UNIVERSITY OF PLYMOUTH

Faculty of Science and Engineering

# Maritime Cyber Threats research group

Prof Nathan Clarke and Mr Steve Rice

# Ships & Technology

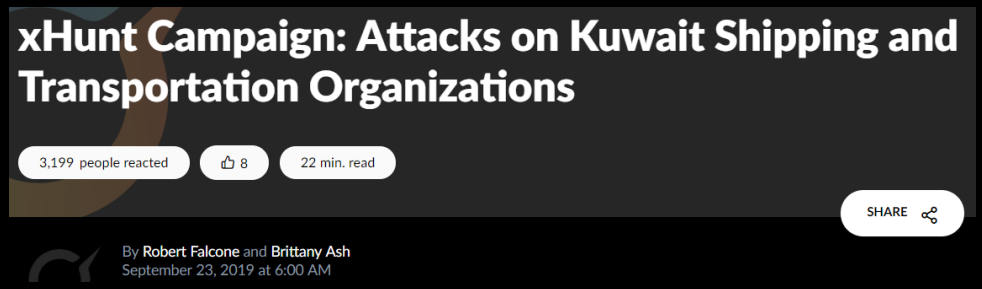
UNIVERSITY OF PLYMOUTH
Faculty of Science and Engineering

# Modern Maritime-Cyber Threat

Ships are becoming bigger and/or more technologically advanced.

Technological aids and autonomous tools are being added for navigation, cargo handling, communication, and safety.

This, paired with the remote mobile nature of ships creates a unique maritime cyber-security landscape.



**xHunt Campaign: Attacks on Kuwait Shipping and Transportation Organizations**

3,199 people reacted | 8 | 22 min. read

SHARE

By Robert Falcone and Brittany Ash
September 23, 2019 at 6:00 AM

**Iran spoofing ship GPS signals, warns US**

*The US Maritime Administration warns of 'spoofed bridge-to-bridge' communications from 'unknown entities falsely claiming to be US or coalition warships'. Despite not naming Iran as the source, Marad's advisory listed six incidents since May attributed to the country*

08 Aug 2019 | NEWS

DAILY NEWS 10 August 2017

**Ships fooled in GPS spoofing attack suggest Russian cyberweapon**

UNIVERSITY OF PLYMOUTH
Faculty of Science and Engineering

# Research Aims

UNIVERSITY OF PLYMOUTH
Faculty of Science and Engineering

**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

UNIVERSITY OF PLYMOUTH
Faculty of Science and Engineering

- **Global fleet equipment, statistics**
  - Collaboration with industry and universities
- **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
- **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

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

# Plymouth's Leading Approach to Model-Based Risk Assessment

- A pioneering Model-based approach to characterize and quantify risk to specific operation and vessel type
- Based on three parameters to determine actual risk and focus for mitigation actions
- Model ship (target) and attacker

**System Vulnerability**

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

**Ease of Exploit**

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

**Attacker Reward**

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

UNIVERSITY OF PLYMOUTH
Faculty of Science and Engineering

# 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.

UNIVERSITY OF PLYMOUTH
Faculty of Science and Engineering

Cyber MAR

# Outputs from Cyber-MAR

**Proposal Title: Cyber-MAR**

O1. Enhance capabilities of cybersecurity professionals and raise awareness on cyber-risks

O2. Assess cyber-risks for operational technologies (OT)

O3. Quantify the economic impact of cyber-attacks across different industries with a focus on port disruption

O4. Promote cyber-insurance market maturity in the maritime logistics sector (adaptable to other transport sectors as well)

O5. Establish and extend CERTs/CSIRTs, competent authorities and relevant actors collaboration and engagement

EU grant in total value of €6M (€644k for Plymouth)

UNIVERSITY OF PLYMOUTH
Faculty of Science and Engineering

Cyber MAR

# 'Designing out' Cyber Threats to Businesses and Personal Data – ISCF Call

- £70 million Digital Security by Design challenge will be delivered by UK Research and Innovation through the Industrial Strategy Challenge Fund
- A further £30.6 million Ensuring the Security of Digital Technology at the Periphery programme will be delivered by UK Research and Innovation
- This supporting the development of collaborative research between leading industry and research players to increase UK share of a global market predicted to grow to £39 billion in a decade


UNIVERSITY OF PLYMOUTH
Faculty of Science and Engineering

# Improve Cyber Security in the Internet of Things / More Resilient, Intelligent Systems

- The competition aims to join up the UK's research base with industry to transfer knowledge and develop new products and services that tackle cyber security in the IoT.
- Projects should include artificial intelligence or machine learning and have a clear plan for commercialisation and can include operational resilience technologies that can protect and recover data
- Projects could also look at complementary technologies, such as distributed ledger technologies that support the sharing of data across multiple locations, or 5G mobile networks.


UNIVERSITY OF PLYMOUTH
Faculty of Science and Engineering

# 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.
- This unique facility can then be used to determine key vulnerabilities when subjected to a range of attacks, leading to the development of safeguards at technical, system and operational level.

