DIN STRATEGIC INVESTMENT INITIATIVE
PROBLEM STATEMENT 1: ONGOING USE OF A SYSTEM DESPITE COMPROMISE, ESTABLISHING AND (SELF)RESTORING TRUSTWORTHINESS

PROBLEM

How can we estimate or know whether a compromised system might still be fit for a specific purpose or mission at the operational edge, and what technologies might be applied to establish, assess and restore trustworthiness?
How can a system self-check or cross-check other parts of the system autonomously, and the system self-correct errors?
Include options for human input, in/on the loop. Consider reducing attack surface. Consider in terms of confidentiality, integrity, availability. Include partially and totally compromised systems, but where we still wish to employ it.

NEED & RELEVANCE TO DEFENCE

Cyber security is important for Australia's national security, innovation, and prosperity, and is a major priority for Defence. It cuts across all of the Defence StarShots, in particular Information Warfare. It is critical for the sustained integrity of systems and infrastructure.

RESEARCH QUESTIONS

- What ML techniques can be used and how can we assess their trustworthiness and reliability?
- What happens to ML algorithms when trained away from the operational edge and then deployed?
- How can we assess the authenticity of the links in our system?
- How can we determine which parts of the system are compromised, isolate them and dynamically reroute information around compromised parts with a dynamically changing threat?
- How can we have mission assurance and real-time situational awareness in systems that have departed from their original architecture?

EXPECTED OUTCOMES

Minimal impact on performance, e.g. network bandwidth; response times; energy consumption; size of equipment; SWAP.
Explainability of the answer of how we have established trustworthiness – establishing confidence in the machine response.
Explainability of how parts of a system can self-check or cross-check other parts.