Future of Maritime Autonomy:

Cybersecurity, Trust and Mariner’s Situation Awareness

Authors

Juan Dorje Palbar Misas

Rory Hopcraft

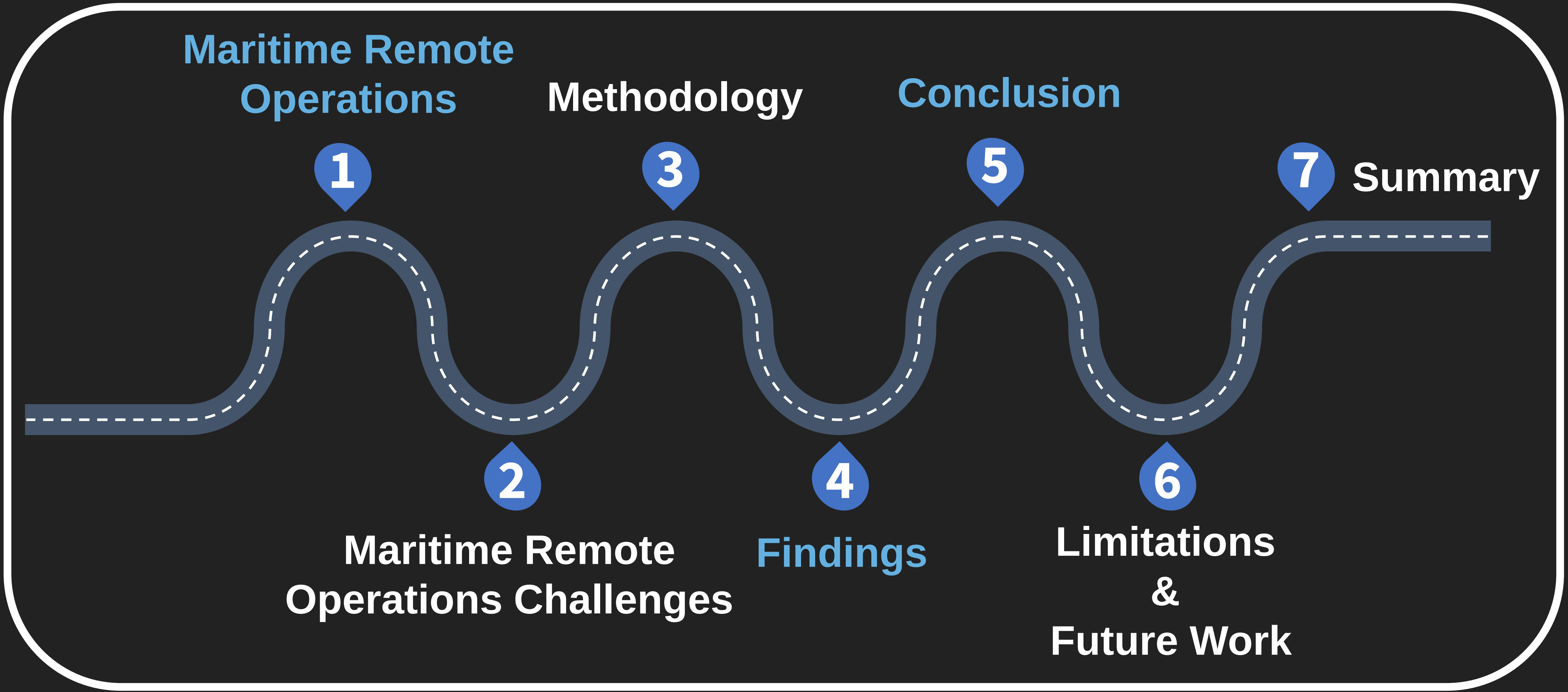
Dr Kimberly Tam

Cyber-SHIP Lab
SECURING MARITIME

UNIVERSITY OF PLYMOUTH

Cyber MAR

Outline of the Presentation



1 Maritime Remote Operations

2 Maritime Remote Operations Challenges

3 Methodology

4 Findings

5 Conclusion

6 Limitations & Future Work

7 Summary

Maritime Remote Operations

Source: (Kon, 2022)

- Remote operations reliant on **digital data**.
- The issue and the importance of the **human element** specially for remote operations (IMO MSC.1/Circ.1638).
- **New operational risks** are introduced.
- Misalignment between organisations innovation strategies to their **machine operator** work processes to achieve fully **autonomous ships**.

