Securing our ships in a cyber-world

Prof Kevin Jones

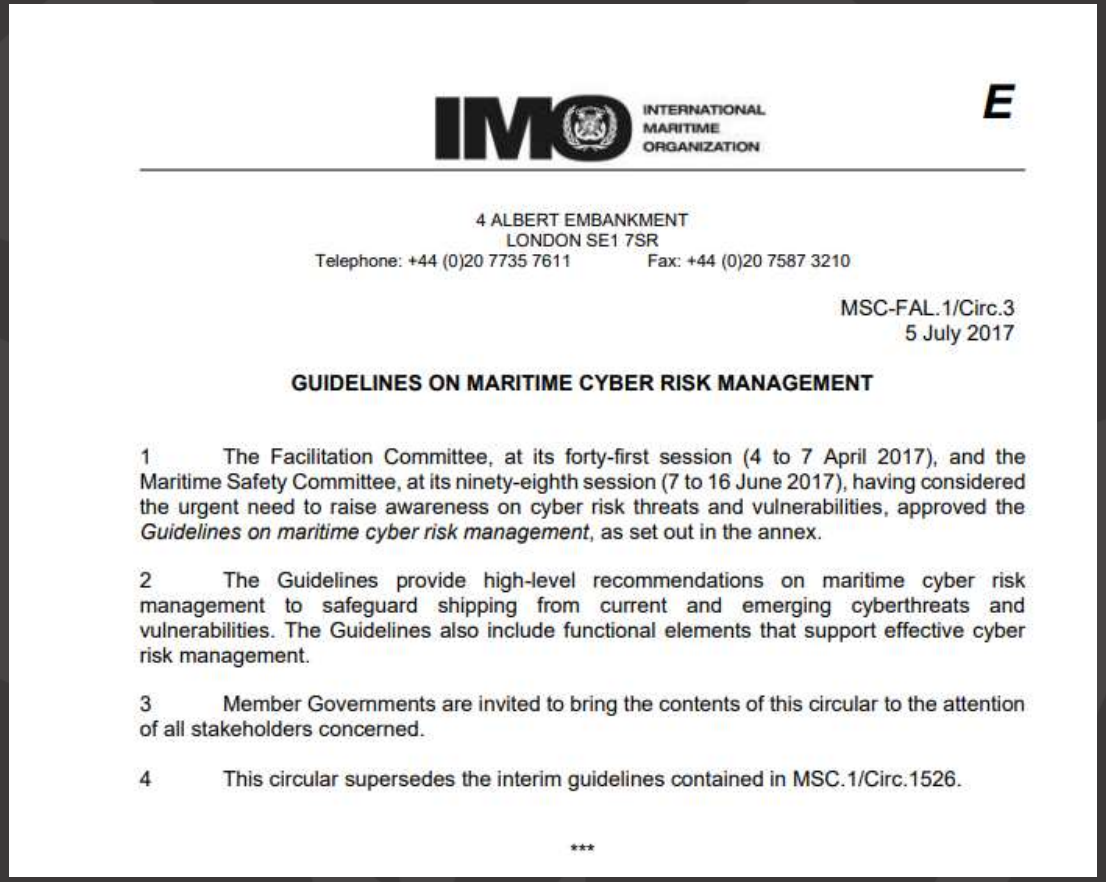
UNIVERSITY OF PLYMOUTH

Advantages of advanced technology

- More accurate and up-to-date information
- Heightened situational awareness
- Emergent information from analysis of large datasets (big data analysis)
- Better Land-to-Sea and vessel-to-vessel communication
- Remote access/control and increased autonomous systems
- Safety for people, goods, and environment

The sector is changing

- From the beginning of 2021, cyber can't be ignored.



IMO INTERNATIONAL MARITIME ORGANIZATION

E

4 ALBERT EMBANKMENT
LONDON SE1 7SR
Telephone: +44 (0)20 7735 7611 Fax: +44 (0)20 7587 3210

MSC-FAL.1/Circ.3
5 July 2017

GUIDELINES ON MARITIME CYBER RISK MANAGEMENT

1 The Facilitation Committee, at its forty-first session (4 to 7 April 2017), and the Maritime Safety Committee, at its ninety-eighth session (7 to 16 June 2017), having considered the urgent need to raise awareness on cyber risk threats and vulnerabilities, approved the *Guidelines on maritime cyber risk management*, as set out in the annex.

