



Cyber-SHIP: Developing Next Generation Maritime Cyber Research Capabilities

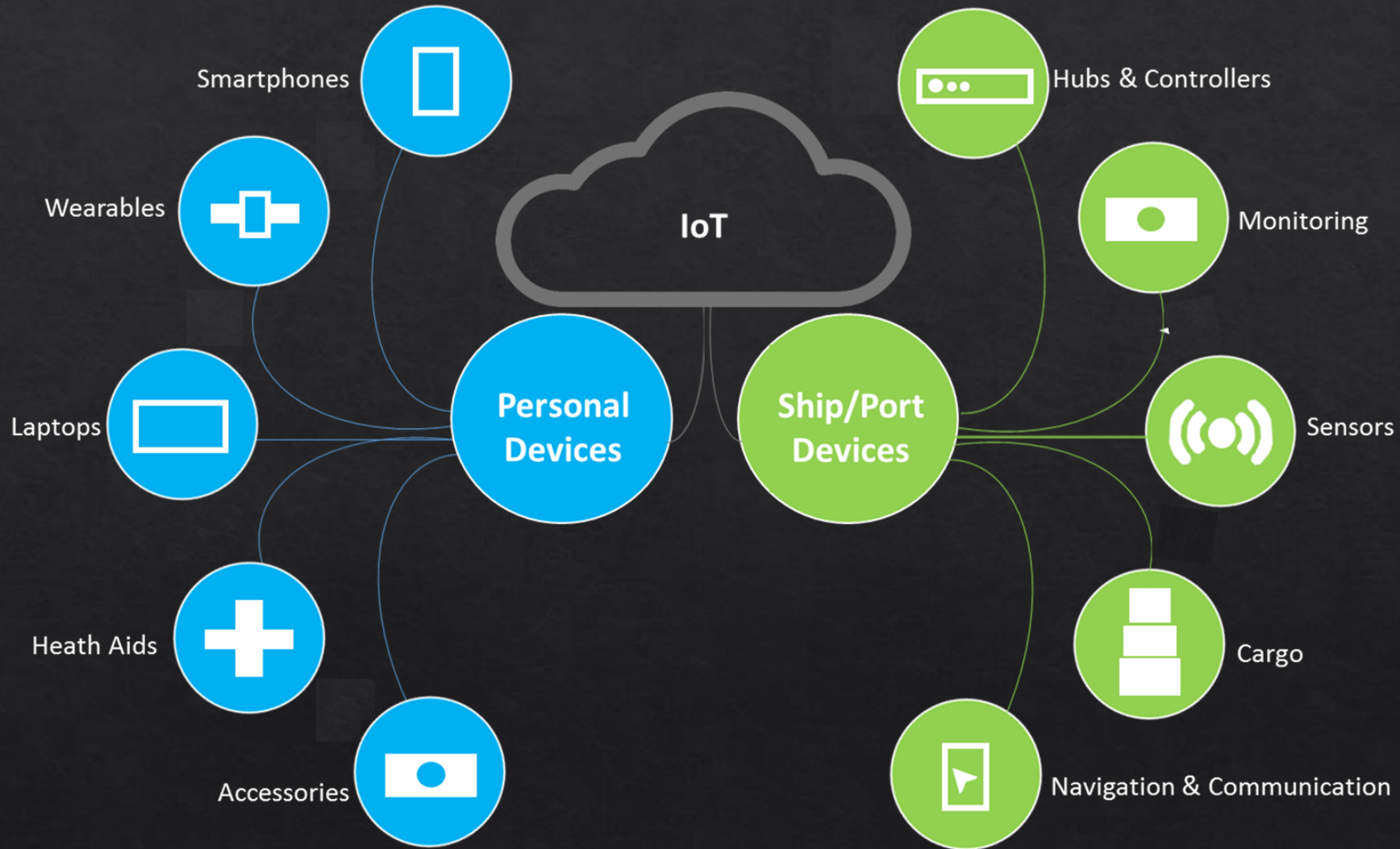
ICMET Oman 2019, 5-6 November

Prof Kevin Jones

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



More Devices and Connectivity



Maritime-Cyber Research Challenges

- ◆ Risk assessment/management of maritime cyber threats (cyber, and cyber-physical)
- ◆ Find/fix vulnerabilities from hardware, software, and human-computer interactions
- ◆ Work with stakeholders to improve resiliency and cyber-safety of individual systems
- ◆ Analyse the cybersecurity of a collection of bridge systems (System-of-Systems), connected in real world configurations
- ◆ Discover maritime-cyber threats that can be used to educate future mariners and Navies
- ◆ Determine future cyber threats to assets, economy, human lives, and environment.

Next generation research capabilities are needed.