Source: (Mtiinstruments, 2022)

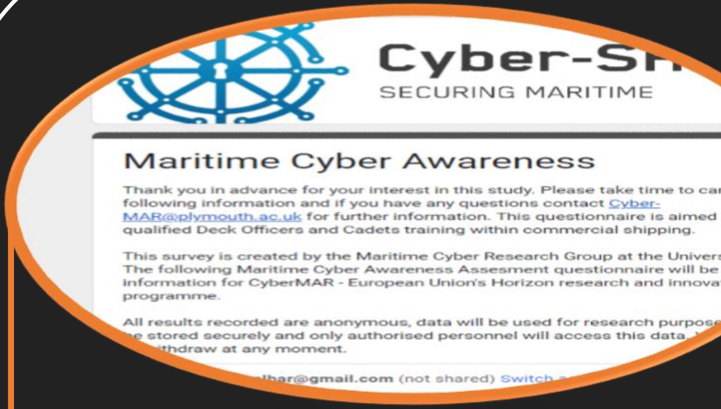
***Automation Conundrum** or “**Human-in-the loop**”*

Maritime Remote Operations Challenges

Situational Awareness	Reliant on information gathered from digital data
Cyber Security	Reliant on security of information gathered from digital data
Trust	Confidence in digital data for decision-making
Roles and Responsibilities	Implications when having the command of the ship remotely
Training	Competences for remote operated vessel

Methodology

Data Collection



Cyber-SH
SECURING MARITIME

Maritime Cyber Awareness

Thank you in advance for your interest in this study. Please take time to car ully read following information and if you have any questions contact Cyber-MAR@plymouth.ac.uk for further information. This questionnaire is aimed e ecially qualified Deck Officers and Cadets training within commercial shipping.

This survey is created by the Maritime Cyber Research Group at the University o Ply The following Maritime Cyber Awareness Assesment questionnaire will be collec information for CyberMAR - European Union's Horizon research and innovation programme.

All results recorded are anonymous, data will be used for research purpose e stored securely and only authorised personnel will access this data. ithdraw at any moment.

lhar@gmail.com (not shared) Switch a

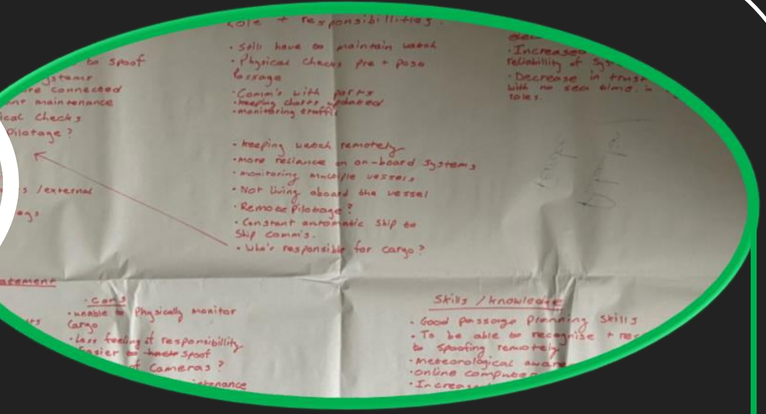
Maritime Cyber Awareness Questionnaire

- Divided into two parts:
  - **Quantitative**: maritime cyber awareness questions
  - **Qualitative**: opinions or details
- After this **maritime cyber lecture** (3 hours duration).

Full Bridge Cyber-attack Simulation Exercises

Two **20-minute simulation exercises**:

- **GPS drift** (300m every 2 min) in a Traffic Separation Scheme (TSS).
- **Loss** of **rudder** and **engine** control in inbound passage to port.



Future of Remote Operation Tabletop Exercises

- **Five questions** referred to IMO degrees of autonomy 2-4.
- **50 minutes tabletop** discussion.
- Groups of 5-6 people.

