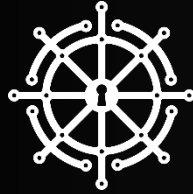




UNIVERSITY OF
PLYMOUTH



Cyber-SHIP Lab
SECURING MARITIME



Improving Maritime Digital Skills

Turning Research into Operational Practices

Cyber Security Training and Awareness

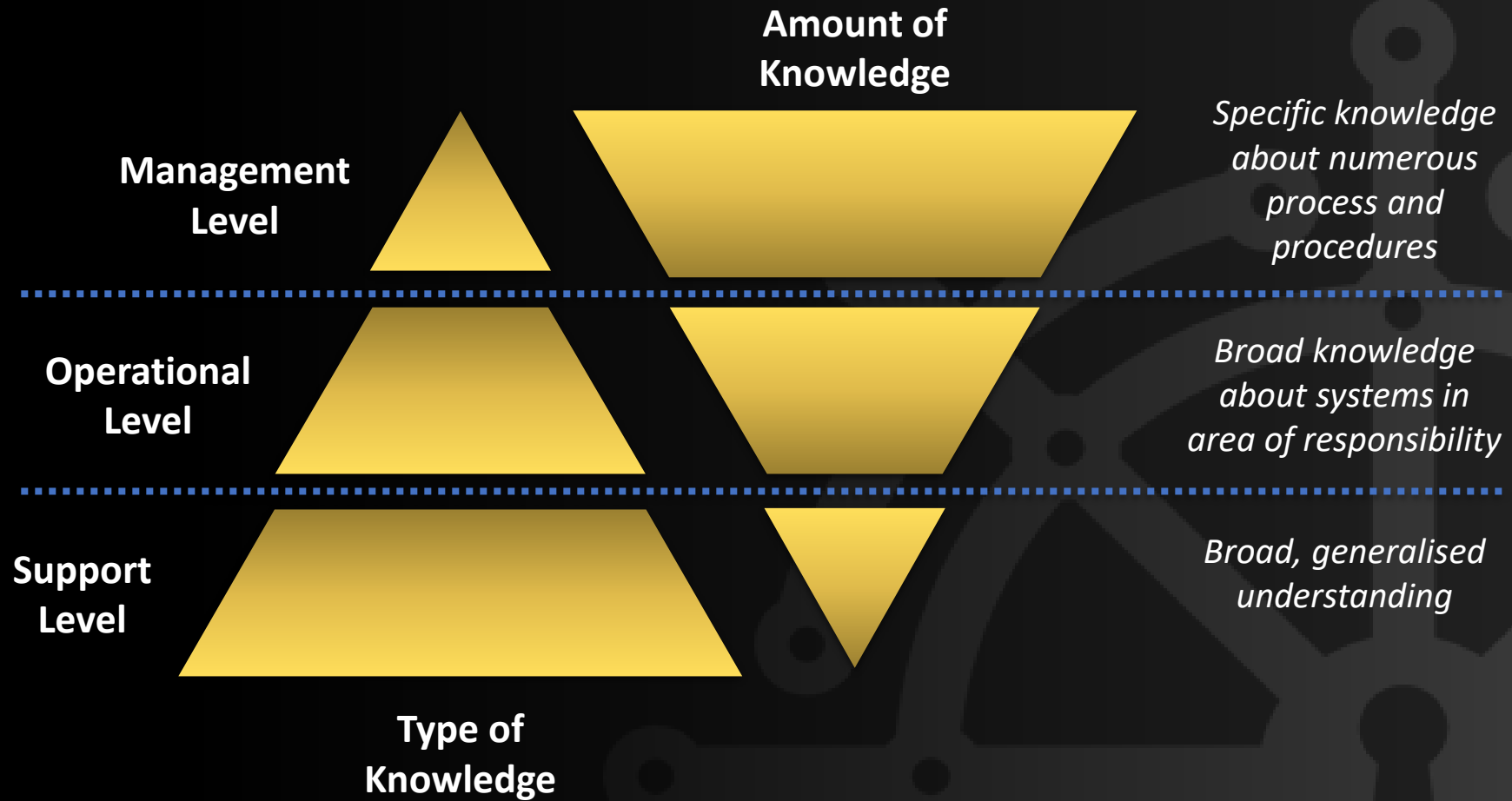
UK Government listed training and awareness as one of the core components of *Protecting against Cyber Attack*

UK Government Cyber Security Strategy 2022-2030

“...shall identify when basic cyber hygiene procedures are not in place onboard.” including: Passwords on display, reliance on USBs

USCG CVC-WI-027(2) - 2020

Appropriate Training



Consider the Scenario...



