# Maritime Cyber Research at the University of Plymouth

## WORKING WITH MARITIME STAKEHOLDERS TO IMPROVE RESILIENCE FOR THE SECTOR

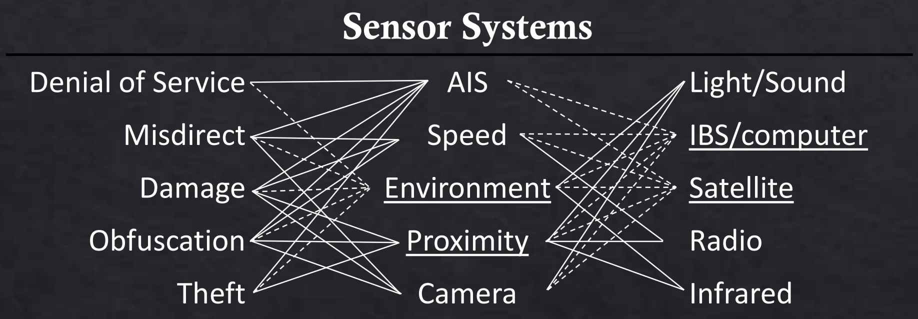
The SMART SHIP Exchange, Athens Greece, 10-11 October

Kevin Forshaw

world
ports
nature
trustworthiness
growth
investigation
mariners
ship
research
tools
quantitative
framework
IT
factors
cyber
evidence
digitization
configurations
Classified
trade
readiness
hackers
post-analysis
forensic
risk
efficient
IoT
OT
data
cyber-threats
threats
range
issue
sector
cyber-physical
cyber-risks
maritime
operational
unique
users
Training
capabilities
cyber-risk
mitigation
cybersecurity
operators
global
digital
represent
operations
aware
economy
industry
autonomous
functionalities
support
dynamic
vulnerabilities
ships
measure
owners
assessment
shipping
decisions
maritime-cyber
regulators
automation
sector
community
analysis
technological
safety
methods
Simulation
environmental
profiles
insurers
hazards
scenarios
model-based
importance

# Cybersecurity: Autonomous

## Technical Research



**Sensor Systems**

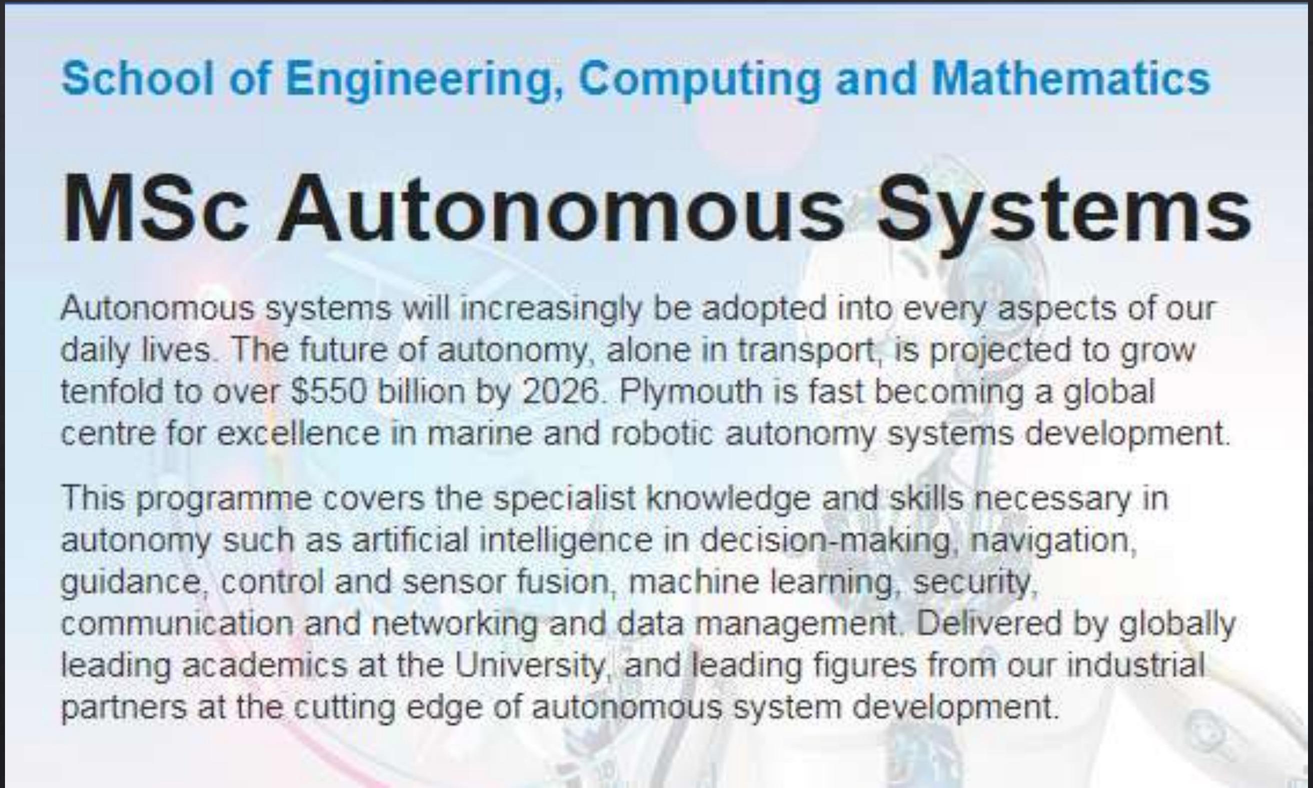
Denial of Service  
Misdirect  
Damage  
Obfuscation  
Theft