Participants:
60 Navigational students

Findings

01.SA Challenges for Remote Operations

02. Cyber Security Affecting SA

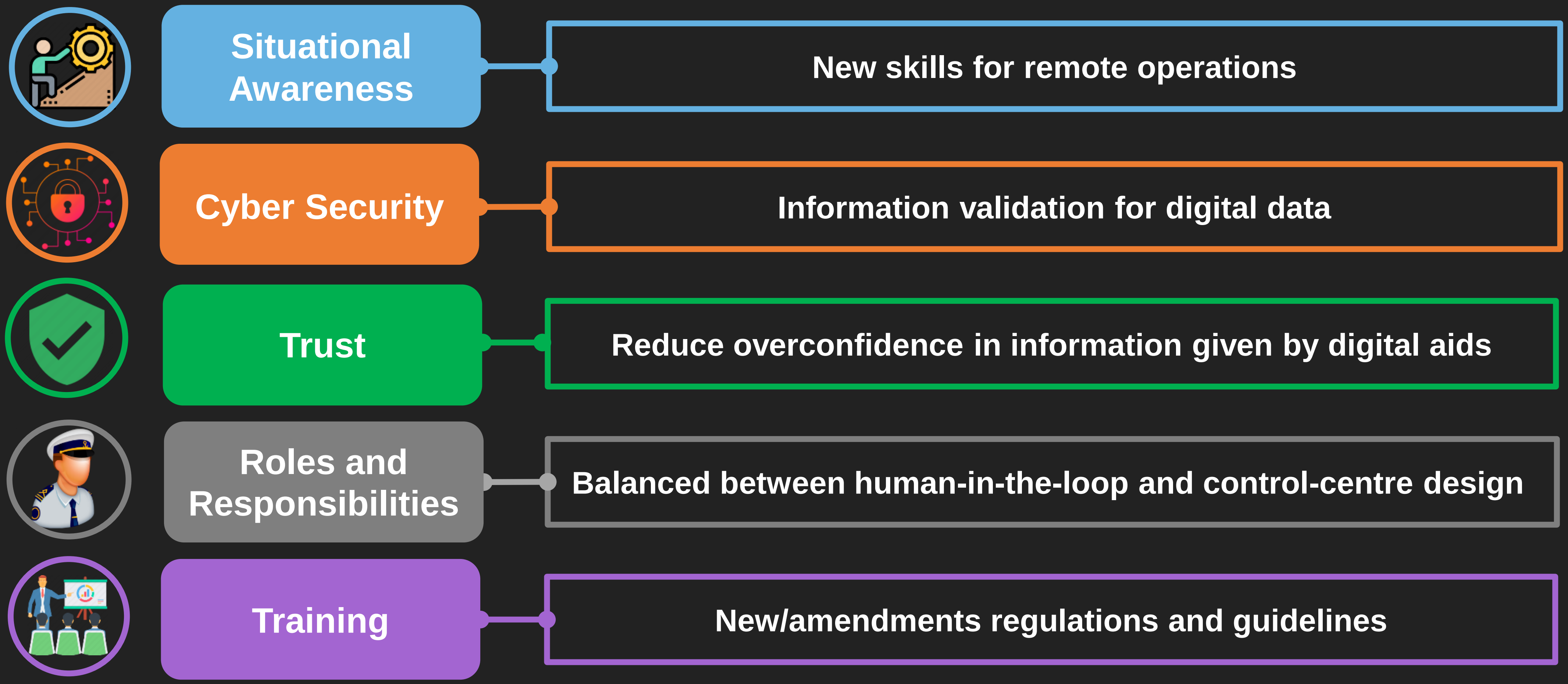
03. Trust in Autonomous Systems

04. Roles and Responsibilities in Remote Operations

05. Remote Operation Training

- 75% agreed that training needed to stop a cyber-attack.
- New skills needed for remote operations.
- Gaps in perception can be mitigated with awareness training and cultural changes.
- New, or amendments to, regulations (such as ISM Code and STCW).

