Enhanced Transparency: Improving Maritime Cyber Governance

MARESEC 2021 – 14th June 2021
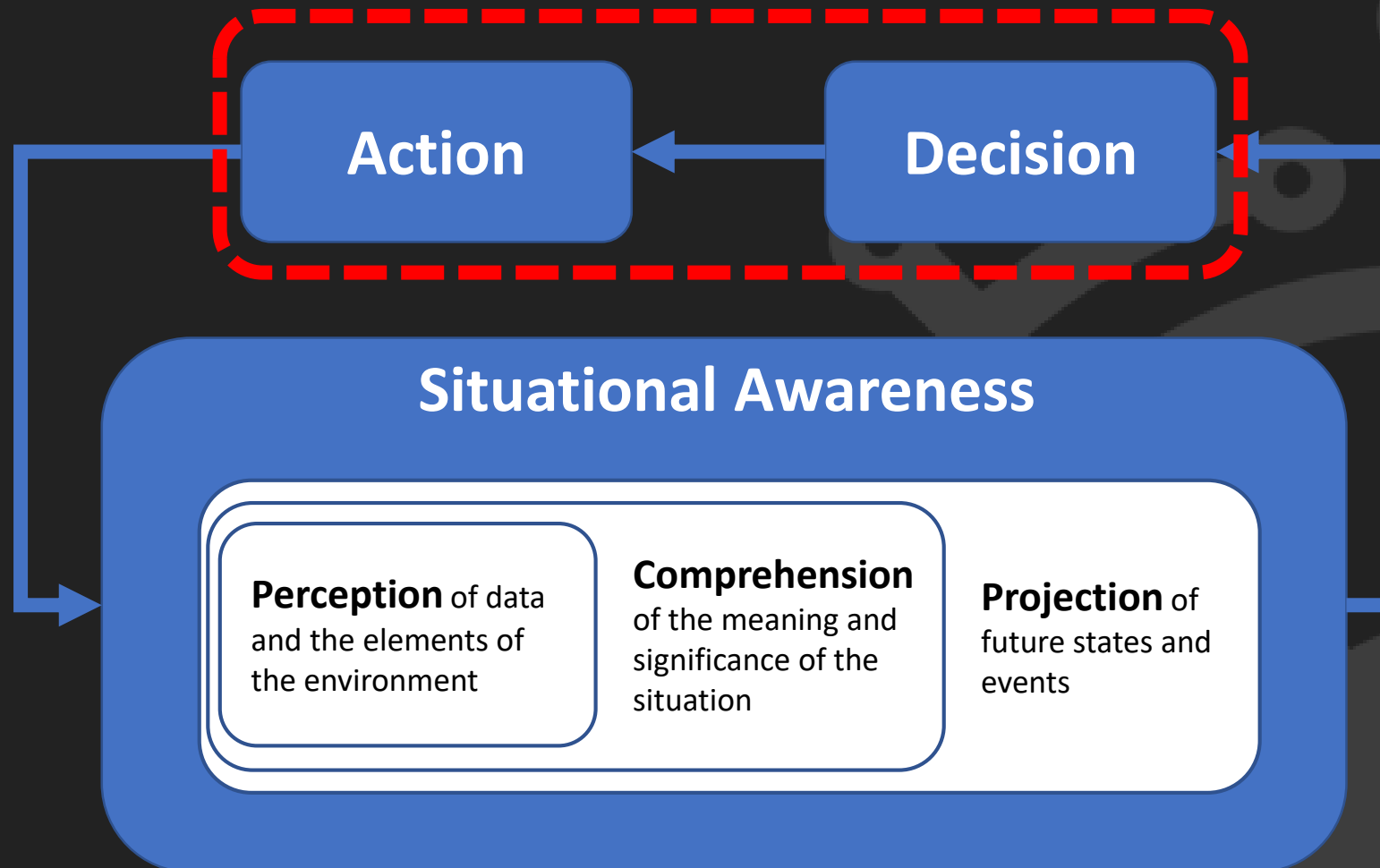
Rory Hopcraft

