DSC 1475 – REV 3

PARTNERING WITH CYBER AND ELECTRONIC WARFARE DIVISION

Cyber and Electronic Warfare Division engages with Australia's industry and science and technology community through a range of innovative and mutually beneficial arrangements, and actively seeks opportunities to work with industry to commercialise DST technology and transition our innovative concepts into Defence capability.

Potential areas for collaboration include:

- Cyber Vulnerability Discovery
- Mobile Power Technologies
- Wireless Security
- Resilient Communications
- Antenna and RF Technologies
- EM Phenomenology
- Fibre Laser Technologies
- EW Countermeasures

For further information
Email: partnerwithdst@dst.defence.gov.au

www.dst.defence.gov.au

MAJOR RESEARCH PROJECTS AND ACTIVITIES

Force Protection Capability

Three force protection products have been developed by DST to defeat attacks by improvised explosive devices – a handheld device for dismounted soldiers and two more powerful systems for vehicles. The technology has been transitioned to industry for device mass production.

Ship Self-Defence Electronic Warfare Capability

DST provides S&T expertise to all aspects of the Nulka Active Missile Decoy program. This includes advice to Government on the technical merits of upgrades, assessment of contractor proposals, and support for new and updated tactics for the decoy. The Nulka decoy is fitted to over 130 warships in three fleets, and the program is currently developing next generation capabilities.

Fibre Lasers

DST conducts world-leading laser research and development. Fibre laser technology is the main area of interest because of its efficiency and ability to deliver high power from a compact and robust unit. DST laser technology has been commercialised for use in systems to protect military aircraft from guided missiles.

Light-Cone Direction Finding

DST has developed a light-cone direction finding algorithm capable of estimating the direction of arrival of multiple radio signals in order to reduce interference in an increasingly complex electromagnetic environment. The ability to perform direction finding in such an environment is a significant improvement on existing systems.

Cyber Security

DST is providing ongoing scientific support to the development of capability which will enable the Cyber security authorities within Defence and wider Government to more effectively monitor and secure national communications networks and information systems.Vulnerability discovery and mitigation, trustworthy ICT systems and autonomous cyber defence are key focus areas.

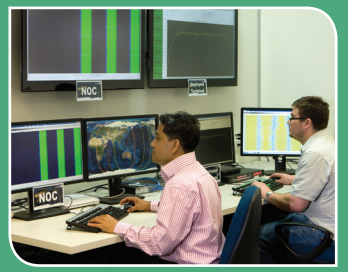
Signals Intelligence

DST continues to undertake research in a range of niche technologies as key enablers of evolving Australian Signals Directorate (ASD) capabilities in signals intelligence.

Australian Government
Department of Defence
Science and Technology

PARTNER WITH DST

CYBER AND ELECTRONIC WARFARE DIVISION



DST | Science and Technology for Safeguarding Australia

Major Science and Technology Capabilities (MSTC)

Cyber and Electronic Warfare Division undertakes research and development focused on identifying, analysing and countering threats to Australia's defence and national security through electronic means. Areas of major science and technology capability are:

MSTC Cyber Assurance and Operations - Supports enhanced performance in the presence of threats and unauthorised activities on computer resources.

Active Security Technologies develops concepts and specialised cyber technologies including computer network applications in support of Defence and National Security. A key area is high-assurance capabilities for resilient cyber systems in hostile environments including cross-domain solutions and multi-level security.

Cyber Defence Analytics addresses the S&T challenges associated with understanding and responding to advanced cyber warfare threats to the ADF's operational systems. Specific areas of focus are countering software threats, robust defences against attacks on machine learning, and autonomous cyber operations. This includes use of software program analysis, statistical and machine learning approaches, machine reasoning under uncertainty, data fusion, and autonomic computing.

Cyber and Cryto-Mathematics Research located within the Australian Signals Directorate (ASD), and is strongly focused on addressing operational problems through the application, research and development of mathematics and data science. This includes the use of modern mathematical techniques and high-performance computing, and statistical and machine-learning approaches, to address cryptological and data analysis challenges of secure and successful cyber operations.

MSTC Cyber Sensing and Shaping - Develops techniques for accessing, characterising and shaping communication networks to enable cyber operations.

Access Technologies Cyberspace is bridged to the real world through physical layer technologies, from photonic sensors, antennas and RF systems that interface the electromagnetic spectrum, through to the high speed computational systems that format and modulate raw data. This STC develops prototype solutions to niche problems and undertakes research and development in such technologies for cyber access and tailored wireless links.

Communications Network Research The infrastructure of cyberspace is a vast and interconnected network of networks. Security of cyber systems is critically dependent on the resilience of these networks to intrusion and manipulation and it is important that discovery of vulnerabilities, threats and malicious activity is undertaken towards a network gateway with a holistic view. This STC conducts research and development in the characterisation, modelling and exploitation of telecommunication core networks.