Conclusion



Situational Awareness — New skills for remote operations

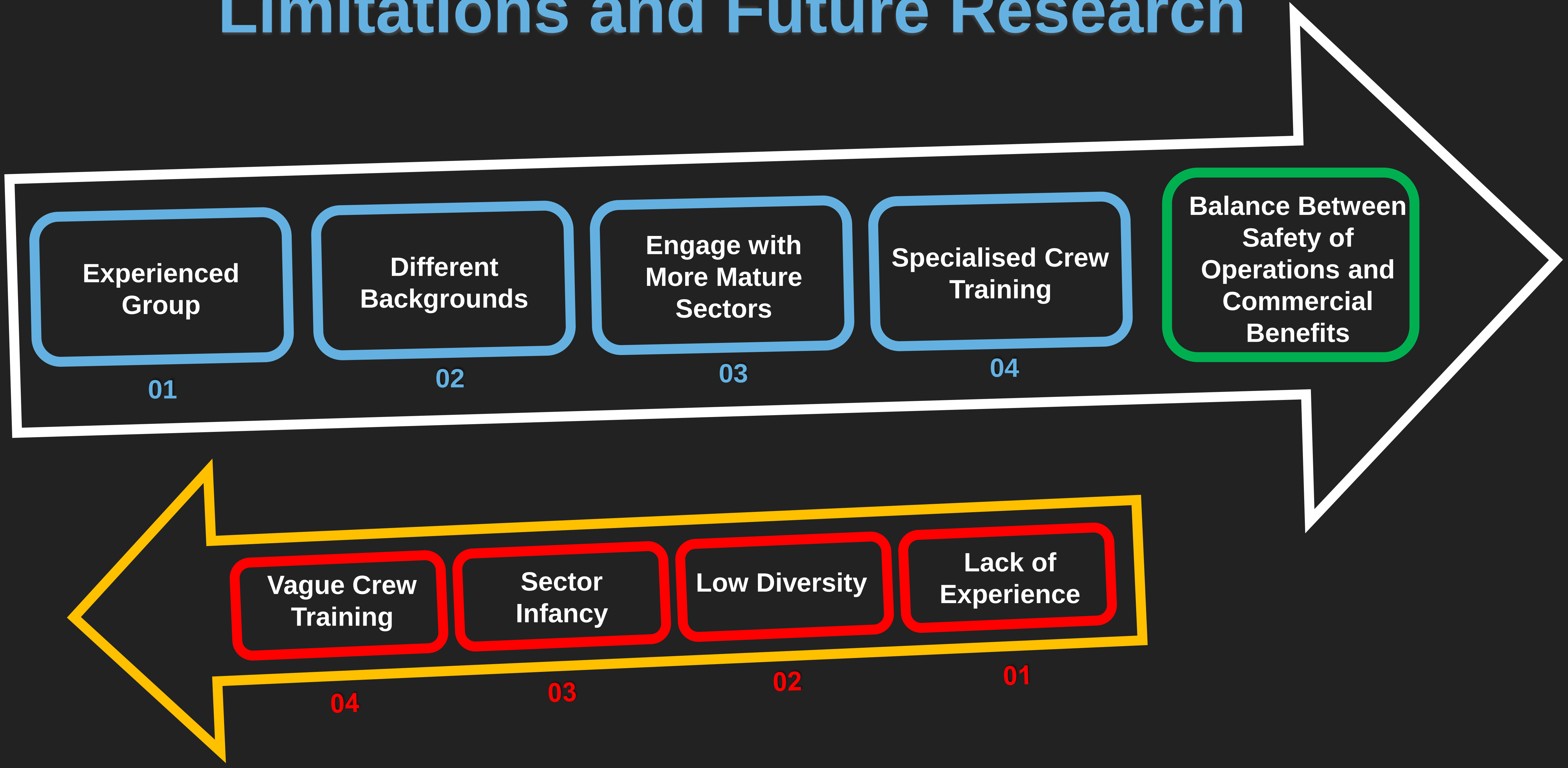
Cyber Security — Information validation for digital data

Trust — Reduce overconfidence in information given by digital aids

Roles and Responsibilities — Balanced between human-in-the-loop and control-centre design

