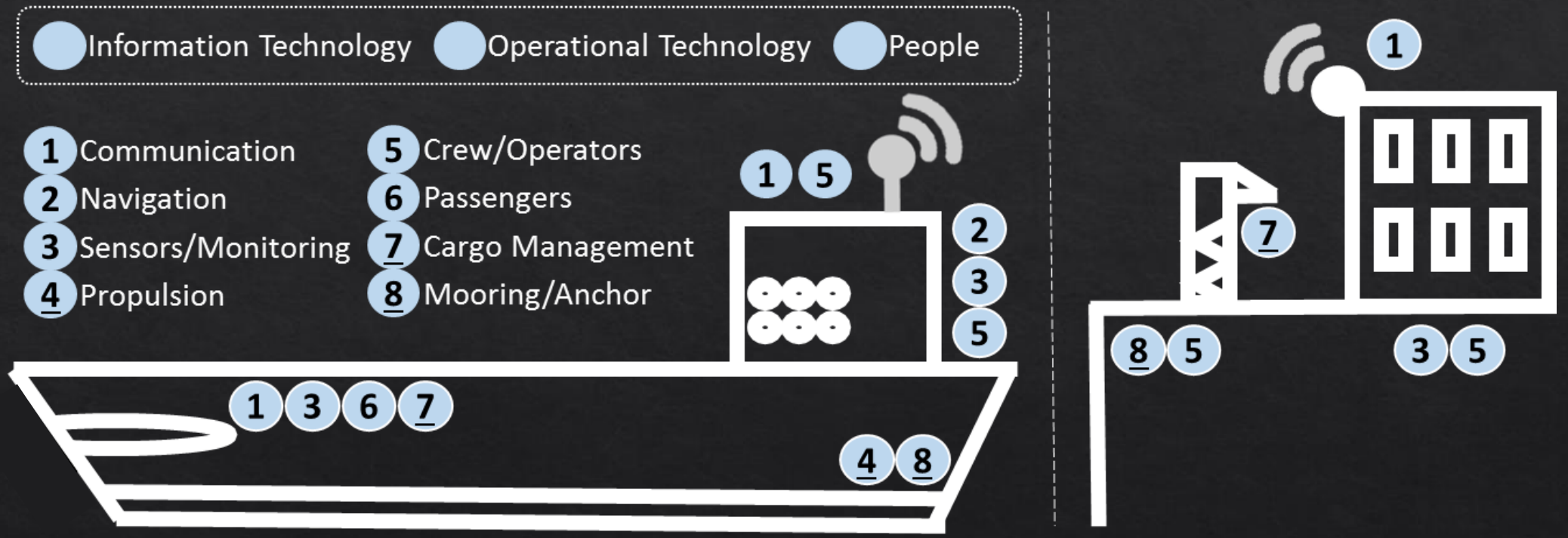
A Cyber-Security Review of Emerging Technology in the Maritime Industry

