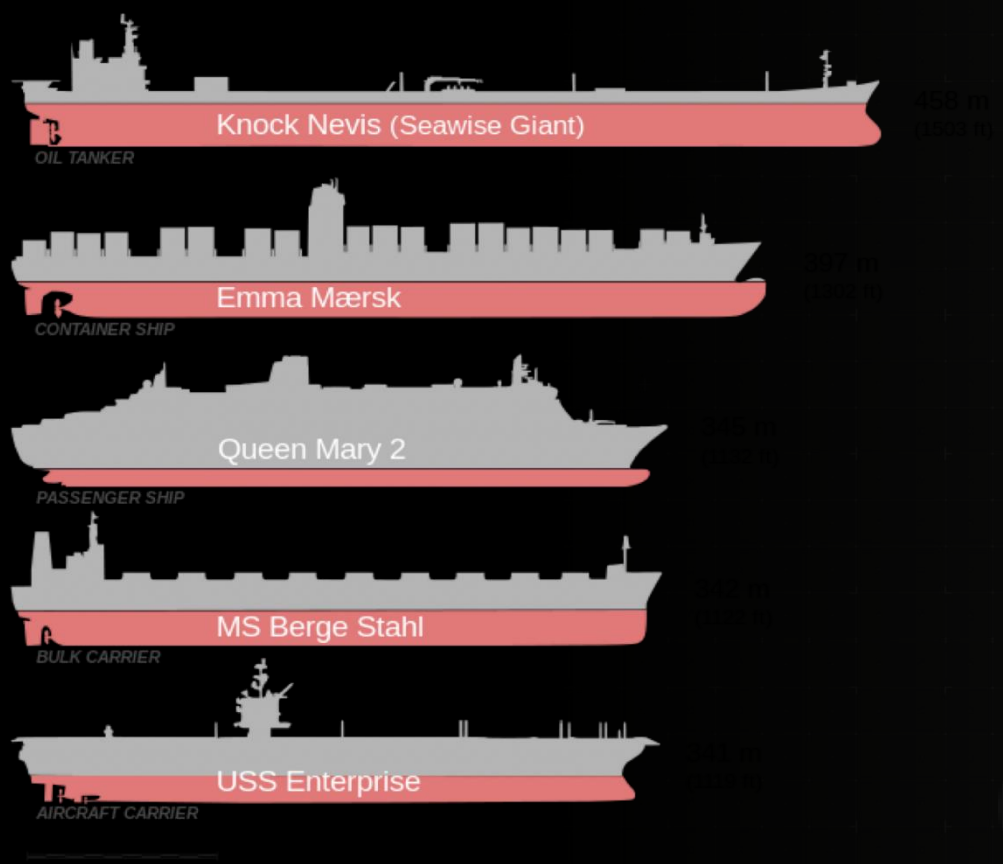
- Raise awareness/body of Knowledge
- Understand attackers & targets
- Assess the current security landscape
- Vulnerability, Risk Analysis and Intrusion Detection
- Individual systems, ship/fleet/port infrastructure, & supply chain
- Future technology (autonomy, IoT, augmented reality)
- Maritime Cyber-Security Training, Certification
- Maritime Cyber-Security Policy, Insurance, and Regulation

