Tier 1 Priority: Cyber

Defence is seeking to advance new science, technology, methods and concepts to support operations in cyberspace. This includes advanced capabilities to support Defence requirements in: cyber security; defensive cyber operations; intelligence; and effects and is conducted through research in: trustworthy and resilient systems; situational awareness; mission assurance; threat countermeasures and effects; cyber artificial intelligence and autonomy; and the human element. The Cyber theme is interested in proposals that address the following problem statements:

1. Information Warfare:

In support of the Information Warfare Science, Technology and Research (STaR) Shot, research is required into the application of artificial intelligence and machine learning (ML) techniques to cyber security.  High priority applications include the discovery of vulnerabilities in cyber systems, software, networking protocols and the discovery of anomalous behaviours in military and enterprise cyber systems.  Research is also needed into vulnerabilities of AI-based cyber defences, including mitigation against adversary use of data-driven attacks on ML-based cyber defences.

1. Operating in Chemical, Biological, Radiological and Nuclear (CBRN) Environments:

Research is required into Operating in CBRN Environment’s STaR Shot, particularly in relation to the management of vulnerabilities around large-scale sensor networks comprising sensors that might be low in cost and with small size, weight and power characteristics.  The research could consider such factors as: the identification of security vulnerabilities in individual sensors, solutions to improve trust in these devices; concepts for developing and maintaining cyber situational awareness of these distributed sensor networks; and for the autonomous management of cyber defences.

1. Agile Command and Control:

Agile military Command and Control requires decision makers at all levels to have an appropriate level of understanding of all factors that impact on decisions.  With military systems now almost completely dependent on digital information systems, cyber security is emerging as a critical element of full spectrum military situational awareness.  Research is required into technologies to support cyber situational awareness, including the ability to provide a level of abstraction suited to the needs of the military decision maker and the integration of cyber into full spectrum situational awareness.