UNIVERSITY OF PLYMOUTH
Faculty of Science and Engineering

# Benefits of Engaging with **Cyber-SHIP Lab**, Our Stakeholder Community

- **Ship Builders and Component Technology Supply Chain**
- **Shipping Operators and Port Infrastructure**
- **Classification Agencies**
- **Insurers**
- **Policy and Regulatory Organisations**

## Benefits

- Using outputs of research to develop resilience and risk-mitigation from a 'System of Systems' approach
- Using outputs of research and training to minimise risk to business operation and ensure safety of crew
- Leading development of future standards for the sector
- Insight into social and technical best practice to mitigate risk, and risk modelling
- Insight into social and technical best practice to shape policy and safeguard National Security

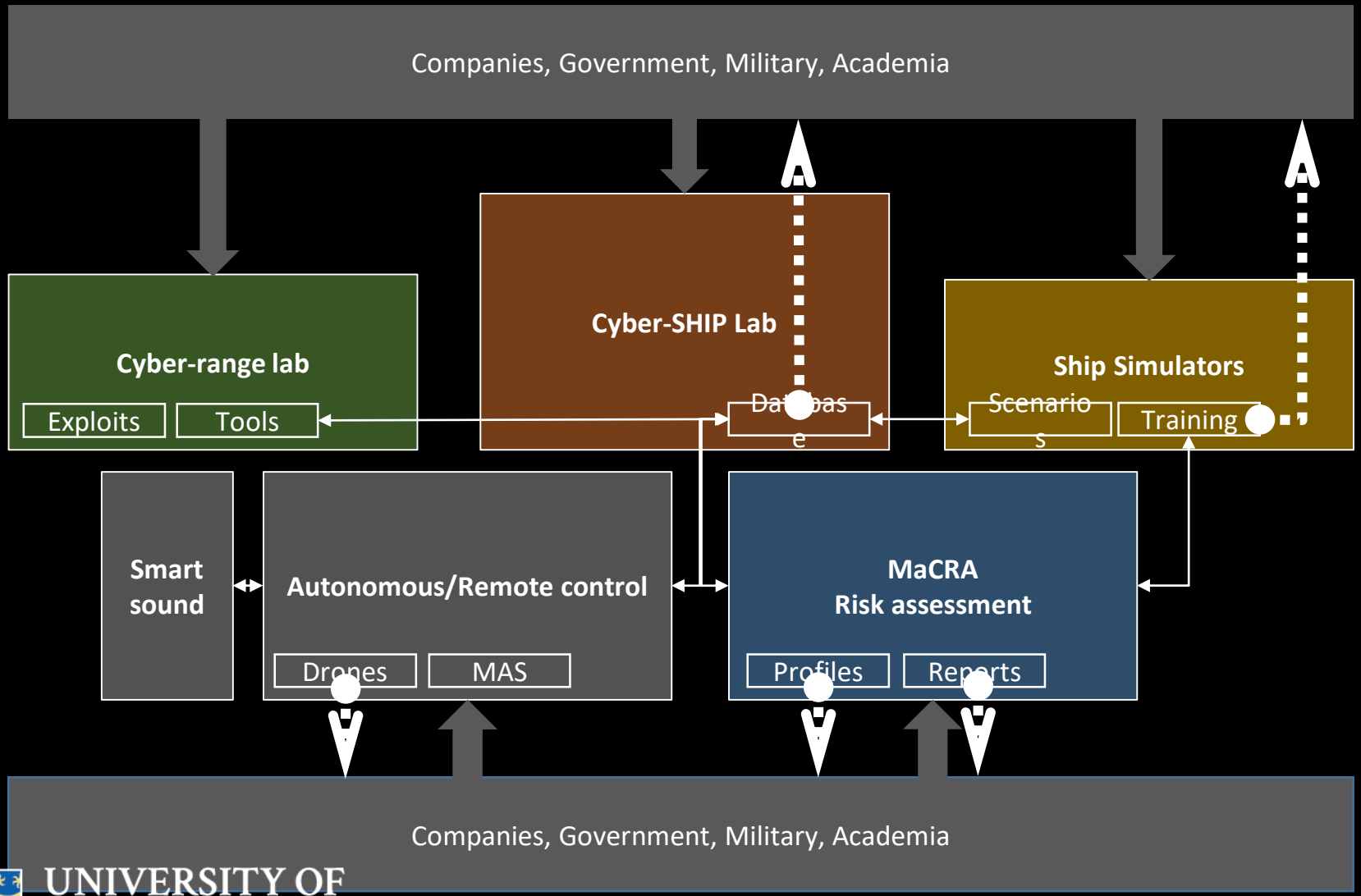
UNIVERSITY OF PLYMOUTH
Faculty of Science and Engineering

# Join with us in the creation of the Cyber-SHIP Lab

- University of Plymouth has an unrivalled track-record of industry engagement translating research into everyday societal benefit. We are now actively seeking partners to join with us in the creation of the Cyber-SHIP Lab.

- Whether your interest is in shaping future collaborative research, meeting future training needs, or to ensure equipment resilience, please contact us to discuss how your organisation can be engaged.

UNIVERSITY OF PLYMOUTH
Faculty of Science and Engineering




UNIVERSITY OF PLYMOUTH
Faculty of Science and Engineering

# Thank You

**Prof Nathan Clarke**
Deputy Head of School
(Engineering, Computing and Mathematics)
N.Clarke@plymouth.ac.uk

**Mr Steven Rice**
Marine-i Project Manager
Steven.rice@Plymouth.ac.uk

**Find out more**

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

www.Cyber-MAR.eu

Cyber_MAR