Australian Government
Department of Defence
Science and Technology

Cyber and Electronic Warfare Division

S&T to understand and counter the threat using electronic means




Strategic Plan 2016-2021

DST | Science and Technology for Safeguarding Australia

Cyber & Electronic Warfare Division: Foreword

Chief Cyber & Electronic Warfare Division
Dr Jackie Craig

Cyber and Electronic Warfare Division was formed as a result of the recognition that cyber and EW domains share a number of characteristics; both develop situational awareness to gain warning of threats and to characterise the signatures of existing known threats in order to enable rapid identification, both develop defensive techniques to neutralize the effect of threats when they are encountered, and both develop effectors intended to shape the battlespace and to impact on an adversary's capability to operate in the cyber or EW domain. They also both face challenges from the increasing ease of use of commercial technology to create previously unseen threats at relatively low cost. There should be important synergies and complementary activities that can each inform efforts in the other domain.

A natural next step is to think about how cyber and EW may be integrated, or perform complementary functions. The idea of an overlapping Cyber-EW concept then led to the birth of the Cyber-EW Continuum. This concept is a representation in which the "pure" or "traditional" cyber and EW capabilities reside at each end of the continuum, the essential enabling capabilities of SIGINT and communication lie within, and the overlapping and synergistic cyber-EW capabilities lie in the centre. This concept is at the heart of CEWD's structure as well as its strategies for technology development and transition to ADF capability.

This plan is the first attempt to develop an integrating strategy, built on the EWRD strategic plan of 2011 and the 2014 Cyber 2020 vision. In addition to integrating across the Division, the plan is intended to provide useful guidance on trends, priorities, and directions in investment intentions to inform both internal and external stakeholders.

Dr Jackie Craig
Chief, Cyber and Electronic Warfare Division

Part I

Contents

Executive summary

The Cyber & Electronic Warfare Division (CEWD) Strategic Plan has been developed to guide the Division's activities across the breadth of its program and to provide key stakeholders, and the national and international science communities, a detailed view of CEWD's approach to addressing the current and future challenges faced across the Cyber-EW continuum.

The Plan situates CEWD and its role in a rapidly evolving and challenging environment, describes its approach to meeting these, and sets out the Vision and Mission. Significant successes are highlighted to illustrate a high-performing track record of achievement for Defence and National Security. The role of, and challenges facing each of the six Major Scientific and Technology Capabilities (MSTC) that comprise CEWD are outlined, along with the approach each will take, in terms of the trajectory of its S&T focus, key partnerships and infrastructure plans.

The Plan identifies five foundational research themes that are enduringly relevant, sufficiently comprehensive to explore the Cyber-EW problem space, support the development of future capability, and can be readily applied to priority problems.

These are:

- Future Threat Estimation
- Integrated Vulnerability Assessment
- Integrated Effects against an Unknown Threat
- Cyber-EW Battle Management
- Full Spectrum Mission Survivability

CEWD's approach to planning and delivering its program is delineated, enshrining a balanced, integrated and strategic intent, which also encompasses principles by which the sustainment and development of S&T capabilities, equipment, facilities and skills will be maintained and developed.

People, their skills and capabilities are absolutely critical to CEWD achieving its Mission and delivering to stakeholders. A clear statement of intent is made covering our approach to personal, professional and leadership development of all staff.

Cyber & Electronic Warfare Division Overview

Part II

CEWD - Narrative

Cyber and Electronic Warfare Division has deep science and technology expertise in cyber, signals intelligence, communications and electronic warfare. The core activities undertaken by the Division are: scientific and technical intelligence (STI) to provide an understanding of the current and future threat landscape; development of techniques, technologies and tools for vulnerability assessment, threat warning, situational awareness and communications in complex electromagnetic and cyber environments; development and validation of countermeasures; and development of techniques, technologies and tools for ensuring cyber and EW mission success.

CEWD has a significant track record in developing and delivering advice and solutions for Defence and National Security, often in partnership with other parts of Defence, industry or overseas partners. Examples of this include counter improvised explosive device capabilities; improved electro-optic self-protection for air platforms; naval platform self-protection against anti-ship cruise missiles; improved battlespace communications; improved electronic surveillance capabilities; specialised capabilities in cryptomathematics; and specialised capabilities in Cyber Operations, novel computer security devices and applications, tailored communications and network analysis.

A key role for CEWD is to provide S&T leadership in defining and influencing the rapidly emerging relationships between cyber, SIGINT, communications and EW. It is the convergence of these areas into a continuum that is shaping both the threat landscape and future capability. A major focus will be on countering challenging (zero-day) threats in a networked system-of-systems context and achieving mission assurance in contested cyberspace and electromagnetic environments. The approach will be multi-disciplinary, integrating concepts, techniques and technologies from across the cyber-EW continuum to identify and develop new capabilities that will be relevant and effective in a data-driven, networked, cyber-physical future. There will be a decreased emphasis on traditional concepts and techniques, and an increased investment in emerging technologies such as cognitive EW capabilities to detect and defeat challenging threats. There will be a growing emphasis on cyber within a military systems context and concepts such as survivability will extend to full spectrum (mission) survivability that includes the survivability of platforms, electronic systems and networks against a range of threats, including cyber threats. Ubiquitous technologies within the Division will include software defined systems leading to multi-function concepts and demonstrators, data sciences to support detection of hard targets in highly cluttered environments, machine intelligence and autonomous systems in support of distributed EW, military communications, network management and cyber operations.

The Vision for Cyber and Electronic Warfare Division is:

“CEWD will be a centre of world-class, multi-disciplinary research and development in cyber, signals intelligence, communications and electronic warfare, and will be at the forefront in the integration of these areas to provide innovative solutions to challenging problems in the cyber-EW continuum”.

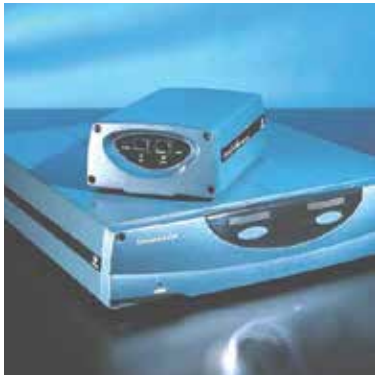
The Mission for Cyber and Electronic Warfare Division is:

“To maintain and develop a Science and Technology capability that will position Australian Defence and National Security Agencies to successfully operate in contested cyberspace and electromagnetic environments against variable, diverse and rapidly evolving threats.”