Nase More 2019, 16-17 October

Prof Kevin Jones

Human/IT/OT: Security Challengers

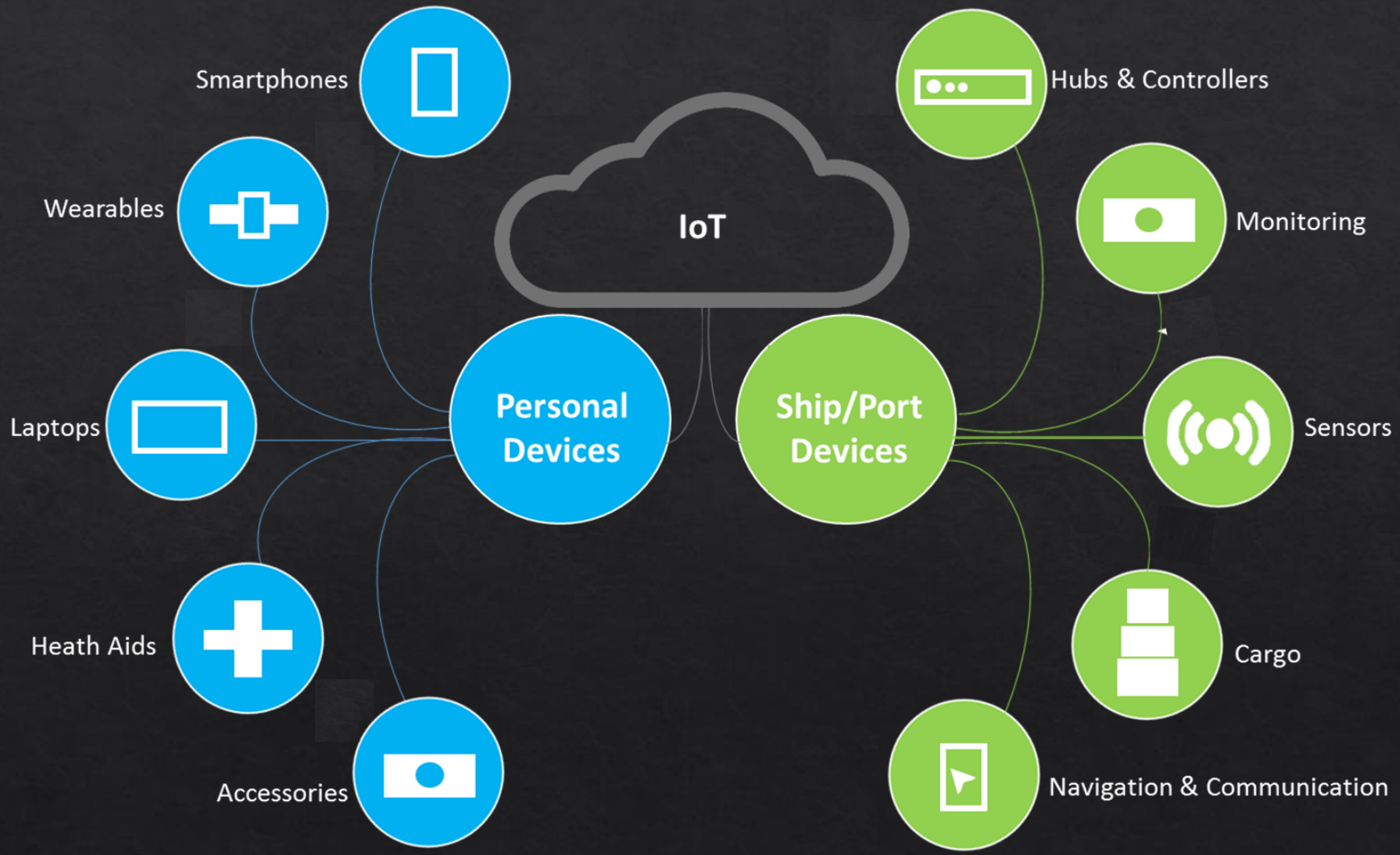


Digital Twin & Virtual Reality & Autonomy

- A suite of simulations models that can be placed in a common platform
- Highly customizable platform for a multitude of analysis, but not cyber-security
- Virtual reality could be misused to feed false information to human asset
- Increase the number of devices in ship/ports to compensate for less/no humans

	Tier 1	Tier 2	Tier 3	Tier 4	Tier 5
SAE-based Ship Autonomy	No/minimal autonomy. Small crew required for most, if not all, ship operations.	Partial automation with local crew for simple tasks, e.g. advanced auto pilot.	Conditional autonomy, potential interventions by crew	High autonomy, ship is mostly self-running. Local or onshore crew is rarely required.	Complete autonomous operations in all potential settings.
Remote operations	Not required	Not required	Not required, but likely	Required for operations	Not required, but likely
Sensors / IoT	Needed to aid crew decision	Needed to aid crew decision	Needed to aid crew and autonomy decision	Needed to aid remote crew and autonomy decision	Needed for complete autonomous decisions

IoT: More Devices and Connectivity



Cyber Ranges (Cyber-MAR)

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.

Cyber MAR


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

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.

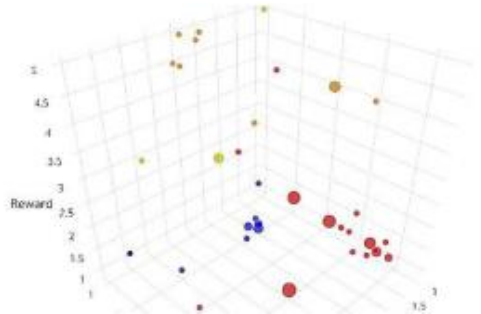
Help us by taking this survey on maritime cyber [open until March 2019]

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

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 EU Project

Cyber-MAR

info@lists.Cyber-MAR.eu