Communications Signal Processing conducts research and development in physical and cross-layer processing and analysis for the security and exploitation of telecommunications and consumer wireless networks.

MSTC Assured Communications - Provides solutions for robust communications in contested, complex and dynamic environments.

Protected Satellite Communications develops technologies and methods to increase the resiliency of Defence satellite communications in the contested Electromagnetic environment. Specific focus areas are autonomous monitoring in satellite networks, satellite network vulnerability analysis, interference mitigation and response, satellite system resilience and advanced satellite communications waveforms.

Protocol Exploitation undertakes research and development and provides S&T advice on the provisioning of robust communications in contested environments. Specific areas of focus include the analysis of protocol vulnerabilities and effects, electromagnetic interference reduction, interference mitigation planning and management, and protection strategies.

Survivable Networks undertakes development of andprovides S&T advice on the management of mission criticalradio networks, providing improved performance through dynamic network reconfiguration andtraffic control mechanisms within contestedtactical communication networks. Specific areas of focus aredistributed and autonomic network management, networkrecovery and mission critical service restoration, includingthe use of unmanned aerial vehicles.

Communications EW focuses on counter IED but is also developing a longer term programme in the area of communications EW and systemic effects. Specific areas of focus include include communications EW techniques, implementation of advanced concepts in hardware and software for force protection, RF systems and electronic engineering, software engineering, specialised RF device and system development, and trials.

MSTC Systemic Protection and Effects - Analyses and supports critical cyber physical systems, with respect to systemic electronic attack.

Automated Analytics and Decision Support undertakes research and development in concepts, technologies and techniques to better understand the current and projected state of own and threat cyber physical systems. Conducts activities in automated cyber analytics and decision support, cyber domain and mission modelling, visual analytics, scientific and threat intelligence, and software prototype development.

Distributed EW Experimentation and Simulation integrates EW systems, sensors, effectors and battle management tools/concepts within an information systems construct to examine Force-level EW concepts and analyse military systems. Infrastructure in this area includes sophisticated modelling and simulation environments and UAV-based distributed EW testbeds.

PNT Technologies and Systems develops techniques for denying Position, Navigation and Timing (PNT) to adversaries while maintaining our own PNT against Electronic Attack. This is a fundamental component of systemic electronic protection and effects.

MSTC Spectrum Sensing and Shaping - Supports enhanced situational awareness in complex RF environments, and defeating the future networked EW, cyber and kinetic threats.

RF Technologies develops and maintains expertise in RF technologies with a focus on maritime off-board EW. Specific activities include Electronic Sensor systems, RF integrated circuits, solid state power amplifiers, wideband receive and transmit multichannel apertures, millimetre wave technologies, RF propagation phenomenology, advanced test and measurement equipment and countermeasure technique development through modelling, simulation, analysis and experimentation.

RF Systems develops and maintains expertise in Radar Warning Receivers (RWR), Electronic Support (ES) and Electronic Intelligence (ELINT) Systems. This requires expertise in advanced ultra-wideband RF-to-digital receiver design, digital signal processing and multichannel architectures. Application areas include next generation EW, SIGINT and Cyber-EM systems for sensing and shaping the EM environment.

RF Techniques and Exploitation builds and maintains expertise in RF off-line analysis by developing leading-edge mathematical and statistical-based algorithms for challenging ES and SIGINT applications. Enabling technologies include parallel processing engines for high-volume data throughput, cognitive signal exploitation and multi-sensor systems for optimising signal processing algorithm performance. The STC is responsible for developing advanced TechSIGINT tools and tactical decision aids.

MSTC EW Operations - Provides countermeasures for detecting and defeating threats using the electromagnetic spectrum.

Electro-optic (EO) Counter-measures undertakes research and development in technologies and techniques to understand, detect and defeat electro-optic threats. Includes EO system design, performance prediction and testing of missile warners and missile seekers, and signal processing and algorithm development. There is significant investment in testing and validating countermeasures, including the development and use of a hardware-in-the-loop test-bed, and design and conduct of complex trials.

RF Electronic Attack develops concepts and technology for defeating future networked, highly adaptive and increasingly complex RF threats. Activities include threat analysis, RF countermeasures development, testing and validation against advanced threats, investigating electronic attack (EA) techniques for use against adaptive software defined threats, and the on-going development of RF countermeasure test beds. RFEA has capabilities in advanced signal processing, machine learning, software and firmware programming, signal injection, and the design and execution of complex EW trials activities.

Laser Technologies focuses on laser technologies and systems for understanding, detecting and defeating threats. Has a world leading capability in solid state and fibre laser physics with the main areas of interest being high power lasers (HPL) and spectral diversity for laser countermeasures. Also investigates and builds prototype novel laser systems for threat detection and mitigation. Specific activities include nonlinear optical physics, fibre Bragg grating design and fabrication, specialised photonic component design, optomechanical manufacture and integration, and laser system design and integration.