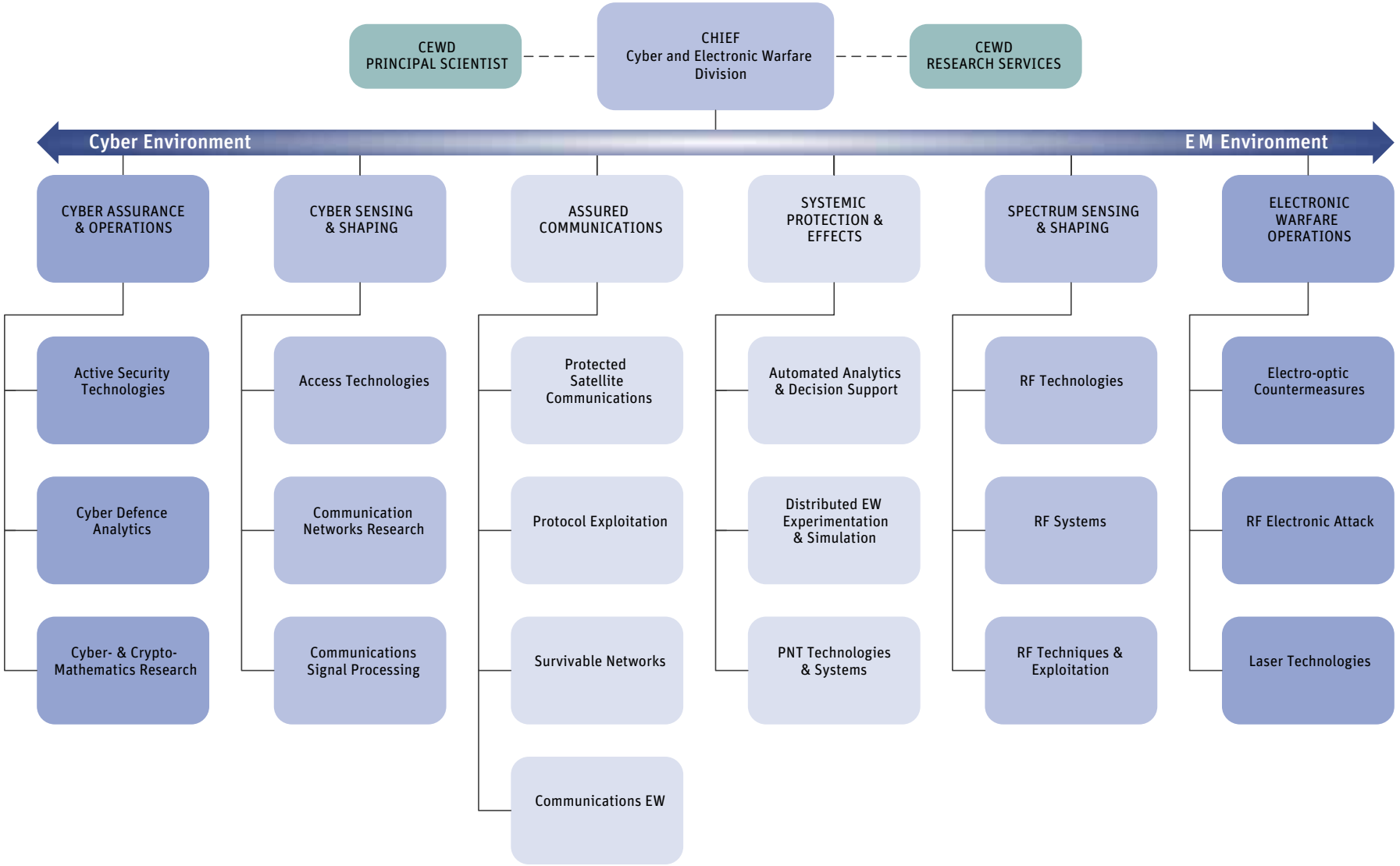
CEWD has been organised to reflect the cyber-EW continuum. At each end there are the traditional cyber and EW capabilities, encompassed in the Cyber Assurance and Operations (CAO) and EW Operations (EWO) MSTCs. The Cyber Sensing and Shaping (CSS) and Assured Communications (AC) MSTCs conduct S&T concerned with modern civilian and military communications systems and networks. Their place on the cyber-EW continuum reflects the increasing convergence of cyber and SIGINT (CSS), and cyber and communications electronic warfare (AC). The Systemic Protection and Effects (SPE) MSTC has a focus on protecting and defeating systems, and in understanding the

vulnerabilities of blue and red systems to a broad spectrum of effects. Its position at the centre of the continuum signals its role in developing concepts and techniques based on combined cyber, EW and cyber/EW effects. Spectrum Sensing and Shaping (SSS) retains its roots in threat warning, electronic surveillance, electronic intelligence and countermeasure techniques and technologies, with some small involvement in cyber through its investment in RF technologies and sensors.

S&T excellence, innovation and collaboration will be central features of the CEWD culture. The Divisional program will range across several MSTCs, building a strong multi/interdisciplinary, forward looking, S&T capability that serves the current and future needs of Defence and National Security. In the following pages each MSTC describes its science and technology "profile" in terms of three key elements: the strategic direction of the science and technology, the important partnerships and the critical infrastructure needs. This includes the major S&T areas that we will invest in, and (importantly) the S&T areas that will be de-emphasised. Understanding what we will leave behind is as important as understanding our new horizons – we cannot do everything if we wish to be excellent in our science and technology and continue to have impact. Each MSTC also provides an outline of how the S&T profile will deliver impact to Defence, thereby providing context to our decisions.



CEWD Organisation Chart



CEWD - Successes

Trustworthy ICT

Prototyping and demonstrating the hardware Trojan threat.

DVG

DVG enabled tablet

Digital Video Guard

A small peripheral inserted between a host computer and a screen enables trusted video display

Winner of the South Australian ICT Innovation Award 2014.

Wideband Global SATCOM Anchoring Monitoring System

A rapidly delivered solution to monitor all ADF satellite communication systems in off-shore anchoring facilities.

CEWD - Successes

Redwing Program

Low-cost, robust, lightweight CIED systems for light vehicles and dismounted personnel in operational areas

"May I express my personal thanks for the efforts of the relevant staff in Communications Electronic Warfare (CEW) Group … for their efforts in developing and delivering this important capability." BRIG Shanahan, COMD CIED Task Force

BLIZZARD

Addition to submarine UHF SATCOM that significantly enhances its reliability.

Geolocation

Capability developments in EA18G-Growler and other strategic and tactical platforms via US-AUS collaboration.

CEWD - Successes

Global Positioning

Developing GPS anti-jam capabilities for ADF platforms.

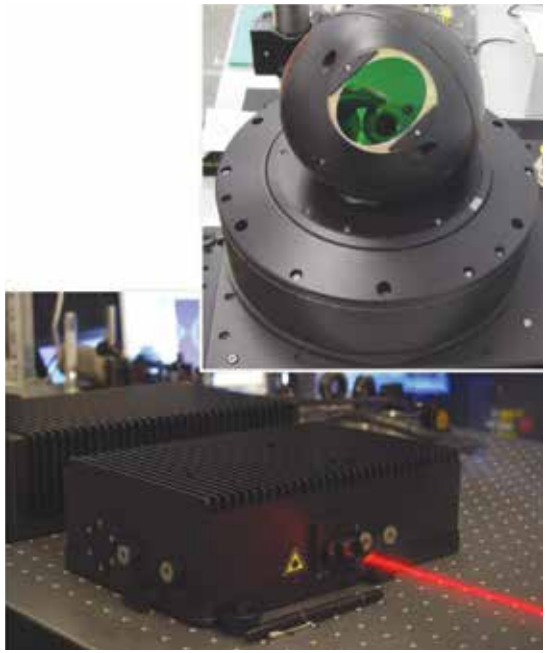
Maritime Situational Awareness

LIVE demonstrator exploits third party surveillance data and intelligence data to support beyond-the-horizon situation awareness for Royal Australian Navy vessels

ES/ELINT S&T Transition into MOTS

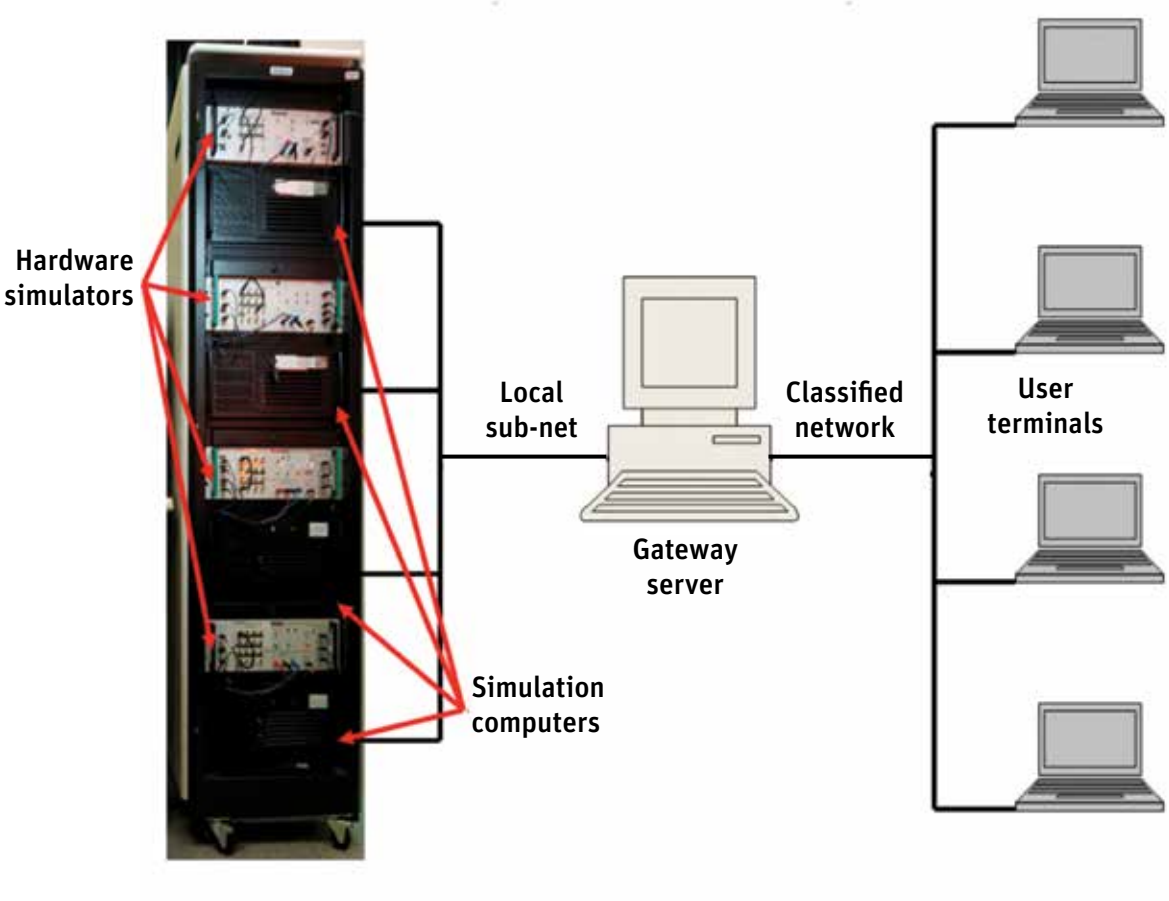
Independent carry on/carry-off tactical ELINT & integrated ES system variants transitioned to industry for supply to military forces.