Industrial Researcher

Situational Awareness

"Situational Awareness is the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future"
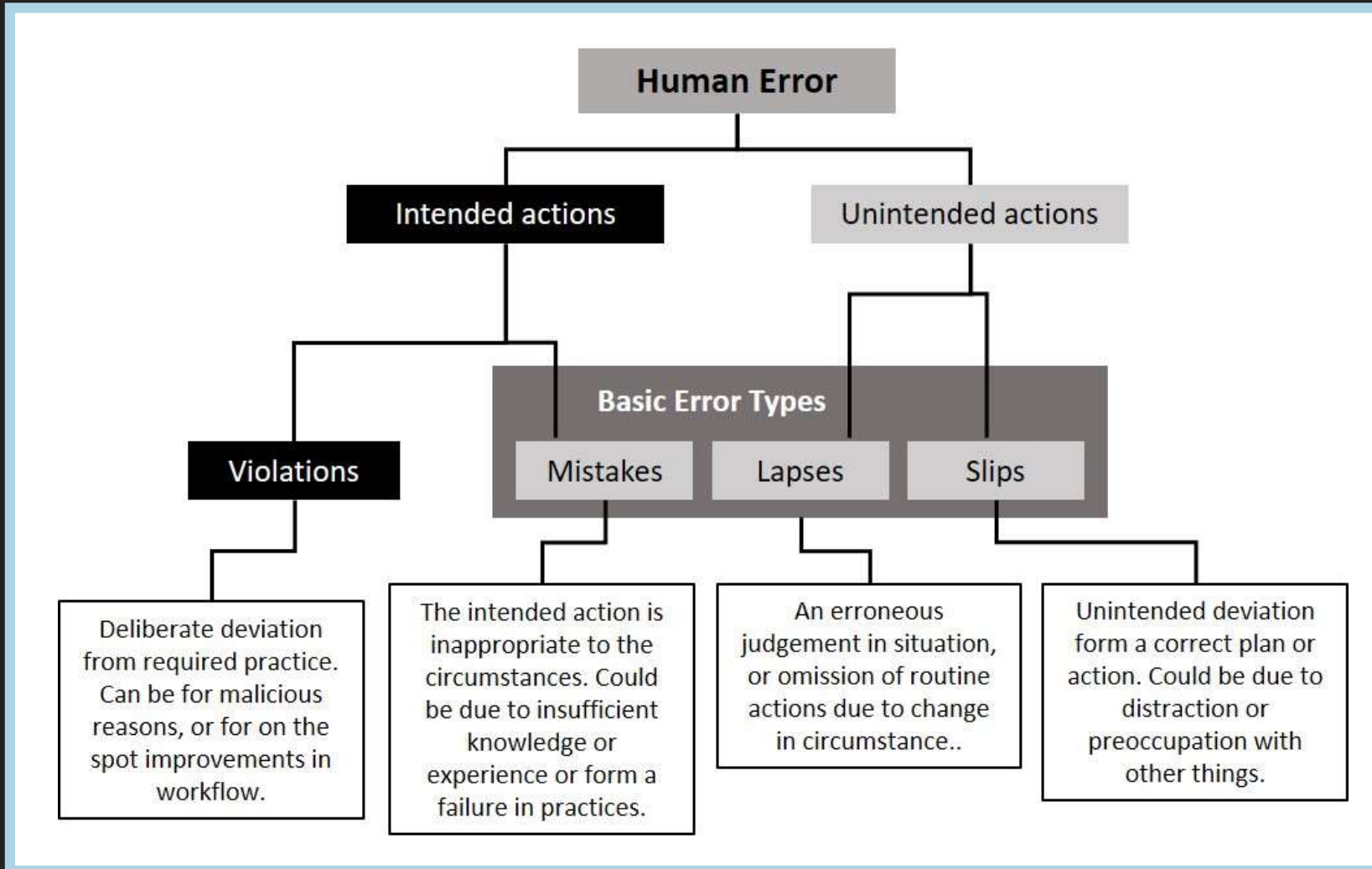
(Endsley, 1995)

- What does this mean in terms of:
  - Maritime Operations?
  - Cyber security?

Situational Awareness Loop

Adapted from: (Stan Institute, 2015)

Human Error in Decisions

Human Error

Intended actions · Unintended actions

Basic Error Types

Violations · Mistakes · Lapses · Slips

Violations: Deliberate deviation from required practice. Can be for malicious reasons, or for on the spot improvements in workflow.