Security Lab / Cyber Range

Marine Navigation Suite

Cyber-SHIP Lab

Ships & 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

UNIVERSITY OF PLYMOUTH

Cyber-SHIP Lab

Cyber-SHIP Lab

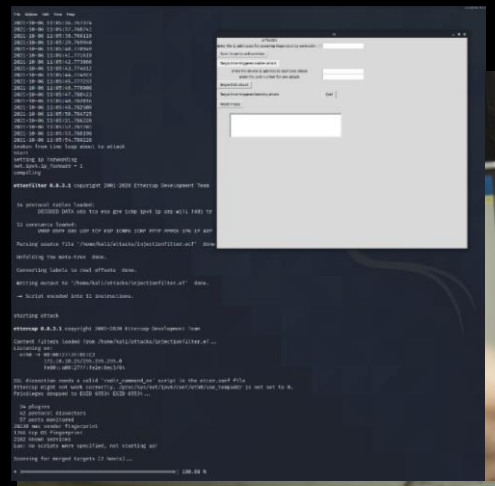
SECURING MARITIME

Software
Hardware
Information
Protection

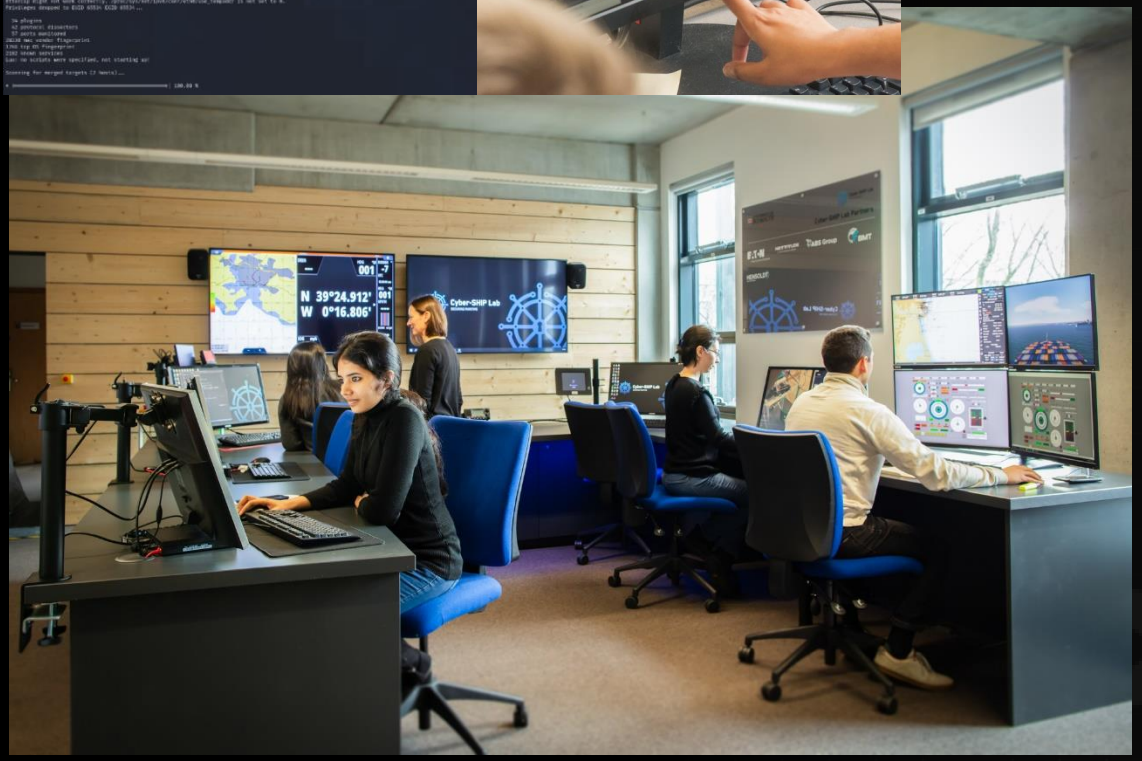
- Unique £3.2 million **hardware-based** platform: cyber risk-assessment of ships' systems
- **Configurable** research and training facility – physical twin
- Combines maritime tech with leading-edge cyber security research and practice to provide real-world solutions to real-world problems

UNIVERSITY OF PLYMOUTH

The Console Room



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



Cyber-SHIP Lab

UNIVERSITY OF PLYMOUTH

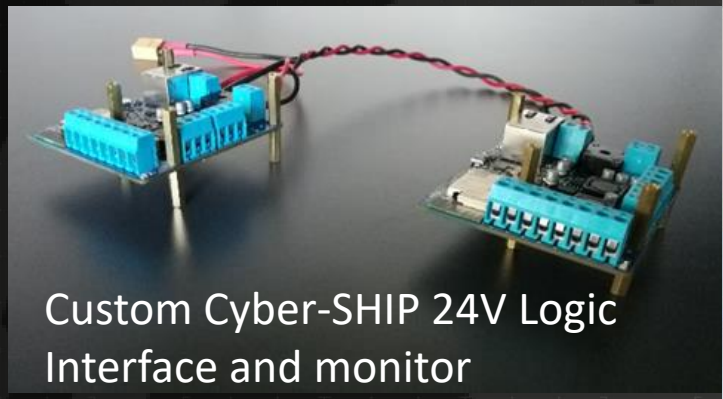
The Vault


Drones and USVs


Radar equipment


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
HENSOLDT


Data recovery from
ECDIS


FIRST
AID
POINT


AIS
Static Data
Link Settings
Encryption Keys
Region IDs
W-AIS Installation
Secure Time (UTC)
Main
Back
W-AIS Configuration