CEWD - Successes



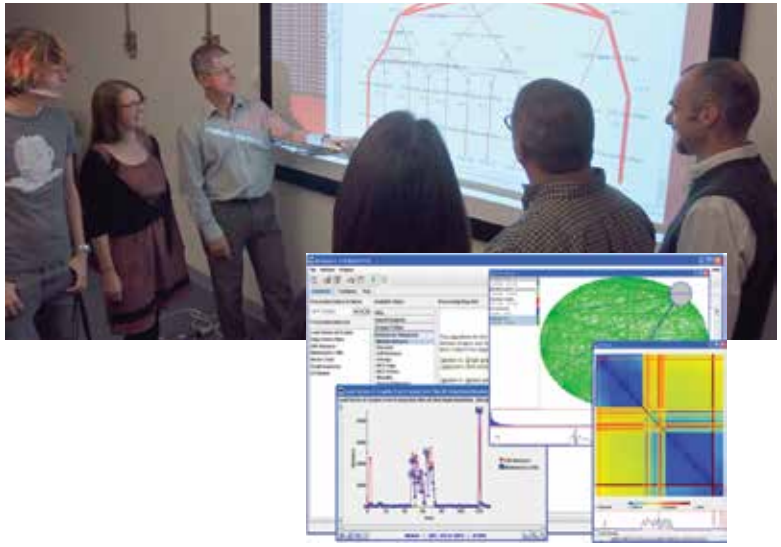
World-class Laser Research - DIRCM

Directed Infra-Red Counter-Measure Laser (DIRCM), provides a robust, compact, capable laser solution to the infrared missile threat, transitioned to industry under licence.



Integrated Hardware In Loop Simulation Facility

CEWD - Successes



Digital network intelligence

Analytical tools for characterising and understanding large scale, complex communication and computer networks.

Operational capability enhancements at the JDFPG

An ongoing program of over 20 years of S&T support to enhance Australian interests and the mission of the Joint Defence Facility Pine Gap

"The impact … was tremendous. Without it we would have very little useful data to work with."

"Very exciting! … rapidly moving from a development/engineering project to sustained production status."

CEWD Science & Technology Plan

Part III

Cyber Assurance & Operations - Vision and Mission

Vision

The Cyber Assurance and Operations (CAO) MSTC will be regarded by 2019 as a critical enabler of effective cyber operations and trustworthy and resilient systems.

Mission

To enable autonomous, resilient and effective cyber capabilities with an operational edge in the face of ubiquitous encryption, untrustworthy ICT and a highly dynamic, sophisticated and perimeter-less threat environment

Challenges and Technology Drivers

There is an increasing national dependence on information and communications technology (ICT) driven by growth in digital productivity and services. Cyber-physical systems – the coordinated coupling of physical, computational and networking elements – pervade (the Internet of things), giving rise to typically Internet facing homes, possessions, vehicles, critical infrastructure, military capability and national enterprise. With growth in ICT dependence is a lag in cyber security, increasing the vulnerability of government, industry and society to threats in various forms. Mitigating this vulnerability necessitates that systems be designed and built for cyber security, defended against an ever-evolving cyber threat, and operated in a manner which maximises effectiveness within and through cyberspace. Australia's 2013 National Security strategy highlights development of "sophisticated capabilities to maximise Australia's strategic capacity and reach in cyberspace…" as a matter of national security. The 2013 Defence White Paper shows critical dependency of modern military capabilities on information systems.

Brief overview

It is considered that during the 5-year term of this strategic plan:

Enhanced functionality, productivity and services will continue to drive developments in ICT ahead of cyber security

Significant national security drivers for sovereign operational cyber capabilities will remain

Commercial developments in cyber security will be many and far reaching

Generic intrusion detection and protection, and forensic malware analysis tools will become commodity items, and any required tailoring will not be a matter of research

R&D challenges will need to be overcome before commercial vulnerability analysis and incident response tools appear which can reason about dynamic system properties and context

Commercial multi-level security products will not have matured which strike the right balance of cost, performance and security required for high-assurance applications

Acquisition times for military capability will mean that military deployed networks and more so platforms will lag behind corporate Defence infrastructure in cyber security

Given this context, drivers and challenges, the core areas of S&T for the CAO MSTC are:

Vulnerability discovery and mitigation: Discovering application and operating system vulnerability, Discovering and countering malicious cyber activity and Autonomous cyber defence

Future threat estimation: Forecasting and prototyping advanced forms of adversarial software and hardware, and concepts of future autonomous adversarial cyber capabilities

Crypto-mathematics: Exploiting/employing and combating ubiquitous encryption

Trustworthy and Resilient Systems: Resilient ICT and Pervasive security policy and architectures

Cyber Assurance & Operations Science & Technology Profile

S&T Trajectory

Invest

- Future Threat Estimation
  - Forecasting and prototyping advanced forms of adversarial software and hardware
  - Concepts of future autonomous adversarial cyber capabilities
- Vulnerability discovery and mitigation
  - Discovering application and operating system vulnerability
  - Discovering and countering malicious cyber activity
  - Autonomous cyber defence

Crypto-mathematics

- Exploiting/employing and combating ubiquitous encryption

Trustworthy and Resilient Systems

- Resilient ICT
- Pervasive security policy and architectures

Reduce

Mainstream intrusion detection and protection

Mainstream malware analysis tools

Partnerships

Within DST Group

- CEWD MSTC's CSS, SPE and EW Ops
- NSID MSTC's Intelligence Analytics (IA) and Information Integration (II)
- JOAD

National

- Nicta/CSIRO
- Dept Foreign Affairs & Trade
- University of NSW
- Aust Centre for Cyber Security/ADFA
- Attorney General's Dept/CIPMA
- Defence Science Institute
- Northrop Grumman
- CISCO