AIS  
Speed  
Environment  
Proximity  
Camera

Light/Sound  
IBS/computer  
Satellite  
Radio  
Infrared

- ⟐ How is technology changing?
- ⟐ Cyber-threat landscape?
- ⟐ How does this affect risks?

## Socio-Technical Training



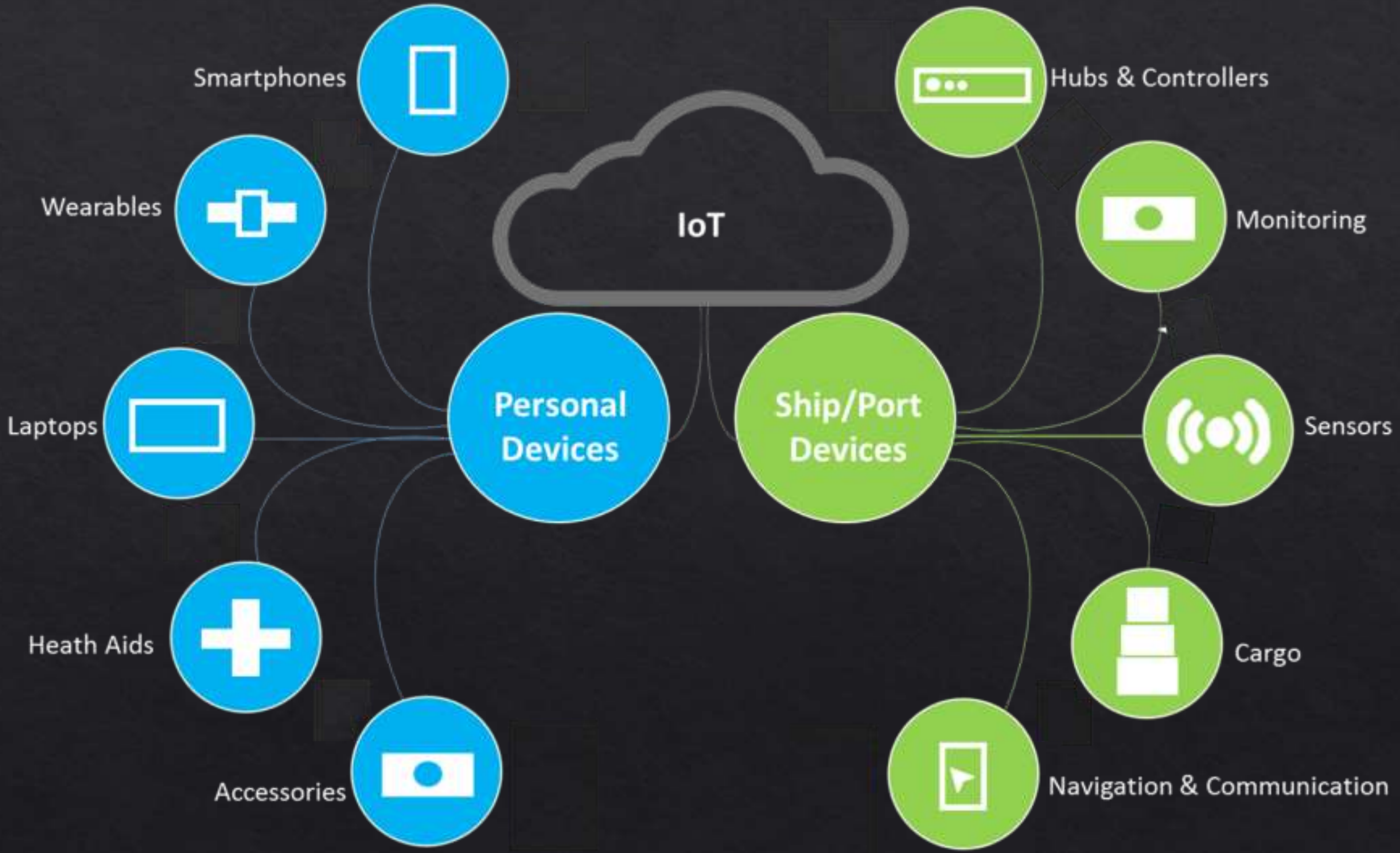
School of Engineering, Computing and Mathematics

# MSc Autonomous Systems

Autonomous systems will increasingly be adopted into every aspects of our daily lives. The future of autonomy, alone in transport, is projected to grow tenfold to over $550 billion by 2026. Plymouth is fast becoming a global centre for excellence in marine and robotic autonomy systems development.

This programme covers the specialist knowledge and skills necessary in autonomy such as artificial intelligence in decision-making, navigation, guidance, control and sensor fusion, machine learning, security, communication and networking and data management. Delivered by globally leading academics at the University, and leading figures from our industrial partners at the cutting edge of autonomous system development.

# Cybersecurity: Increased Connectivity



# Projects – EC H2020 Cyber-MAR

**Proposal Title: Cyber** preparedness actions for a holistic approach and awareness raising in the **MAR**itime logistics supply chain **{Cyber-MAR}**

- Cyber-MAR will develop 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 6 Million Euro Project or which 650 K Euro will go to Plymouth for a forensics lab, able to host a number of virtual machines and a portable ship simulator.

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*

# New Cyber-SHIP Lab at Plymouth
## (Software, Hardware, Information and Protection)

- The Cyber-SHIP Lab will combine maritime technology with leading-edge thinking from cyber-security - A national resource for research and training, encouraging opportunities for ongoing maritime-cyber consultancy and research to safeguard the sector going forward.
- A key component is our intention to obtain necessary systems and hardware that can be configured to become a ship's bridge - complementing our Ship's Bridge Simulator, bringing together key equipment readily used in today's fleet that can then be configured in vessel-specific layouts.
- Unique facility to determine key vulnerabilities when subjected to a range of attacks, leading to the development of safeguards at technical, system and operational level.

CYBER-SHIP
Lab

# Research Aims

**Awareness/Body of Knowledge**

- Who are the attackers & targets?
- What is the current security landscape?