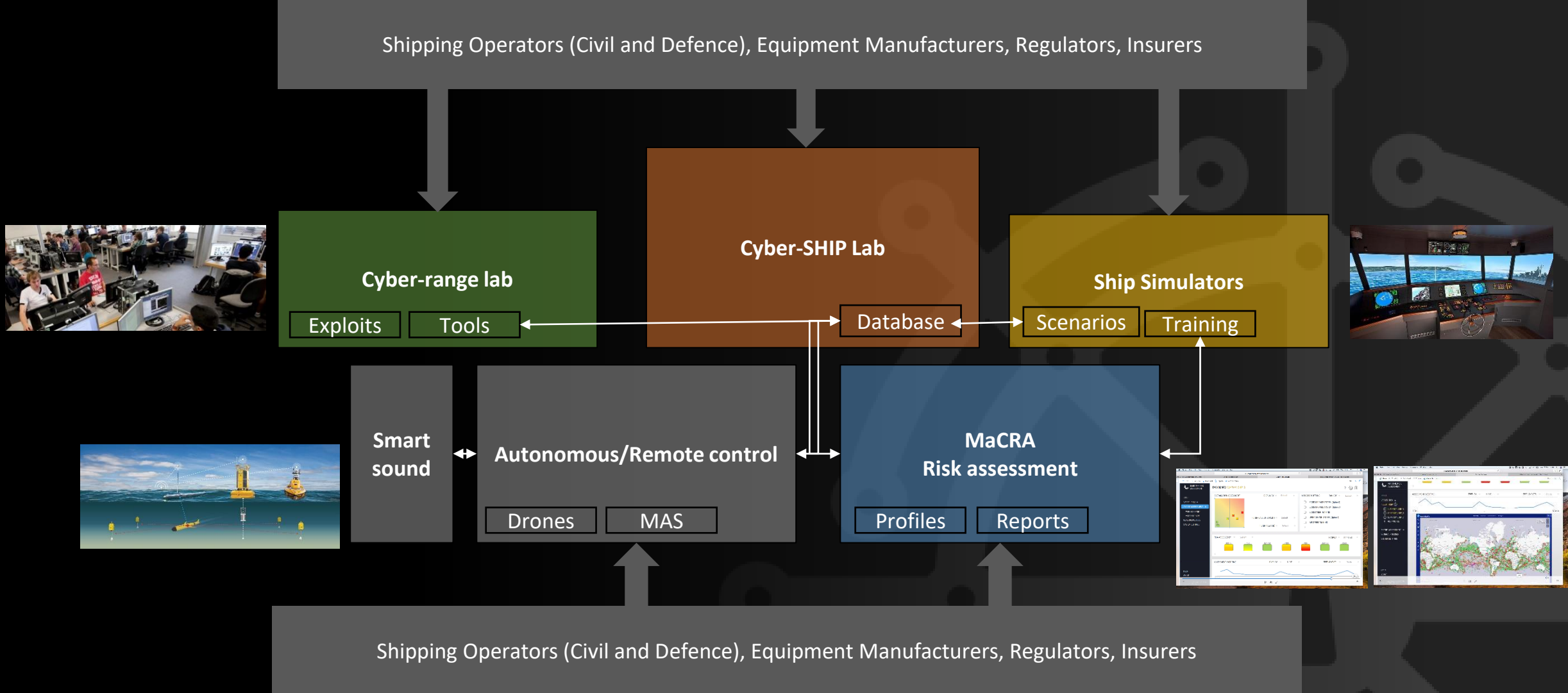
Need for a Holistic Approach

- Penetration Tester
- Security governance, risk, compliance and legal
- Security architect
- Security operations
- Security or software engineer
- Threat analyst
- Network security
- Incident management, response and recovery

- Harbourmaster
- Pilots
- Customs staff
- Search and Rescue Crews
- VTS operators
- Port operatives
- Passenger operatives
- Engineers
- Administrative staff

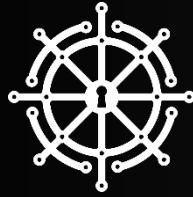
- Ships Master
- Chief Engineer
- Crew
- Vessel systems
- Ship Owner
- Ship Operator
- System designer
- System integrator
- System maintainer

The Plymouth 'Teaching Ecosystem'





UNIVERSITY OF
PLYMOUTH



Cyber-SHIP Lab
SECURING MARITIME



Rory Hopcraft
Research Fellow

rory.hopcraft@plymouth.ac.uk

Thank you



This paper is partly funded by the research efforts under 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.