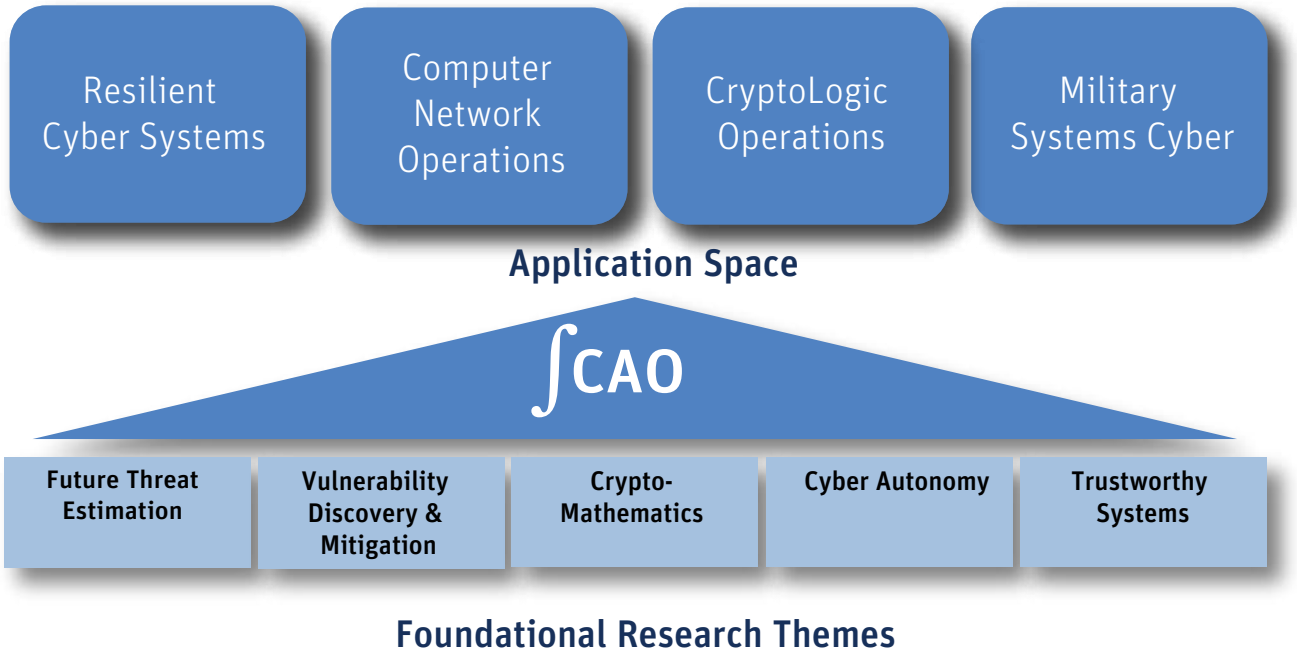
International

- Military 5 Eyes Cyber (MSIC, DSTL, GCHQ)
- Secure Mobile (5 Eyes)
- Trustworthy Systems (TTCP)
- Mission Assurance and Situational Awareness (TTCP)
- UKUSA/DOMEPLATE
- US Dept Homeland Security

Key Infrastructure Plans

- Provision of an Unclassified network supporting cyber research and experimentation
- Establish a TS level Innovation Environment with client connectivity
- Establish a presence on the Joint IO Range
- Continue to use and enhance ASD's High Performance Computing infrastructure
- Sustain hardware and software engineering laboratories

Cyber Assurance & Operations Major S&T Capability



Cyber Sensing & Shaping - Vision and Mission

Vision

Recognition as world class leaders of S&T in cyber aligned signals intelligence

Mission

Delivery of concepts, techniques and technologies for sensing and shaping modern communication networks to address challenges in cyber and related areas of signals intelligence.

Challenges and Technology Drivers

Cyberspace is continuing to grow in complexity and dynamism. This is being driven by an increasing demand for mobility, explosion in the number and diversity of networked devices, ubiquitous encryption, escalation of data volumes, and widespread use of software defined systems. These technology trends collectively present significant research challenges to maintain and extend Sigint and Cyber capabilities for access, analysis, exploitation, and defence. Communication networks and wireless capabilities in Cyber are central to this problem space.

Brief overview

Cyber Sensing and Shaping (CSS) MSTC develops concepts, techniques and technologies to provide access, characterisation, analysis & shaping of modern communication systems and networks. Aligned with the growing convergence between signals intelligence and cyber, the focus of the MSTC extends from physical through to network layers, with S&T capabilities comprising Access Technologies, Communication Networks Research, and Communications Signal Processing. The interests of the MSTC extend from the core network of modern telecommunications systems and the internet, through to fixed and mobile nodes and bespoke wireless systems.

Research in physical layer technologies includes antennas and RF systems, optical sensors and micro-technologies, through to high speed reconfigurable transceivers. Skills in communication theory and signal processing, software defined radio, wireless protocols, and RF geolocation underpin research in telecommunications and consumer wireless networks. Research in telecommunication networks and cyber security draws on skills in communications engineering, graph theory, statistics, decision theory, information sciences, data mining, machine learning, and information retrieval.

Cyber Sensing & Shaping Science & Technology Profile

S&T Trajectory

Invest

Fixed and wireless network characterisation and vulnerability research

Network knowledge and communications situational awareness

Cross-layer/bearer feature discovery and data association

Technologies for information access

Secure communications theory and technology

Antennae

Reduce

RF collection systems

Traditional physical layer signals analysis

Partnerships

Within DST Group

Electromagnetic cyber (AC and CAO)

Cyber situational awareness (SPE)

RF technologies and signal processing (AC and SSS)

Space and information fusion (NSID)

National

Bodyworn and metamaterial antennae (Adelaide Uni)

Network analysis and data sciences (Adelaide Uni, RMIT)

Signal processing adjunct researcher appointments (UniSA, ANU)

International

UKUSA community

TTCP: Cyber Strategic Challenge and Community of Interest Lasers

US Dept Homeland Security: Internet routing security

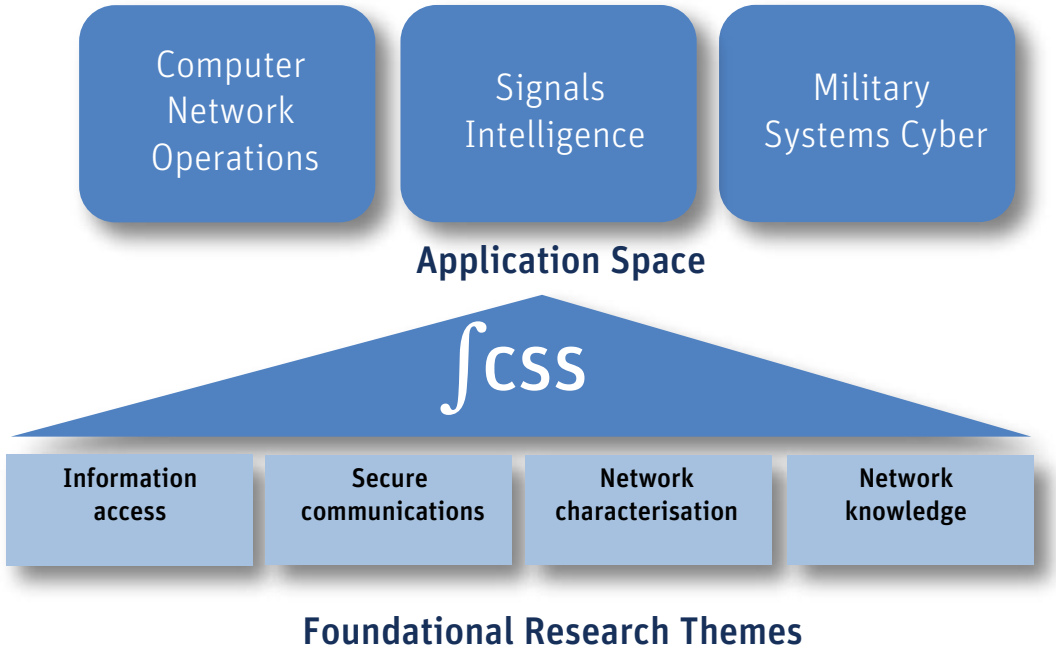
Key Infrastructure Plans

Additive manufacturing capability for 3D antenna printing

Establish experimental classified cloud environment

Establish tactical wireless Cyber laboratory

Cyber Sensing & Shaping Major S&T Capability



Assured Communications - Vision and Mission

Vision

To conduct R&D to assist ADF in achieving robust and survivable global communications systems operating in complex and dynamic military environments that have similar attributes and performance to the modern communications systems people take for granted in their personal lives.

Mission

To develop survivable tactical communications and electronic warfare solutions for contested and denied cyber electromagnetic environments.