2 The Guidelines provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyberthreats and vulnerabilities. The Guidelines also include functional elements that support effective cyber risk management.

3 Member Governments are invited to bring the contents of this circular to the attention of all stakeholders concerned.

4 This circular supersedes the interim guidelines contained in MSC.1/Circ.1526.

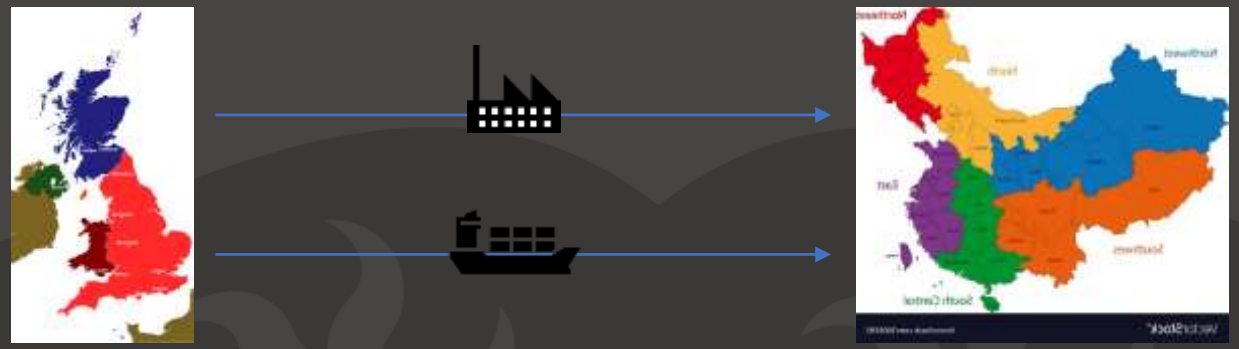
***

UNIVERSITY OF PLYMOUTH

Isn’t our problem already solved?

- IT
  - Well understood
  - Rapidly evolving, constantly updated
- OT
  - SCADA
  - Physical consequences

Ships are Different



UNIVERSITY OF PLYMOUTH

Maritime Cyber incidents from October 2020

- International Maritime Organization website hacked, when IMO is asking member nations to enforce IMO 2021
- French shipping giant CMA CGM says it has been hit with a ransomware cyber attack.
- Ships have reported an increasing number of cases of significant GPS interference and jamming in recent months.
- The US Justice Department has charged six Russian intelligence officers for NotPetya ransomware attack that shut down Maersk Group's IT systems and paralysed ports.

UNIVERSITY OF PLYMOUTH

IT

Servers 2017
Ransomware

Emails 2019
data breach

Port authority
servers 2018

2018 Internet outage
2020 **unconfirmed** website outage - 2020 IT equipment - 2020 servers - 2020 data breach – details **unknown**

Port authority
servers 2018

Converging IT/OT - Moving forward

- Cyber attacks are going unnoticed – sometimes for a long period
- IT/OT **convergence** significantly increases risks
- Cyber attacks are encroaching further into maritime sector

