DIN STRATEGIC INVESTMENT INITIATIVE
CYBER TERRAIN MAPPING AND ANALYSIS OF OPERATIONAL TECHNOLOGY NETWORKS

PROBLEM

Modern military platforms rely on complex, diverse, and potentially volatile operational technology networks. One option for protecting and defending these networks from potential cyber threats is to deploy teams of Defensive Cyber Operators (DCOs). To prioritise defence of mission-essential systems and ensure the platform can effectively fight through cyber-attacks, DCOs must rapidly develop accurate and detailed cyber situational awareness on unfamiliar systems.
The aim of this project is to develop tools and techniques to accelerate mapping and analysis of unfamiliar operational technology networks. Goals include, but are not limited to:

- discovering devices on the network,
- identifying these devices and their relationships to other devices and subsystems,
- characterising typical device and system behaviour and evolution,
- and detecting anomalous behaviour.

DCOs must ideally be able to complete this mapping and analysis:

- passively, as active probing of mission-critical systems may be risky,
- with limited prior knowledge or annotated data,
- and as a small team with limited computational resources.

We are looking for innovative solutions to this problem which consider the operational constraints and can be applied to a wide variety of platforms, devices, and network protocols.

NEED AND RELEVANCE TO DEFENCE

Cybersecurity has been identified as a key strategic priority for Defence, with specific reference in the 2023 Defence Strategic Review and the AUKUS trilateral security pact. Development of new capabilities to support defensive cyberspace operations is critical to ensuring the resilience of Australian military platforms and missions in contested environments. Cyber terrain mapping and analysis is particularly essential, as it is foundational to the execution of effective defensive actions.

POTENTIAL RESEARCH QUESTIONS

- How might one fuse data from different networks and Purdue model layers?
- What techniques may be applied to discover, identify, and characterise devices?
- What device features and analysis techniques best generalise to different networks?
- What options are there for human-machine teaming to leverage operator knowledge?

EXPECTED OUTCOMES

- Tools and techniques, including models, algorithms, and analyses, for cyber terrain mapping.
- Evaluation of tools and techniques on diverse datasets demonstrating generalisability.
- An initial hardware or software prototype demonstrating tools and technique use by DCOs.
- A report covering the research and development process and potential future directions.