Challenges and Technology Drivers

Challenges

- Current ADF communications capability has significant shortfalls
- Threats are increasing and evolving with time
- Commercial solutions do not offer adequate capability
- Allied solutions are not sufficient
- The ADF procurement process has difficulty keeping up with the fast pace of technology change in communications and IT
- Consolidation of communications, ELINT and EW functions onto the same hardware platform
- Increase in cyber threats and therefore in cyber defence

Technology Drivers

- Autonomous software agents
- Small autonomous vehicles acting as mobile communication network nodes
- Use of modern networked communications for IED threats
- Decreased cell size in modern networked communications reduces risk of interference
- Integration of software for communications, ELINT and EW functions to gain capability from convergence

Brief overview

Customised systems can sometimes be used by the military but the majority of military applications need communications that are far more protected and resilient than commercial systems can offer. Many military platforms such as submarines and fighter aircraft have no commercial counterparts and custom systems need to be developed to meet their needs. Assured Communications Branch leads DST Group's research in specialist military communications. It concentrates on military specific problems and techniques not addressed by commercial developments. It advises ADF on capability development and procurement.

The Protocol Exploitation Group develops algorithms for assessing vulnerabilities in radio networking protocols to better protect ADF networks. It develops innovative techniques to mitigate co-site interference among radio and EW systems on military platforms.

The Survivable Networks Group develops autonomous networking systems to increase the robustness and throughput of terrestrial ad-hoc radio networks.

The Protected Satellite Communications Group develops novel satellite communications capabilities for ships, submarines and land forces, enhancing ADF's ability to recognise and respond to cyber-EW threats to satellite communications

The Communications Electronic Warfare Group develops countermeasure techniques and devices to protect Australian forces from Improvised Explosive Device (IED) threats.

Assured Communications Science & Technology Profile

S&T Trajectory

Invest

- Automation and machine learning for electronic warfare capability and vulnerability protection
- Anti jam satellite communications
- Software agent technologies for satellite communications cyber network defence
- Radio networking using autonomous vehicles in degraded and denied environments
- Defence against improvised explosive device threats based on advanced communications waveforms

Reduce

- Expensive, military-grade software defined radios (transition to commercial devices)
- Time division multiple access satellite communications (research largely completed)
- Satellite communications modelling (transition to contractors)

Partnerships

Within DST Group

- Trusted Autonomous Systems Strategic Research Initiative

National

- Autonomous UAV systems (University of Melbourne, RMIT)
- Land radio networking (University of SA)

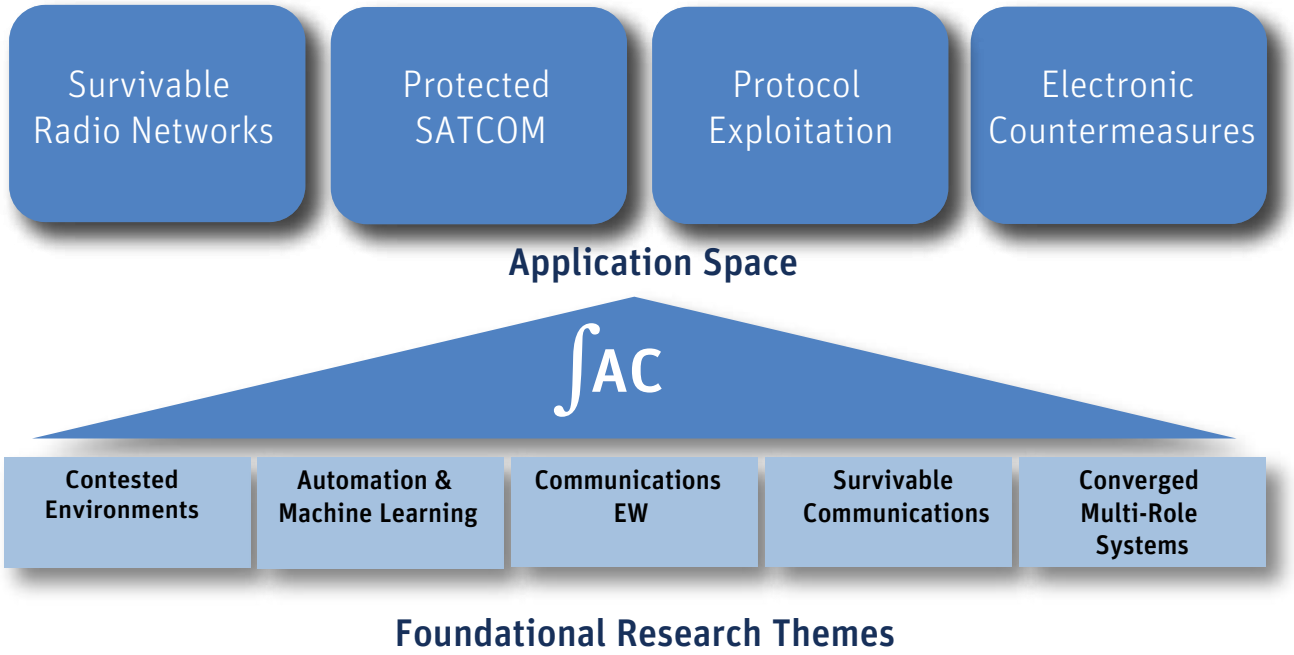
International

- Protection against improved explosive devices (Allies)
- Cognitive electronic warfare and cognitive networking (Allies)
- Next generation satellite communications (US Department of Defence)
- Radio networking (Allies, US Department of Defence)

Key Infrastructure Plans

- Major upgrade to the satellite communications facilities over period FY16/17-FY18/19
- New test range for evaluating effectiveness of electronic countermeasures against improvised explosive device threats

Assured Communications Major S&T Capability



Systemic Protection & Effects - Vision and Mission

Vision

To be recognised leaders in the ADO and internationally in understanding and implementation of future force level EW and cyber capabilities, and their integration with each other and with enhanced command & control.

Mission

Maximise Australian Defence & National Security capability through the development and delivery of solutions for the integration of force-level Cyber and EW with effective command & control.

Challenges and Technology Drivers

Technology advancement is outpacing our ability to use new and future capabilities operationally in both cyber and EW. Increasingly there is a need for automation to support commanders conduct missions. Denial of space is assumed to be a feature of future warfare.

- Increasingly numerous, networked, EM-capable platforms
- Increasingly complex EM environments
- Threat evolution – networked, software-driven
- Increasingly reliant on PNT
- Emergence of Cyberspace as an operational environment
- Critically reliant on cyber-physical systems

Brief overview

The SPE MSTC conducts R&D in the development of concepts, technologies and techniques for the analysis of red and blue military and national critical cyber physical systems, with respect to their vulnerability to and protection from systemic electronic attack. The work of the MSTC supports Defence, the AIC and National Security.

The Distributed EW Experimentation and Simulation STC integrates EW systems, sensors, effectors and battle management tools/concepts within an ISREW construct. The STC has a number of significant underpinning infrastructure elements including sophisticated modelling and simulation environments and UAV-based distributed EW testbeds.

PNT Technologies and Systems STC develops techniques for denying PNT to adversaries while maintaining our own PNT against electronic attack. It is a fundamental component of systemic electronic protection and effects.

Automated Analytics and Decision Support STC undertakes R&D in concepts, technologies and techniques for the understanding of the current and projected state of own and threat cyber physical systems.