GPS signals 2017-2020

Oil pipeline 2020

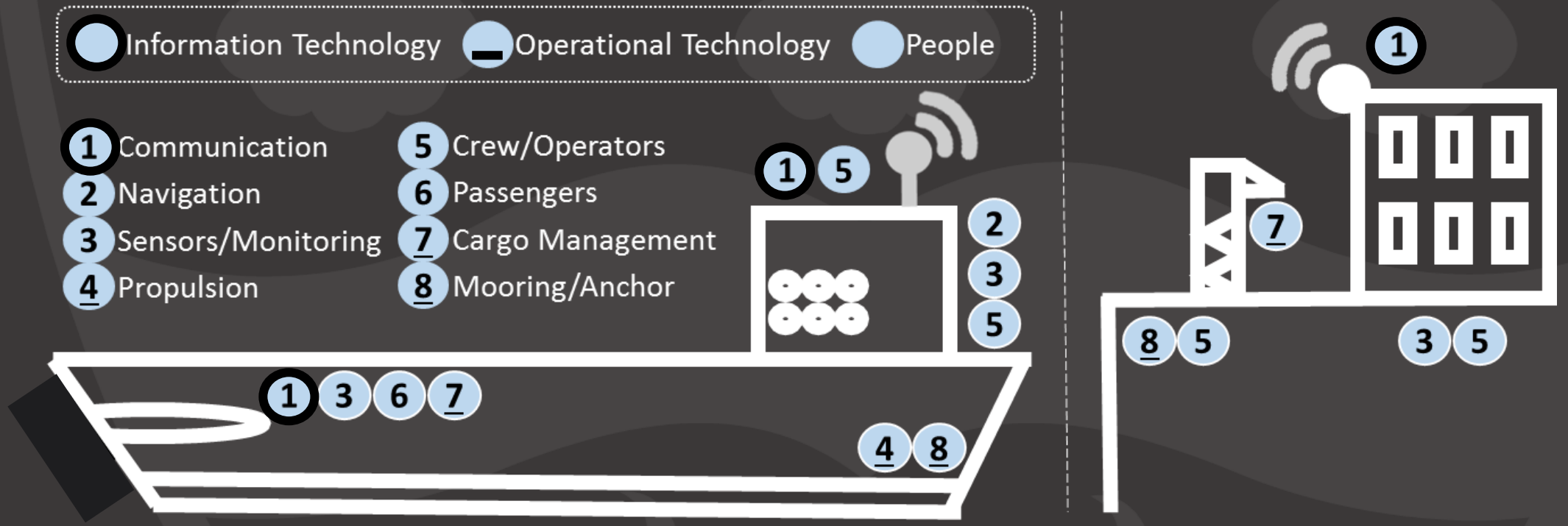
Power 2017
Nuclear 2009

Cargo movement
2013

UNIVERSITY OF PLYMOUTH

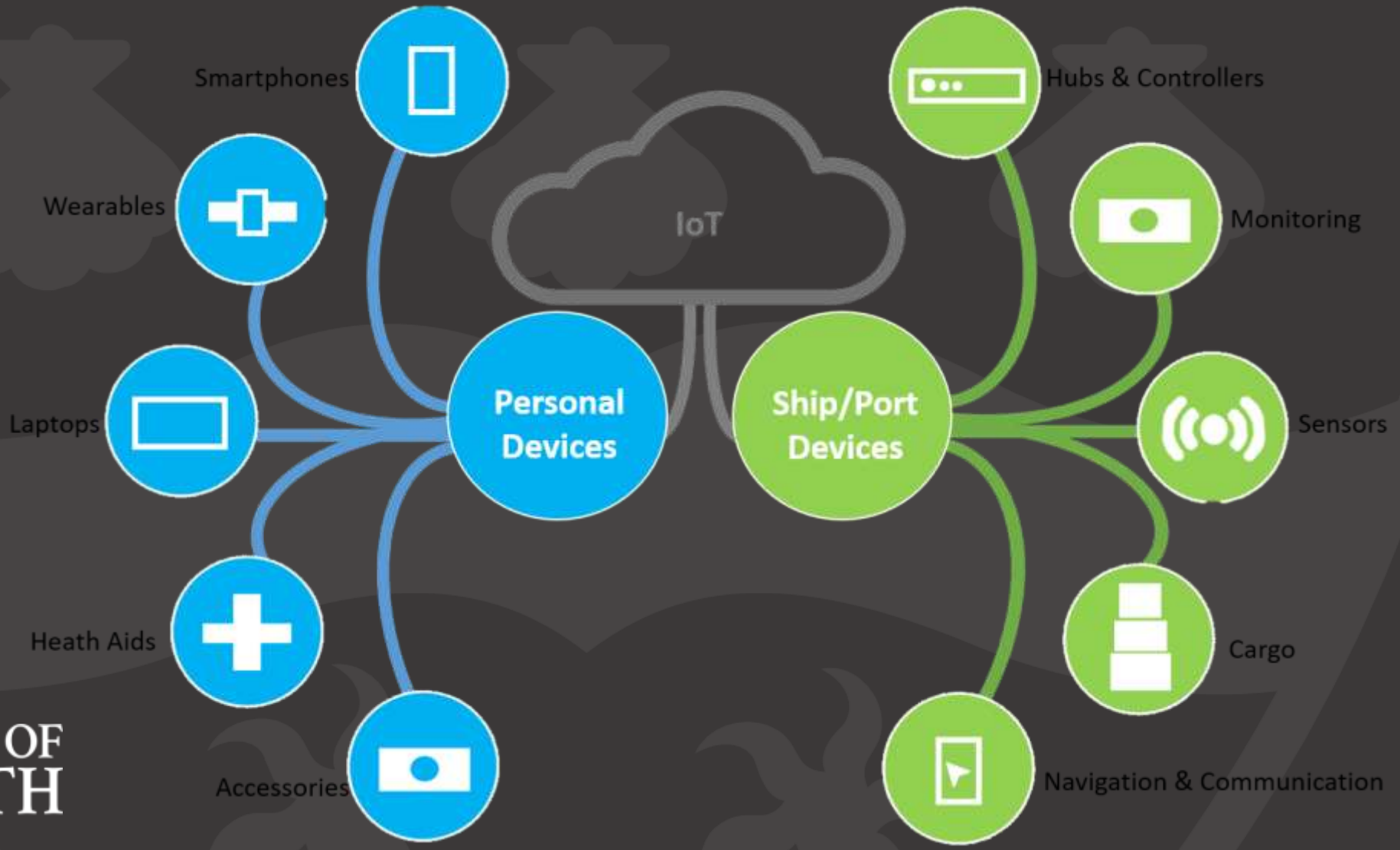
OT

Human/IT/OT: Security challenges



UNIVERSITY OF PLYMOUTH

Internet of Things (IoT)



UNIVERSITY OF PLYMOUTH

UK: SMART PORTS

In Jan 2019 the Department for Transport published its **long-term strategy** for the future of the UK's maritime sector – **Maritime 2050**. The strategy is intended to position the UK as a world leader on clean energy growth, maritime safety and security, and the application of new and emerging technologies.

Maritime 2050 makes a commitment to deliver on a key recommendation: to develop the **first smart port in the UK by 2030**.

UNIVERSITY OF PLYMOUTH

Solutions

Or at least research to get there!

UNIVERSITY OF PLYMOUTH

Research aims

UNIVERSITY OF PLYMOUTH
Faculty of Science and Engineering

Founded in 1862 as the School of Navigation, the University of Plymouth is now the UK's 15th largest university

We combine IT strengths with our Maritime heritage in the Maritime Cyber Threats Research Group to look at:

- **Awareness/Body of Knowledge**
  - Who are the attackers & targets?
  - What is the current security landscape?
- **Vulnerability, Risk Analysis and Intrusion Detection**
  - Individual systems, Ship/Fleet/Port infrastructure and supply chain
  - Future technology (Autonomy, IoT, augmented reality)
- **Maritime Cyber-Security Training, Certification**
- **Maritime Cyber-Security Policy, Insurance, and Law**

