INFORMATION WARFARE AND ADVANCED CYBER TECHNOLOGIES

DEFENCE TRAILBLAZER
CONCEPT TO SOVEREIGN CAPABILITY

The Australian Defence Organisation is no different to any other part of modern society in its reliance on information technology to conduct all facets of its operations, from personal management through acquisition and sustainment program management and operations at all levels, from the tactical to strategic. Modern technologies have also changed the impact of information operations and misinformation, and the Australian Defence Organisation needs to ensure it can conduct influence operations that support the country's objectives and hinder the operations of adversaries

GLOBAL TRENDS

Information Warfare

- Grey zone operations
- Countering Mis/ Dis-Information
- Mixed media consistency

Advanced Cyber Warfare

- Growing use of AI
- Increased Regulation
- Public-Private Partnerships

Potential Negative Impacts

- Reduced Military Capability
- Loss of Public Confidence
- Reduced Economic Confidence
- Delayed Logistics and Sustainment
- Impacted Utilities and Transport Infrastructure
- Reduced Industrial Activity

Worldwide Growth

Increased capability amongst Indo-Pacific nations

TECHNOLOGY DEVELOPMENT PRIORITIES

- Digital Influence
- Cyber & Electromagnetic Activity (CEMA) Tools
- Cyber Autonomy
- Cyber Resilience
- Experimentation and Wargaming

INDUSTRY PROGRAMS

SHORT TERM

Deployable cyber resilience interfaces for Defence platforms

POTENTIAL PROGRAMS

- Electronics Defect Detection
- Establishing Electromagnetic Compatibility (EMC) and Electromagnetic Interference Testing Facilities

UNIVERSITY CAPABILITIES

Information and Influence	Intelligent Cyber Security	Network Systems and Security	Cyber Defence and Attack Mitigation

THE UNIVERSITY of ADELAIDE

UNSW SYDNEY

LINKS TO SOVEREIGN INDUSTRIAL CAPABILITIES

Maintenance, Repair, Overhaul, and Upgrade (MRO&U) of Australian Defence Force Aircraft as it relates to the cyber-worthiness of aircraft and supporting systems.

Development and integration of autonomous systems through supporting operations in the cyber domain.

Integration and enhancement of battlespace awareness and management systems by supporting the development and operation of sensors across the Electronic Warfare spectrum and the cyber domain, as well as through battle space management of the capabilities associated with information warfare and advance cyber technologies.

Test and evaluation, certification and systems assurance as it relates to the cyber-worthiness of capabilities.

APPLICATION TO CAPABILITY