SatCom


NAVTEX/AIS

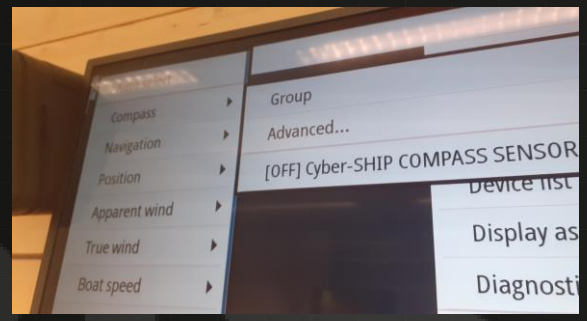
#228301

Current status – Sept 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…*

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

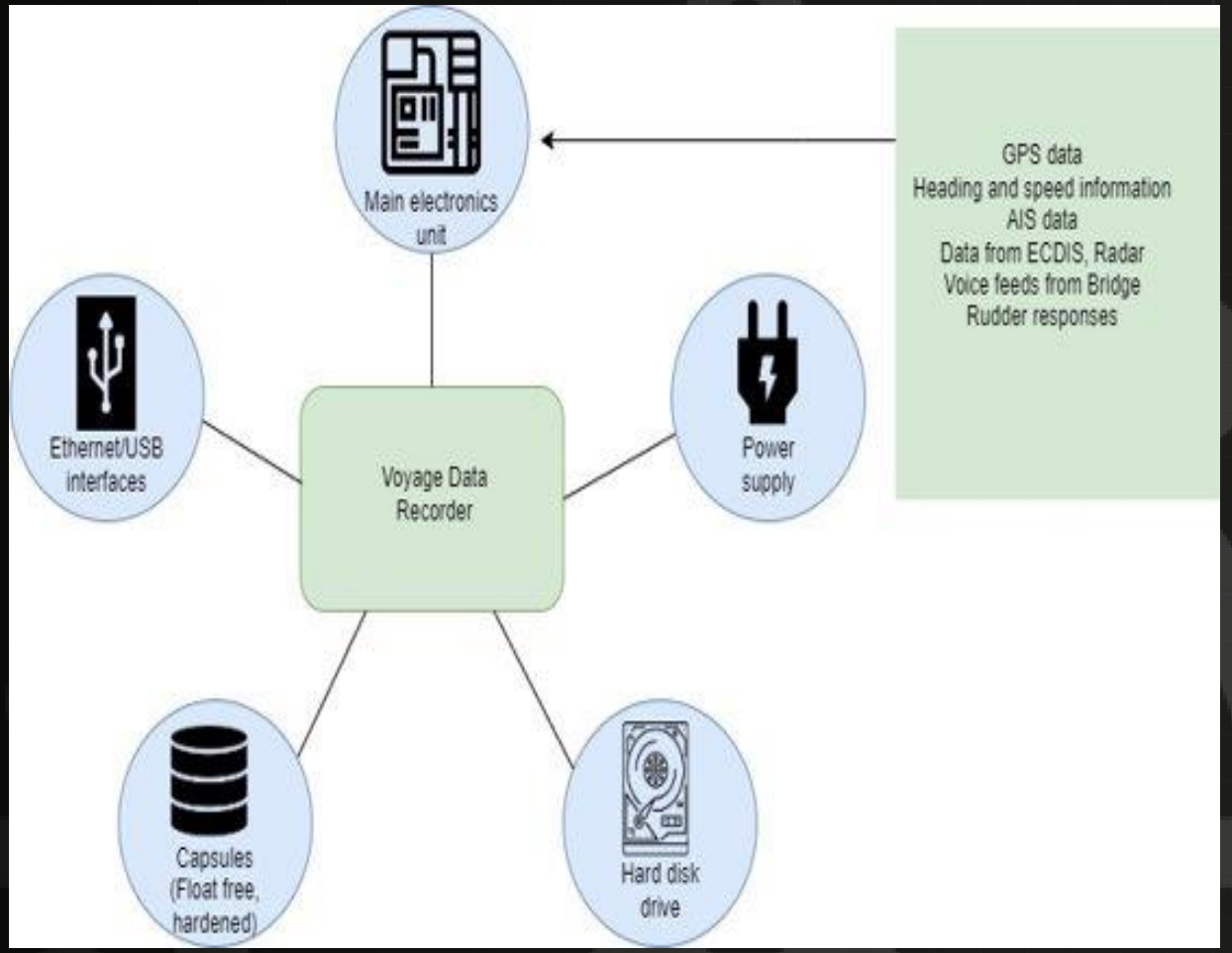
Software Defined Radio

Rubber Ducky

Cyber-SHIP Lab

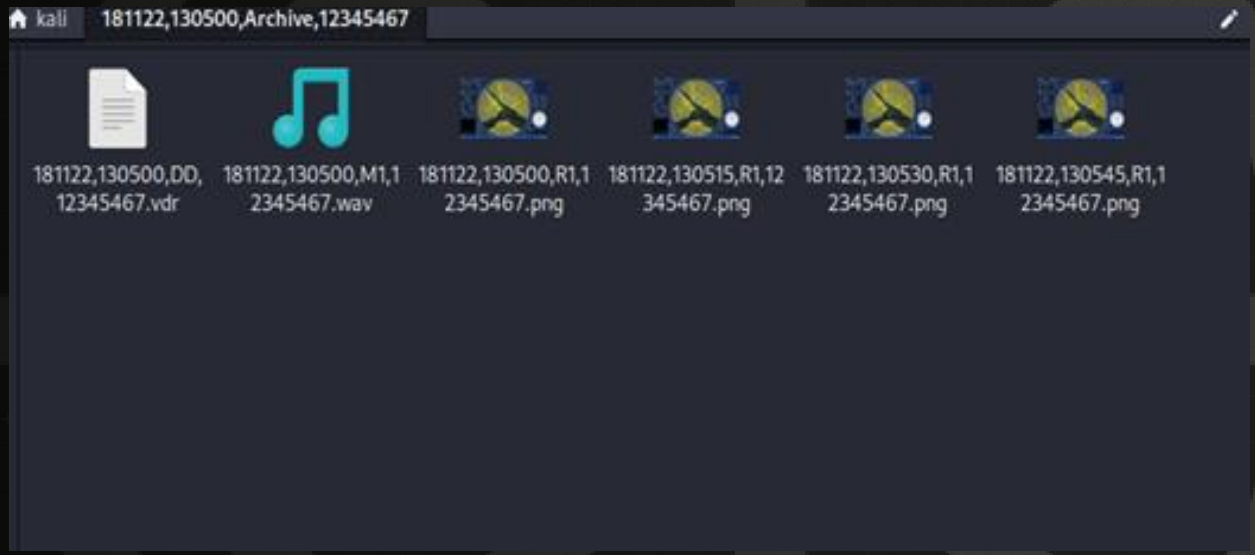
Voyage Data Recorders (VDRs)

- '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



The Plymouth “ecosystem”

UNIVERSITY OF PLYMOUTH

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

Cyber-range labs

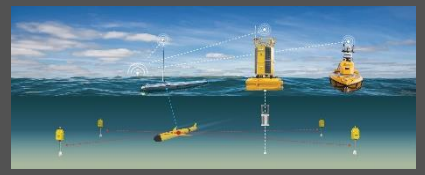
Exploits Tools

Cyber-SHIP Lab

Database

Ship simulators

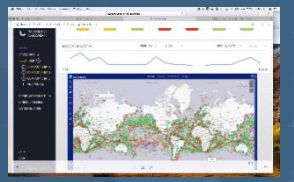
Scenarios Training



Smart Sound

Autonomous/Remote control

Drones MAS



Profiles Reports

MaCRA

Risk assessment

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

Cyber-SHIP Lab

MaCRA: Model-Based Risk Assessment

UNIVERSITY OF PLYMOUTH
Faculty of Science and Engineering

- **MaCRA (Maritime Cyber Risk Assessment) framework uniquely provides dynamic, multi-dimensional risk assessment tooling, that uniquely addresses both IT and OT elements of a specific vessel system, by factoring in threat associated with cargo transported, and route operated**