Security Lab / Cyber Range

Marine Navigation Suite

MaCRA: Model based risk assessment

- A way to characterize and quantify risks
- Model ship (target) and attacker

System Vulnerability

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

Ease of Exploit

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

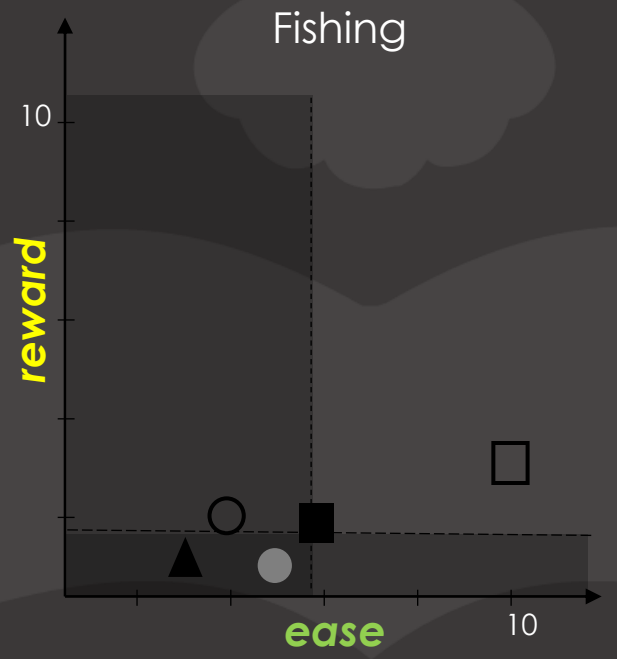
Attacker Reward

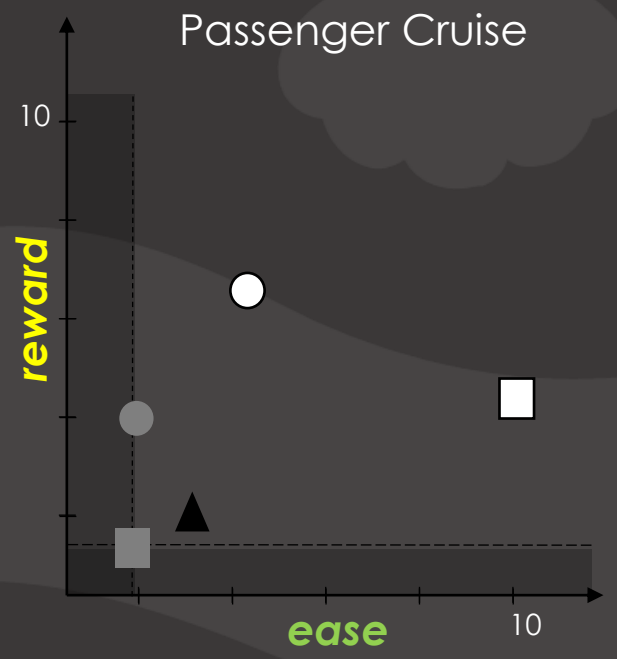
- Profit
- Collision/Damage
- Denial of Service
- Misdirection
- Obfuscation
- …

Example assessment: Criminal

vulnerabilities

Cargo :	Theft
Cargo :	Damage
ECDIS :	Damage
ECDIS :	Misdirect
AIS :	Damage
AIS :	Theft
VDR :	Obfuscate
GMDSS :	Coms DoS





UNIVERSITY OF PLYMOUTH

MaCRA
Maritime Cyber Risk Assessment

New Cyber-SHIP Lab at Plymouth

- The Cyber-SHIP Lab combines 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 collaboration with 18 partners including **equipment manufacturers, ship operators and builders, insurers and Class Societies**, in a project that will see investment of over £3m to create a National Resource for Research and Training.

UNIVERSITY OF PLYMOUTH
Faculty of Science and Engineering

Research England

BT

IRM
INFORMATION RISK MANAGEMENT

EATON

HENSOLDT
Detect and Protect.