Training — New/amendments regulations and guidelines

Limitations and Future Research



Experienced Group
01

Different Backgrounds
02

Engage with More Mature Sectors
03

Specialised Crew Training
04

Balance Between Safety of Operations and Commercial Benefits

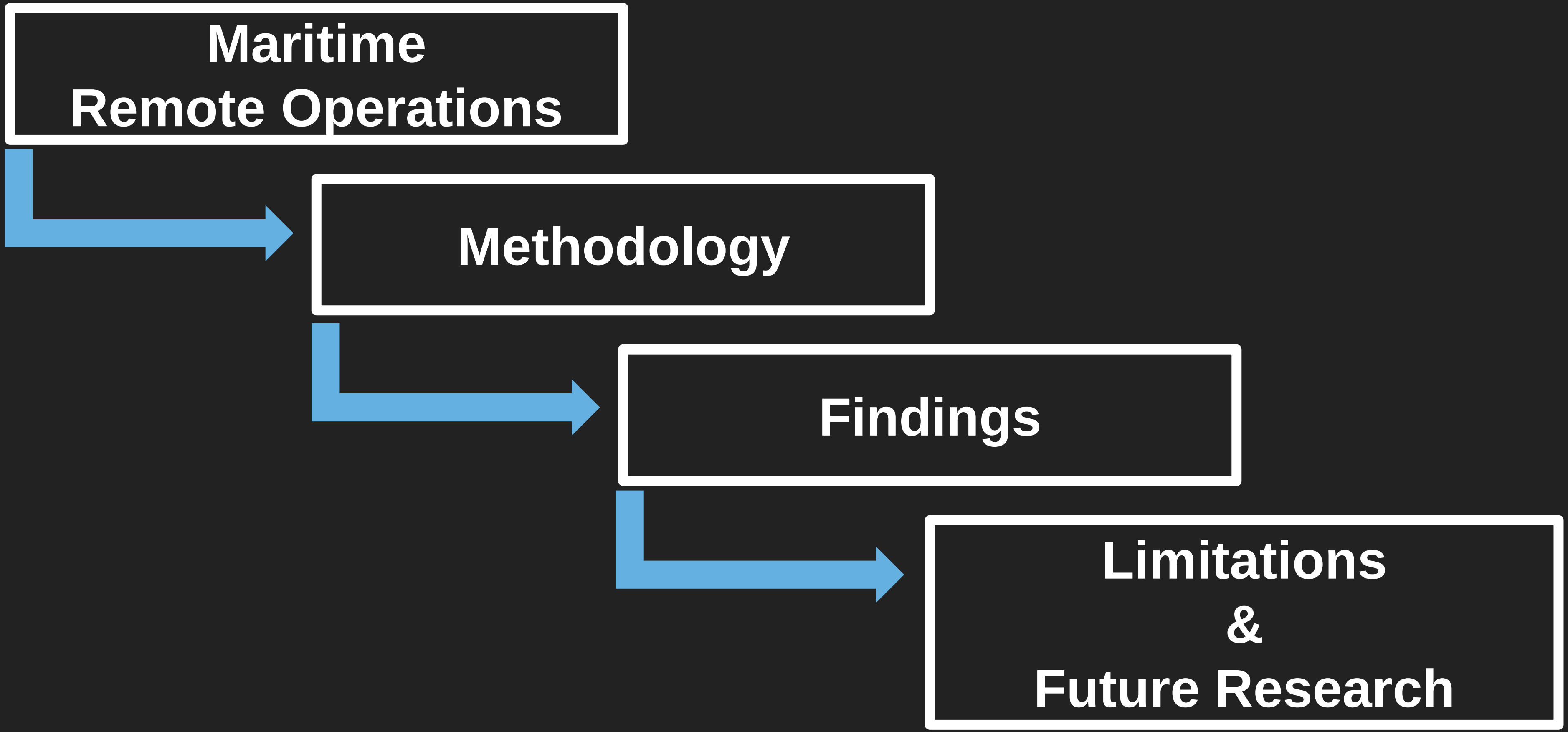
Lack of Experience
01

Low Diversity
02

Sector Infancy
03

Vague Crew Training
04

Summary



Maritime
Remote Operations

Methodology

Findings

Limitations
&
Future Research

Cyber MAR

Cyber-SHIP Lab
SECURING MARITIME

REARDON SMITH
NAUTICAL TRUST

Thank You! Any Questions?

Contact email: juan.palbarmisas@plymouth.ac.uk

Acknowledgements:

- Thank you to the **Reardon Smith Nautical Trust** for funding my PhD to do this research
- **Cyber-MAR project** has received funding from the European Union’s Horizon 2020 research and innovation program 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.
- The authors would also like to thank **Prof Kevin Jones**, **Mr. Tom Crichton** and all the **students who participated**.

UNIVERSITY OF
PLYMOUTH