Systemic Protection & Effects Science & Technology Profile

S&T Trajectory

Invest

- Establish S&T program in precision timing technologies and techniques
- Foundational S&T in novel geolocation techniques
- Research into enhanced M&S techniques for cyber-EW
- Artificial intelligence concepts, techniques and technologies for decision support

Reduce

- GPS related RF propagation studies
- Experimentation under SA-29
- Routine analysis

Partnerships

Within DST Group

- RF systemic EA – TMAP, Chimera
- AI techniques

National

- Academia on precision timing

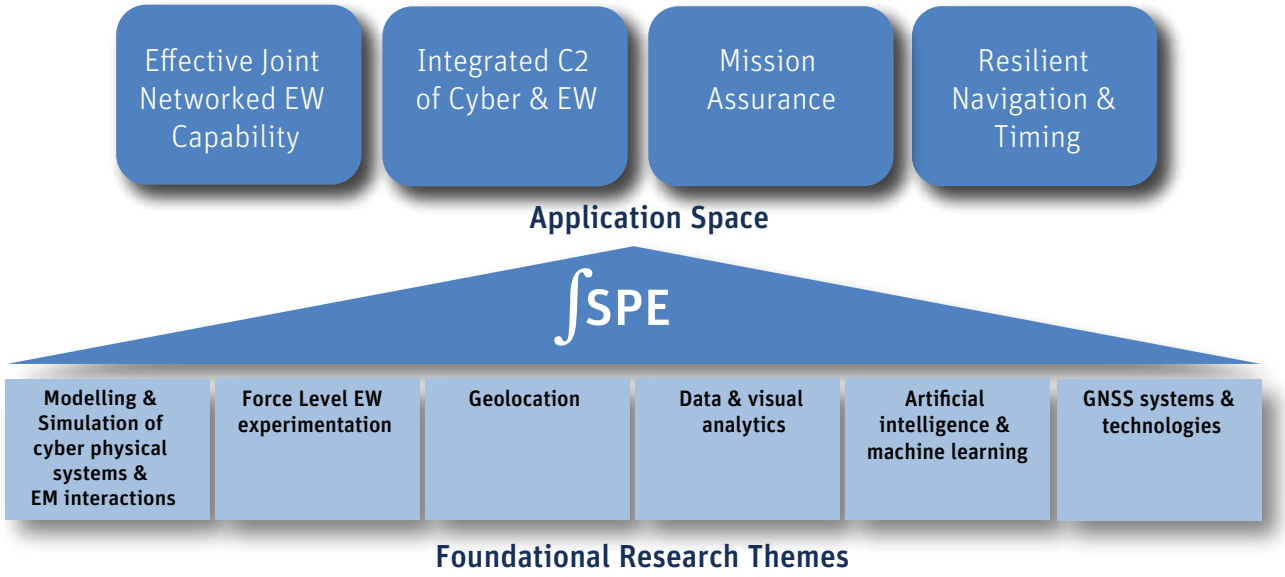
International

- S&T collaboration with ERD partners
- Ramp up MARC PA activities
- Precision timing
- DEWSAR complete 2018

Key Infrastructure Plans

- Establish a precision timing laboratory
- Upgrade SATSIM
- Modify SHEWT to be capable of integrating with Theatre Networked Geolocation
- Transition FLEWSE from STAGE to open source scenario generation [in order to make available to more users]
- Continue with annual upgrades to threat M&S facilities
- Establish shared cyberspace enclave under MARC PA

Systemic Protection & Effects Major S&T Capability



Spectrum Sensing & Shaping - Vision and Mission

Vision

To be recognized by the ADO as the technical experts in state-of-the-art RF technologies, systems and techniques that enable critical Electronic Warfare (EW), SIGINT and Cyber-EM operations of relevance to the ADO.

Mission

To develop and transition RF technologies, systems and techniques to the ADO that sense and shape the EM Battlespace to ensure the ADO can use it as required for EW, SIGINT and Cyber-EM operations, whilst denying the adversary the ability to do the same, in contested, congested and competitive EM (C3EM) environments.

Challenges and Technology Drivers

The EM battlespace is evolving with low cost entry to high performance materials, devices and computation making the “smart edge” accessible to many actors. This has seen the development and proliferation of advanced RF sensors and effectors that will degrade the ADO’s freedom of EM Manoeuvre and ultimately mission effectiveness, particularly in the anti-access area denial (A2AD) military operating environment. Further complicating the traditional EM battlespace is the emerging convergence of RF EW, RF Communications and Cyber technologies that present both threats and opportunities to the ADO. The C3EM environment represents a grand challenge for the ADO to effectively sense and shape the RF spectrum, so as to retain decisive military advantage in this critical global common.

Brief Overview

The Spectrum Sensing & Shaping MSTC is responsible for the development of advanced RF technologies, systems and techniques to provide the ADO with situational awareness, threat warning and countermeasure capabilities in the EW, SIGINT and Cyber-EM domains. In particular the S&T of RF technologies, systems and techniques is pursued by the MSTC to provide timely interception, detection, classification, identification, degradation, deception, disruption, denial and defeat capabilities of the complex threat. The work of the MSTC supports both the ADO and the AIC.

The RF Technologies STC 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, millimeter wave technologies, RF propagation phenomenology, advanced test and measurement equipment, and countermeasure technique development through modelling, simulation, analysis and experimentation.

The RF Systems STC 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.

The RF Techniques & Exploitation STC builds and maintains expertise in RF intercept techniques and exploitation 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 and multi-sensor systems for optimising signal processing algorithm performance. The STC is responsible for developing advanced TechSIGINT tools and decision aids.

Spectrum Sensing & Shaping Science & Technology Profile

S&T Trajectory

Invest

- Advanced wide-band RF digital sensor and effector technology
- Multi-sensor and multi-channel processing technology
- Long-range Electronic Support
- Numerical modelling, simulation and analysis support for Maritime EW Mission Survivability
- Low SWaP RF technology development and experimentation
- Algorithms, techniques, architectures and tools for RF SIGINT big data exploitation
- Cognitive signal exploitation for RF emitter identification/intent

Reduce

- Atmospheric environmental modelling
- Support to F/A-18 RWR co-development
- Support to acquisition of ES-3701
- RF photonics research
- Routine T&E support to Projects

Partnerships

Within DST Group

- Cognitive EW systems (EWO/AC)
- Passive Radar, Radar, Dynamic Signatures (NSID)
- Radar-Communications ES (CSS)
- Tactical Decision Aids (NSID, JOAD)
- Full Spectrum Survivability (SPE, WCSD)

National

- Advanced RCVR transition (Ultra-Avalon, CSIRO)
- Antenna design (Lintek, Puzzle Precision, USA)
- Low SWaP RFEW (BAE, Micreo, MACOM, ASD)
- TechSIGINT/TACAIDS (Ultra-Avalon, USA, ASD)

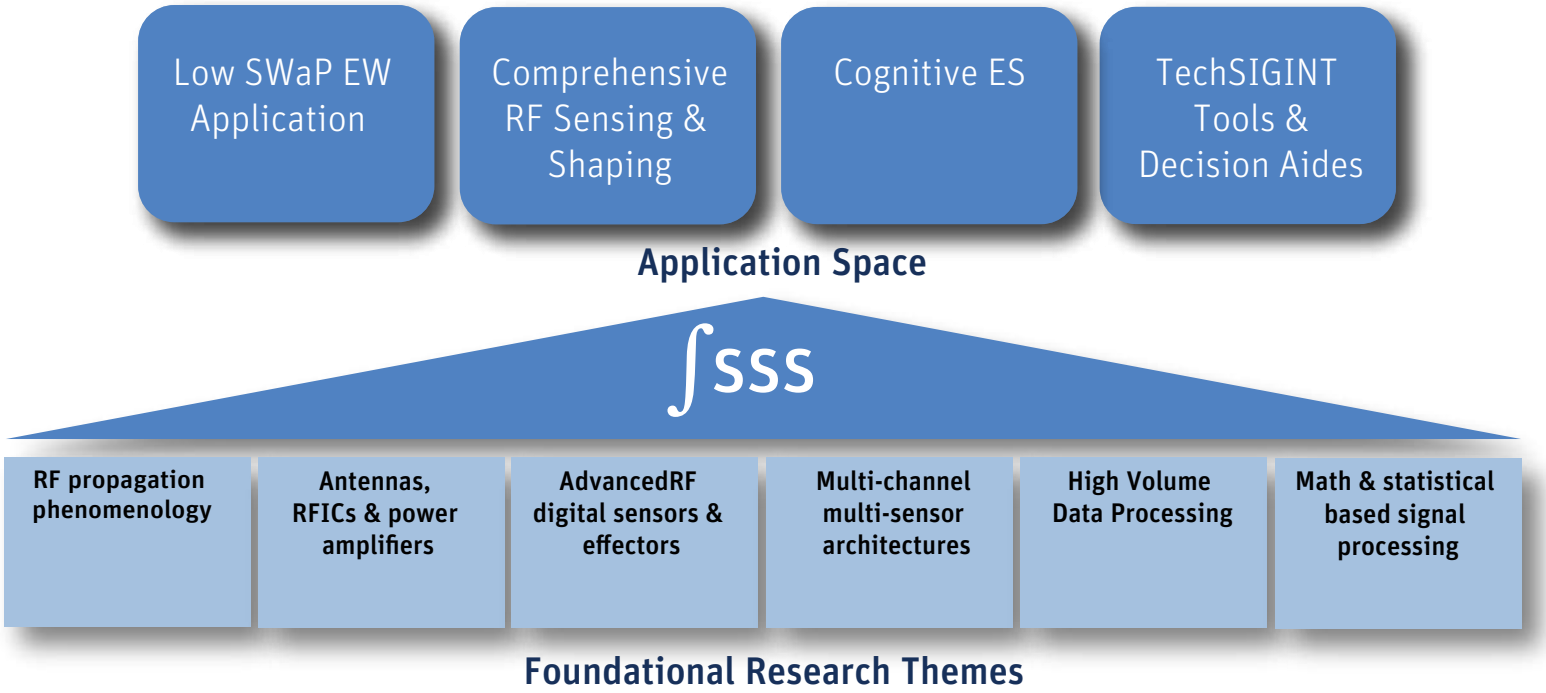
International

- ONR/NRL, NUWC, NSWC Crane, NSWC Dahlgren
- USN TECNAP, SPAWAR
- Dstl, DRDC, DTA, NRO
- TTCP, Square Dance, ABCANZ, Nulka, PFSD MOUs
- Arizona State University