NETTITUDE
A member of the Lloyd's Register group

Cyber-SHIP Lab

UNIVERSITY OF PLYMOUTH

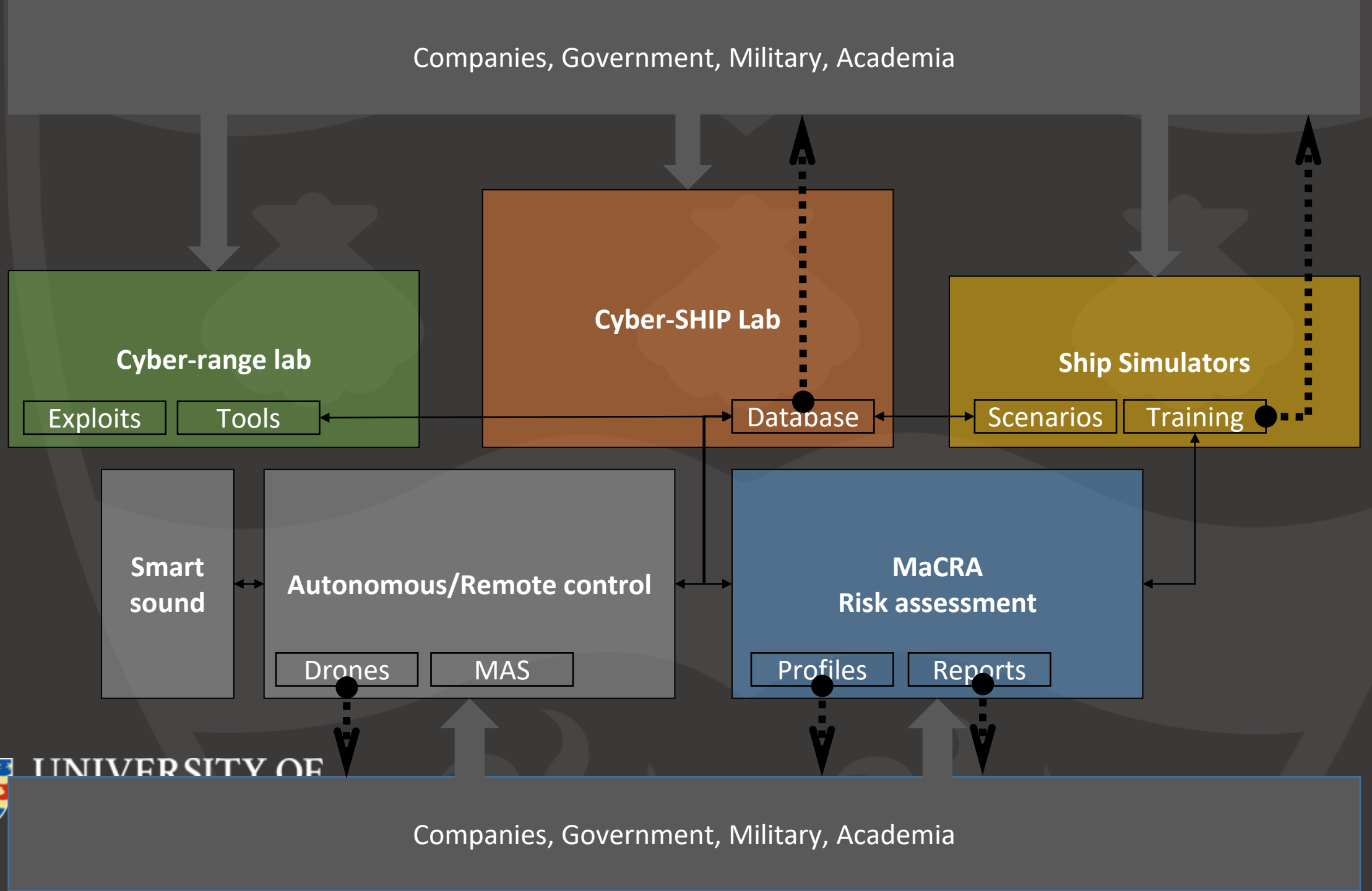
Projects – EC H2020 Cyber-MAR

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

- Develop an innovate simulation environment for training and risk assessment.
- Increase cyber-awareness and validate their business continuity management in a 6 Million Euro Project
- Why ports? Well, 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).

UNIVERSITY OF PLYMOUTH

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


Companies, Government, Military, Academia
Cyber-range lab
Exploits
Tools
Cyber-SHIP Lab
Database
Ship Simulators
Scenarios
Training
Smart sound
Autonomous/Remote control
Drones
MAS
MaCRA
Risk assessment
Profiles
Reports
Companies, Government, Military, Academia

Thank You

Prof Kevin Jones
kevin.jones@plymouth.ac.uk

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

UNIVERSITY OF PLYMOUTH

Newsletter sign-up

Maritime Cyber Threats research group

Investigating marine cyber threats and researching solutions

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.