**Vulnerability and Risk Analysis**

- Individual systems
- Ship/Fleet/Port (infrastructure) security
- Supply Chain
- Future technology (Autonomy, IoT, augmented reality)

**Maritime Cyber-Security Training, Certification**

- Regional & International

**Maritime Cyber-Security Policy, Insurance, and Law**

- Regional & International

**Malware/Intrusion detection and defences/mitigation**

Security Lab / Cyber Range

Marine Navigation Centre

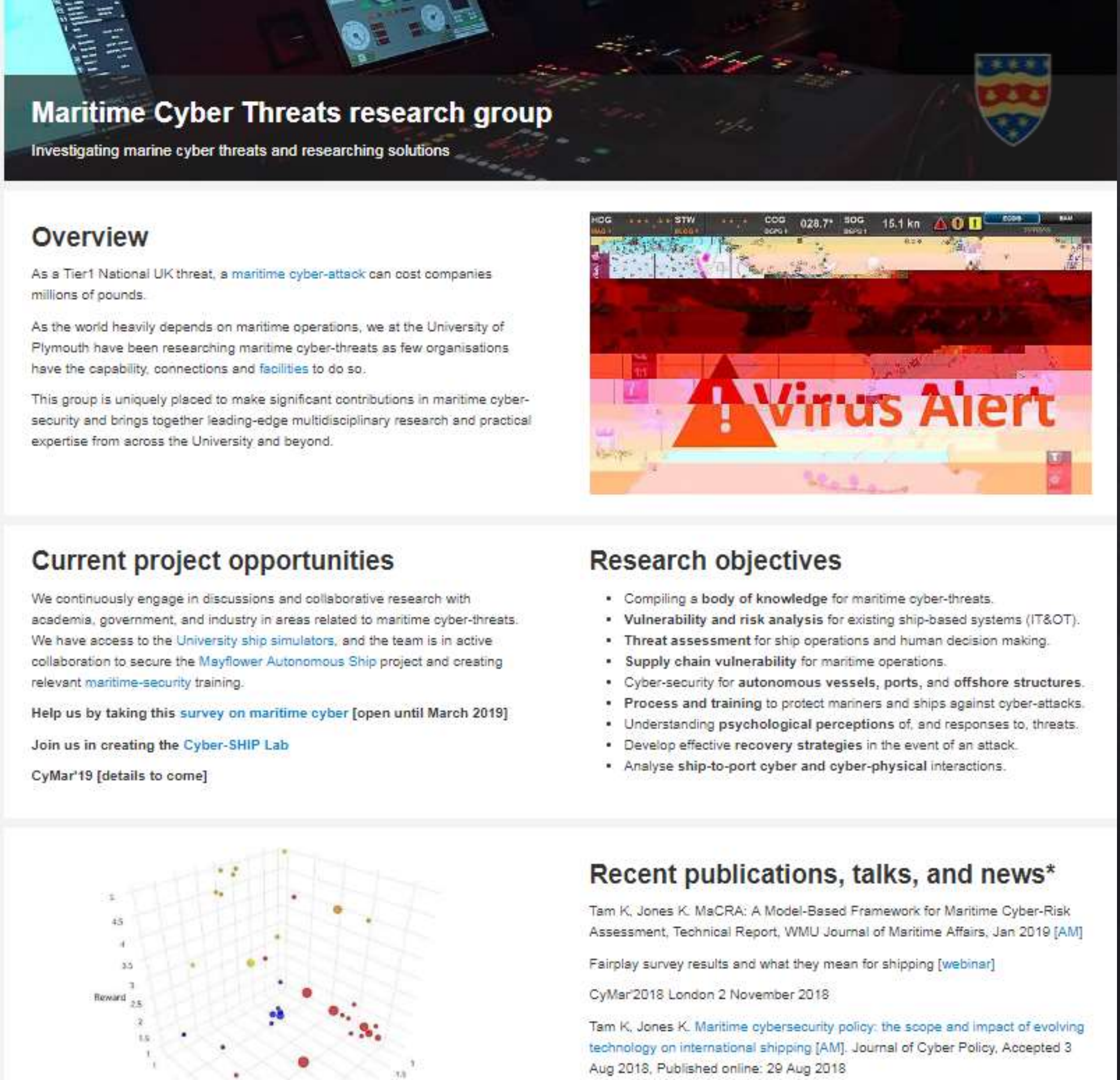
# Awareness & Risk Research

- **Incidents and attacks**
  - Threats and Impacts in Maritime Cyber Security, IET Engineering & Technology, April 2016
  - YouTube videos of simulated cyber-attack scenarios
- **Risk assessment**
  - MaCRA: A Model-Based Framework for Maritime Cyber-Risk Assessment, WMU Journal of Maritime Affairs, January 2019
  - "Forensic Readiness within the Maritime Sector ", IEEE Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), Oxford, 2019
  - "Factors Affecting Cyber Risk in Maritime ", IEEE Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), Oxford,2019 [journal version accepted IJCSA]

# Awareness & Risk Research

- **Evolving technology (autonomous ships) and policy**
  - Cyber-Risk Assessment for Autonomous Ships, Cyber Security, 2018
  - Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping, Journal of Cyber Policy, 2018
  - Cyber-SHIP: Developing Next Generation Maritime Cyber Research Capabilities, ICMET 2019
  - A Cyber-Security Review of Emerging Technology in the Maritime Industry, International Conference of Maritime Science & Technology  Nase More 2019

**Overall awareness of Maritime Cyber-Security is improving.**
**Future research will be using risk analysis to solve important problems.**



## Maritime Cyber Threats research group

Investigating marine cyber threats and researching solutions

### Overview

As a Tier1 National UK threat, a maritime cyber-attack can cost companies millions of pounds.

As the world heavily depends on maritime operations, we at the University of Plymouth have been researching maritime cyber-threats as few organisations have the capability, connections and facilities to do so.