Mistakes: The intended action is inappropriate to the circumstances. Could be due to insufficient knowledge or experience or form a failure in practices.

Lapses: An erroneous judgement in situation, or omission of routine actions due to change in circumstance..

Slips: Unintended deviation form a correct plan or action. Could be due to distraction or preoccupation with other things.

Resolution MSC.428(98)

AFFIRMS that an approved safety management system should take into account cyber risk management in accordance with the objectives and functional requirements of the ISM Code;

NOTING the objectives of the ISM Code which include... the provision of safe practices in ship operations... and the continuous improvement of safety management skills of personnel ashore and aboard ships.

One Size Does <u>NOT</u> Fit all...

- **Ships** have different functionalities
- **Ships** are equipped with different systems
- **Ships** travel through different locations

- **Companies** have different operational practices
- **Companies** are based in different locations
- **Companies** use different systems

- **Attackers** have different interests
- **Attackers** have different resources levels

Digital Competencies & Responsibilities

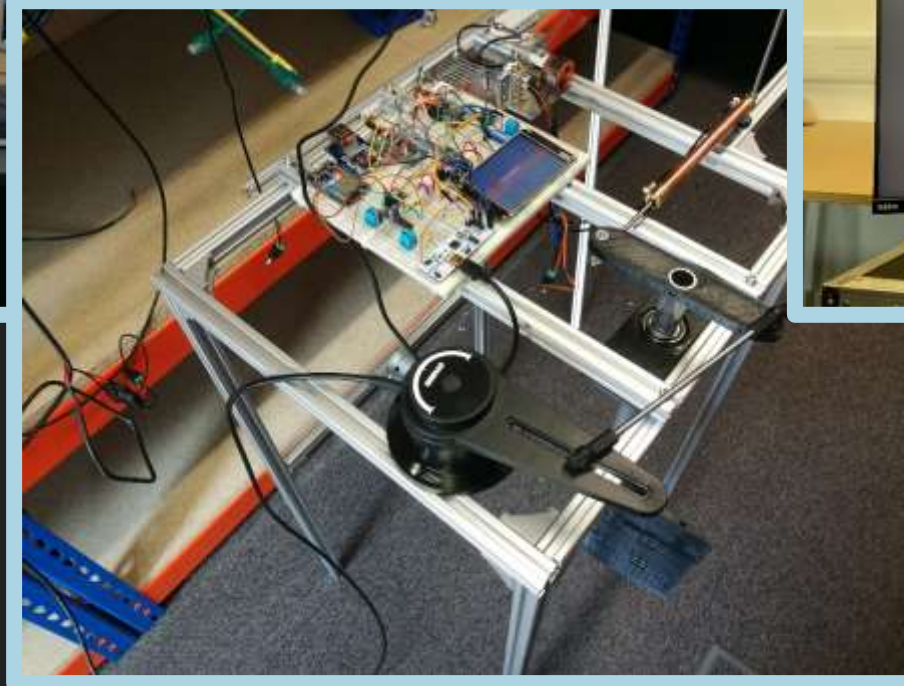*Adapted from:* (Hopcraft, Forthcoming)