1

System Vulnerability

- AIS
- ECDIS
- IBS Internet
- GNSS
- GMDSS
- …

2

Ease of Exploit

- Attacker members
- Attacker resources
- Target defences
- Target location
- …

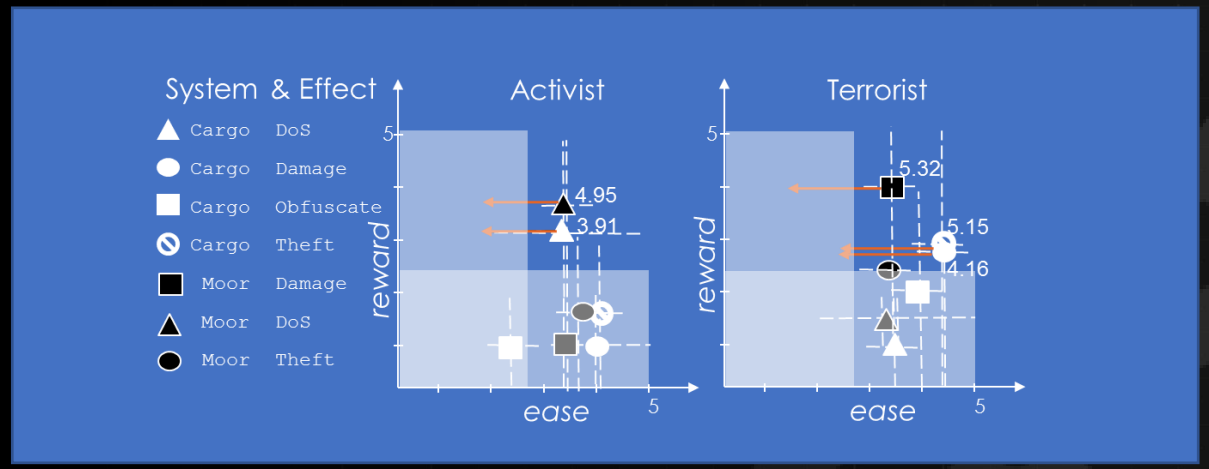
3

Attacker Reward

- Profit
- Collision/Damage
- Denial of Service
- Misdirection
- Obfuscation
- …

Published in 2019

Combining known issues at System level, with Threats posed by Cargo and Route gives real insight into Risk



An analysis of the three autonomous ships showed us the likely risk profile, indicating where attention is most needed

From the risks presented by our model, mitigation can be helped with attention to:

- Secure satellite communications
- Secure environment sensors
- Secure AIS

Events that may push low-risks into high-risk zones included Vulnerability in cargo loading …

Engagement with the university and industry

- Contract Research, Consultancy and PhDs
- Standard Academic programmes, Masters, MRes, PhD
- Bespoke training
- Joint public research
- Scenario development
- Engagement with Armed Forces
- Use of Cyber-SHIP Lab with University team
- Commercial MaCRA services

Cyber-SHIP Lab

SECURING MARITIME

Dr Kimberly Tam

Lecturer in Cyber Security, Lead Academic – Cyber-SHIP Lab

kimberly.tam@plymouth.ac.uk

Avanthika Vineetha Harish

Industrial Research Assistant – Penetration Testing

avanthika.vineethaharish@plymouth.ac.uk

Chloe Rowland

Cyber-SHIP Lab Project and Knowledge Exchange Manager

chloe.rowland@plymouth.ac.uk

Thank you

UNIVERSITY OF PLYMOUTH

Cyber-MAR: A Real World Attack Scenario

Cyber-MAR project has received funding from the European Union's Horizon 2020 research and innovation program 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.