This group is uniquely placed to make significant contributions in maritime cyber-security and brings together leading-edge multidisciplinary research and practical expertise from across the University and beyond.

### Current project opportunities

We continuously engage in discussions and collaborative research with academia, government, and industry in areas related to maritime cyber-threats. We have access to the University ship simulators, and the team is in active collaboration to secure the Mayflower Autonomous Ship project and creating relevant maritime-security training.

**Help us by taking this survey on maritime cyber [open until March 2019]**

**Join us in creating the Cyber-SHIP Lab**

**CyMar'19 [details to come]**

### Research objectives

- Compiling a **body of knowledge** for maritime cyber-threats.
- **Vulnerability and risk analysis** for existing ship-based systems (IT&OT).
- **Threat assessment** for ship operations and human decision making.
- **Supply chain vulnerability** for maritime operations.
- Cyber-security for **autonomous vessels, ports,** and **offshore structures.**
- **Process and training** to protect mariners and ships against cyber-attacks.
- Understanding **psychological perceptions** of, and responses to, threats.
- Develop effective **recovery strategies** in the event of an attack.
- Analyse **ship-to-port cyber and cyber-physical** interactions.

### Recent publications, talks, and news*

Tam K, Jones K. MaCRA: A Model-Based Framework for Maritime Cyber-Risk Assessment, Technical Report, WMU Journal of Maritime Affairs, Jan 2019 [AM]

Fairplay survey results and what they mean for shipping [webinar]

CyMar'2018 London 2 November 2018

Tam K, Jones K. Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping [AM]. Journal of Cyber Policy, Accepted 3 Aug 2018, Published online: 29 Aug 2018

# Thank You

Kevin Forshaw

Kevin.Forshaw@plymouth.ac.uk

UoP Website :

https://www.plymouth.ac.uk/research/maritime-cyber-threats-research-group

www.Cyber-MAR.eu

Cyber_MAR

Cyber-MAR