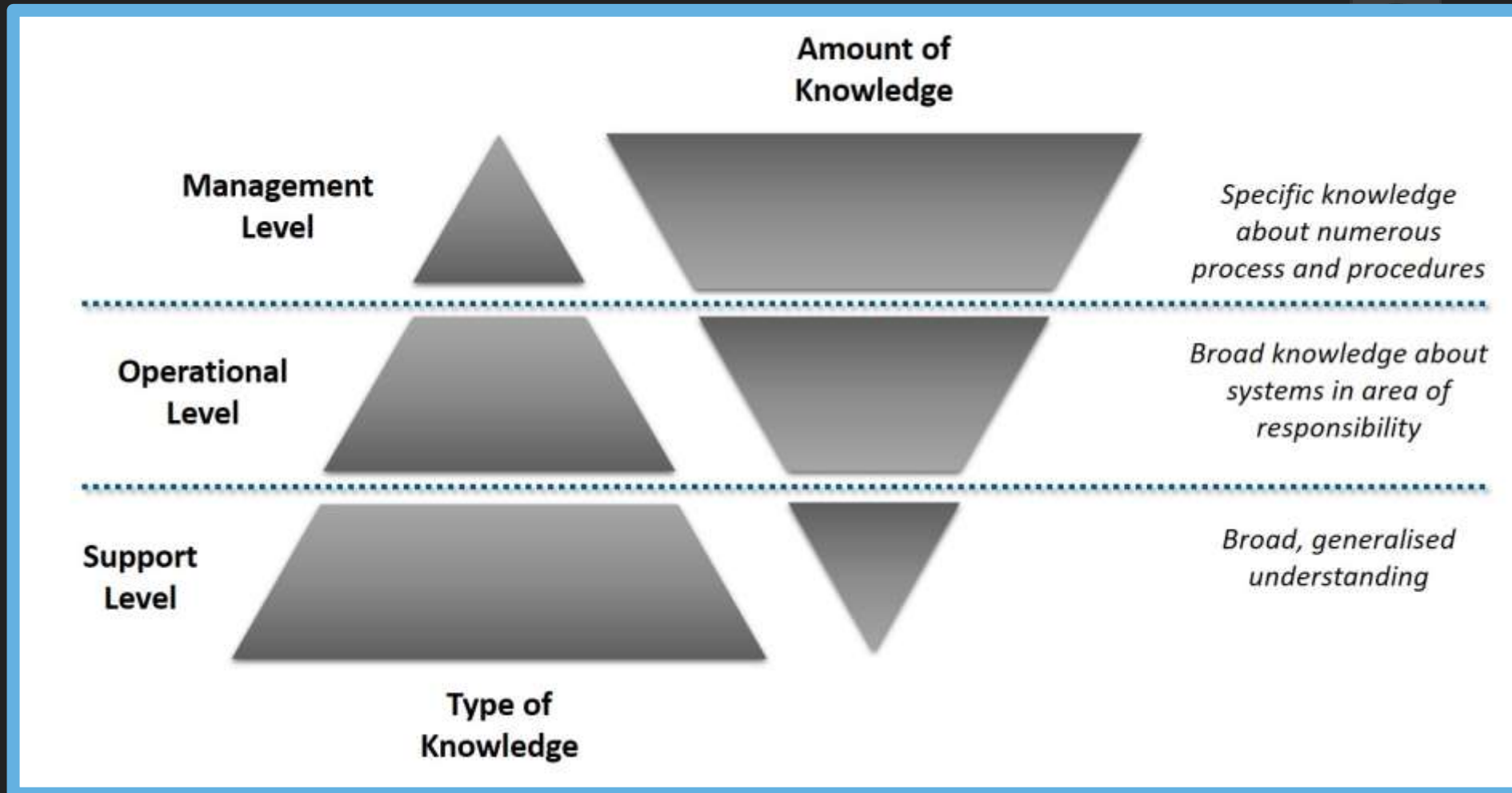
Cyber-MAR – EU Horizon 2020

The Cyber-MAR aims

to develop an innovative cybersecurity **simulation environment** for accommodating the peculiarities of the **maritime sector** while, being easily applicable in other transport subsectors, with the view to fully unlock the value of the use of **cyber range** in the **maritime logistics** value chain.

To achieve its objectives, Cyber-MAR platform will be both a **knowledge-based platform** & a **decision support tool** to cybersecurity measures, towards providing business continuity management

Cyber-SHIP Lab – University of Plymouth

Rory Hopcraft
Industrial Researcher
Maritime Cyber Threats Research Group

rory.hopcraft@plymouth.ac.uk

Thank you

References

- Barnett, M. L. (2005). Searching for the Root Causes of maritime Casualties. *WMU Journal of Maritime Affairs, 4*(2), 131-145.

- Cyber-MAR. (2019). Cyber-MAR - The Project at a Glance. Retrieved 24th April, 2021, from https://www.cyber-mar.eu/about/

- Endsley, M. R. (1995). Toward a Theory of Situation Awareness in Dynamic Systems. *Human Factors, 37*(1), 32-64. doi:10.1518/001872095779049543

- Stan Institute. (2015). Situational Awareness. Retrieved 28th May, 2021, from https://stan-institute.com/en/news/situational-awareness/