Simulation vs Emulation Vs Live systems



	Simulation	Emulation	Live Systems
Positive	<ul style="list-style-type: none">• Quick to develop• Cheaper• Training tools	<ul style="list-style-type: none">• More realistic• Repeatable Experiments	<ul style="list-style-type: none">• Entirely realistic for training & research
Negative	<ul style="list-style-type: none">• Limited by conceptual model	<ul style="list-style-type: none">• Costly• Not entirely realistic	<ul style="list-style-type: none">• Real world consequences can be costly

Cyber-SHIP Lab at Plymouth

(Software, Hardware, Information and Protection)

Join with or growing community of Maritime stakeholders that includes Ship Builders, Operators, Equipment Manufacturers, Class Societies and Insurers to:

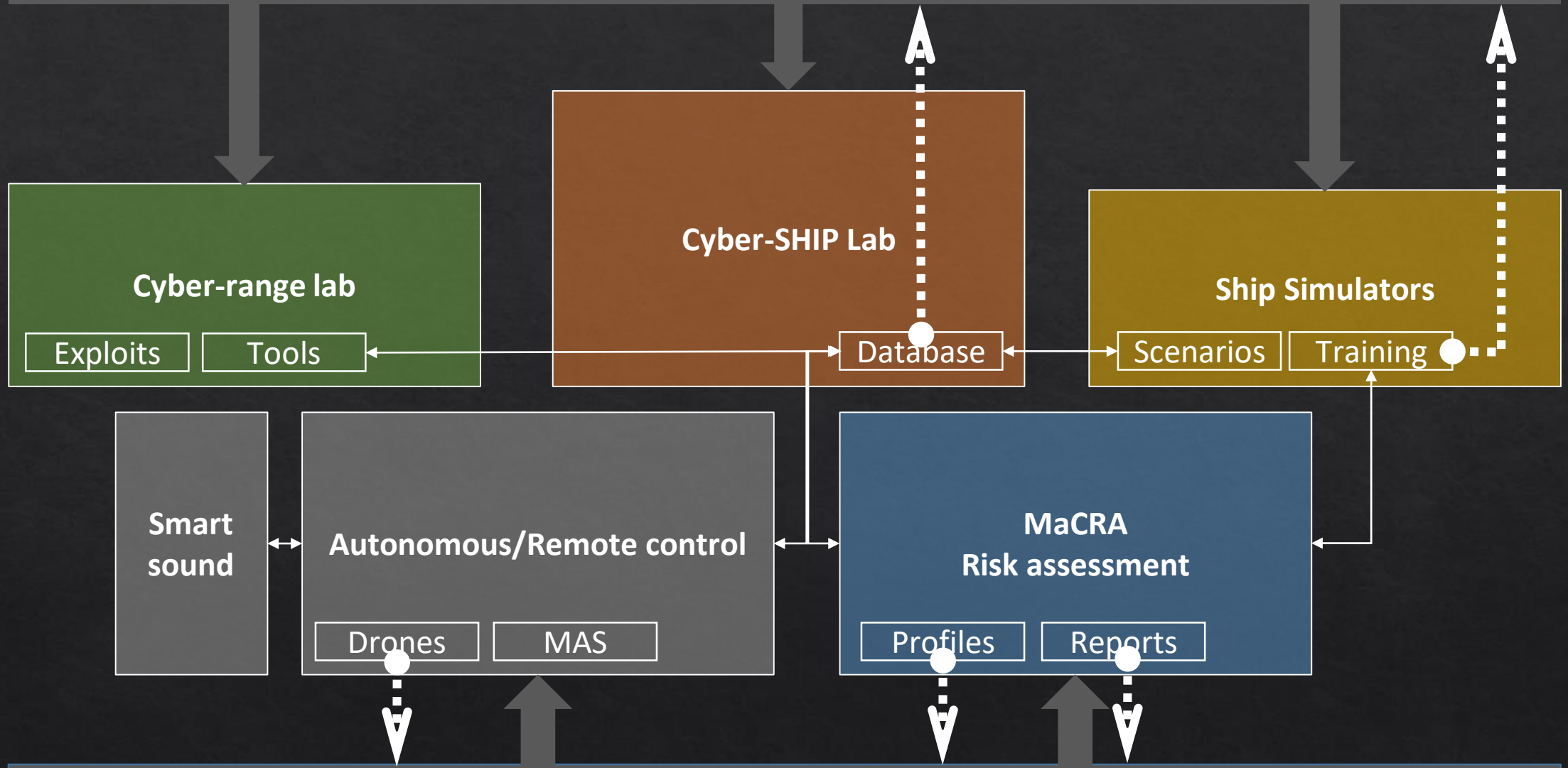
- Make use of our specialist facilities for equipment ruggedization
- Partner with differing aspects of the value chain for collaborative projects
- Engage with all aspects of the Maritime sector to shape the future research agenda and influence policy



**UNIVERSITY OF
PLYMOUTH**
Marine Institute



Companies, Government, Military, Academia



Companies, Government, Military, Academia



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

Related Projects

Proposal Title: Cyber-MAR

- ❖ State of the art analysis regarding simulation environments based on Cyber-ranges
- ❖ OT real/virtual coupling
- ❖ Cyber-range for Intrusion Detection and Prevention
- ❖ Piloting networked Cyber-ranges and interoperability
- ❖ Data analytics and intelligence extraction
- ❖ Situational awareness and knowledge platform



**UNIVERSITY OF
PLYMOUTH**
Faculty of Science and
Engineering



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 833389.



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 [Masyflower 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



Prof Kevin Jones

Kevin.Jones@plymouth.ac.uk

UoP Website  :

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



www.Cyber-MAR.eu



Cyber_MAR



Cyber-MAR