Key Infrastructure Plans

- Develop ultra-wideband multi-channel surveillance technology supporting EW, Communications, SIGINT and EM-Cyber operations
- Maintain ES3701 operational ES system and Radar Test Facility, St Kilda
- ICT network capability for secure laboratory facilities
- Secure Signals Exploitation Facility

Spectrum Sensing & Shaping Major S&T Capability



Electronic Warfare Operations - Vision and Mission

Vision:

Be a world leading provider of innovative S&T in EW technologies and techniques.

Mission:

Conceive, develop and validate EW technologies and techniques to support the ADF.

Challenges and Technology Drivers:

Electronic Warfare (EW) systems face the challenge of continual improvement and diversification of threat weapon systems. With novel sensors, extensive networking and advanced processing, modern weapons present a formidable problem for the defence of ADF platforms and personnel. While it remains a priority to establish control of the electromagnetic spectrum in combat, technical advances are making this more difficult. A major contributor to the problem is the increasing complexity and adaptability of threat systems. This demands a corresponding response in EW domain, exploiting the sciences of autonomy and machine intelligence to sense and interpret the threat environment, and to respond in an effective manner with limited human supervision.

Brief Overview:

RF Electronic Attack: Current research priorities include automated processes for developing novel and robust RF countermeasure techniques. This will be enabled by using modern processing technology to create high fidelity emulations of threat systems, and employing machine intelligence techniques to identify vulnerabilities and develop countermeasures. This will increase the efficiency of countermeasure development and lay the groundwork for future cognitive EW approaches. The intent of a cognitive EW system is to assess the *intent* of threat systems and respond appropriately to enhance the *probability of mission success*. Another major research theme is to use EW to complement stealth capability, specifically by countering adversary systems designed to defeat stealthy platforms. This will require innovative approaches to defeat passive and networked radars, and systems operating in new parts of the radar spectrum.

EO Countermeasures: In the EO domain near term research will focus on high fidelity simulation to assess and validate co-ordinated countermeasure techniques, involving the use of manoeuvre, flares and directed IR countermeasure (DIRCM) systems. The current research program is directed largely to the air domain, but is expected to be extended to the land and maritime domains over the 5 year timeframe of this strategic plan. The adaptation of existing processes to the new environments will involve considerable research in the phenomenology of EO signatures and countermeasures. In addition, the shift from the UV domain to imaging IR for threat warning will involve extensive research in advanced image processing techniques to identify low signature threats in heavy clutter.

Laser Technology: Laser technology is critical to future countermeasure research. The Laser Technology group will maintain its established position as a world leader in fibre laser technology, and leverage this expertise to participate in laser countermeasure and directed energy programs in allied nations. The group will undertake research to increase the power of 2μ fibre laser technology, while also enhancing compactness, robustness and power efficiency as required for defence applications. It will develop technology to combine the beams from multiple fibre lasers for use in directed energy applications, and investigate the complex interactions between high energy pulsed and CW laser systems against various sensors and materials.

Electronic Warfare Operations Science & Technology Profile

S&T Trajectory

Invest

- Adaptive and cognitive approaches to EW
- Countermeasures for counter- LO sensors
- Synthetic approaches to CMD&V
- Novel threat estimation techniques
- Laser effects on sensors & materials
- High power lasers
- Threat warning
- Directed infra-red countermeasures
- Model-based design

Reduce

- Research & validation of “traditional” EA techniques
- EA techniques against older generation threat systems
- Focus on field trials for CMD&V
- Terminal maritime RF countermeasures
- Traditional threat analysis
- Support for stand-alone pyrotechnic CM techniques

Partnerships

Within DST Group

- Cognitive EW systems (EWO/SSS/AC)
- Passive Location Systems & CMs (NSID)
- Engagement M&S to support CMD&V (RF & EO) & IIR TW & SA (EWO/SPE, WCSD, NSID)
- Systems analysis & modelling of laser CMs (WCSD)

National

- Machine learning & mm-wave sensing (Sydney Uni)
- Adaptive Threat Sensors (CEA Technologies)
- Future Advanced Threat Simulator (Industry)

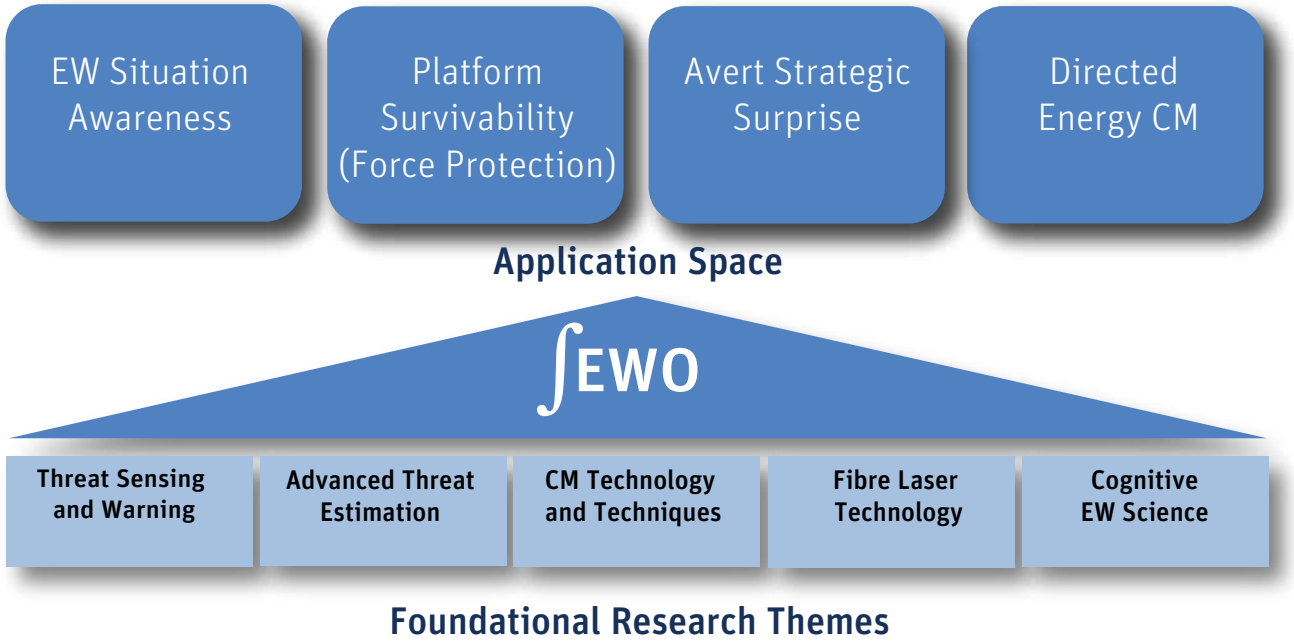
International

- Cognitive EW (DARPA, NRL, AFRL, ONR, AEA IPT)
- High power laser systems & counter-PCL (NRL)
- Lasers in the battlespace & maritime & land CMD&V (NATO)
- Burden sharing 5-eyes collaborations (TTCP, AAMOST, CI, MTEP)

Key Infrastructure Plans

- Development of a re-locatable cognitive EW laboratory
- Advanced RF EA prototyping system
- CMD&V systems to support JP 500 (with JEWOSU)
- HP laser environmental test facility

Electronic Warfare Operations Major S&T Capability



Planning and Delivering the CEWD Program

Part IV

Planning and Delivering the CEWD Program

Balanced program

The CEWD program will be a balanced mix of activities addressing the core roles – support to operations, capability development and acquisition, sustainment (ie force in being) and future proofing (longer term R&D).

In CEWD, the MSTC is regarded as the appropriate level of granularity when assessing balance. An MSTC is expected to have an appropriate mix of such activities, but within the MSTCs, STCs will have varying levels of balance as they may have more effort in some roles and less in the others.

For a given STC this setting will generally change over time, as the primary technologies being researched become more mature, and move towards Capability Project status, acquisition and ultimately used in service.

Integrated program

More substantial programs such as SRI and acquisition projects will generally have activities underway in several MSTCs, both within CEWD and across other Divisions and sites.

CEWD will aim to maximize the interaction, collaboration and integration of activities in different MSTCs and Divisions, applying multi-disciplinary S&T expertise to address Defence problems.

CEWD undertakes to live the “One DST Group” approach.

Strategic R&D

Longer term R&D is an essential part of an MSTC’s future capability to be able to deliver to the client program. Currently such work is funded from the Cyber and Future EW Strategic Research Initiatives, (SRI) and supplemented by some DCP funding through forward-looking projects such as Growler, AIR6000, AIR7000, SEA1000, SEA5000, Land400.

It will be strategically important to forecast and influence future sources of such funding in order to sustain this critical area of work. In times of budget pressure it is possible for one or more MSTCs to have little discretionary funding after essential sustainment.

In such cases CEWD will look to support R&D activity from other sources over which there is discretion within the Division. No MSTC will be left behind.

Planning and Delivering the CEWD Program

MSTC Sustainment

There is a requirement to maintain basic essentials that are the responsibility of each MSTC, such as maintaining compliant software licenses, laboratory consumables, equipment calibration, maintenance, repair and refresh of equipment and facilities, legally required training and staff development training.

CEWD will ensure these costs are transparent and correctly attributed.

Capital

It is recognised that the capital cost of refreshing critical equipment is high, and not affordable from a typical MSTC's annual budget. Accordingly CEWD will establish a 6 year rolling plan that identifies all such requirements and rotates a "capital refresh" allocation through each MSTC successively in order to keep key infrastructure up to date.

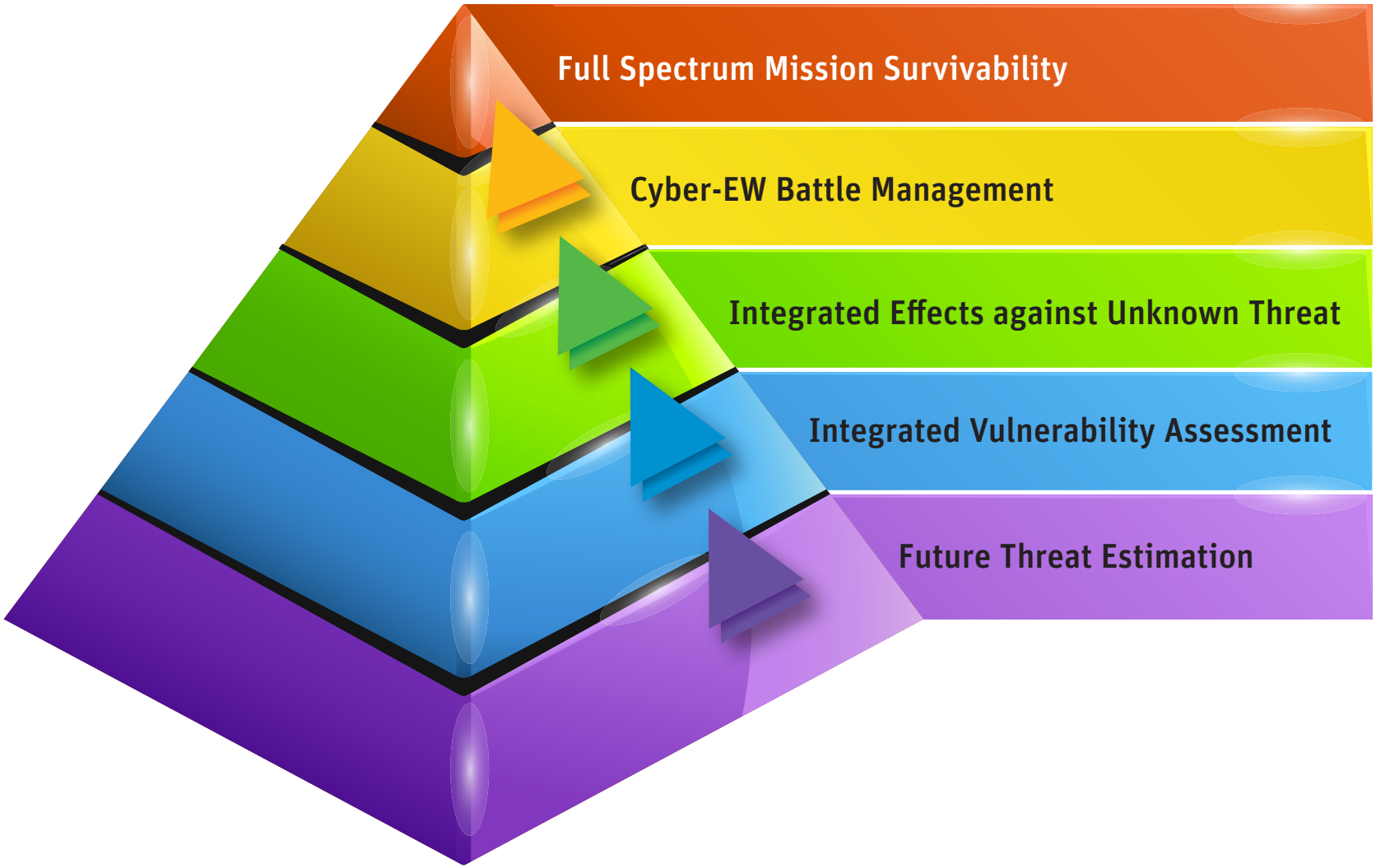
Training

In addition to the requirements and actions identified in Part V "Developing our People", there is a need to provide early career scientists with opportunities to develop their international credentials and to experience the rigours of presenting their work in a forum of internationally credible peer review. Accordingly, it is intended that each MSTC be resourced to provide access to one overseas conference of high standing for attendance by a junior staff member, on condition that the staff member has a paper accepted for presentation.

Training that is legally required in order to perform job functions will be prioritized over all other training.

Participation in technical training and development will be given priority and encouraged, and planned through the PFADS process as well as periodic staff development discussions. Identified training opportunities will be pursued in the first instance through the Secretary's training fund and then through MSTC sustainment funding.

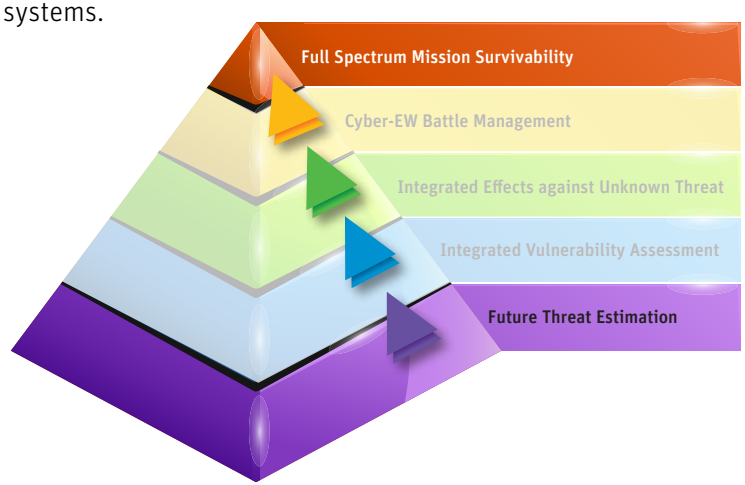
CEWD S&T Themes



CEWD S&T Themes

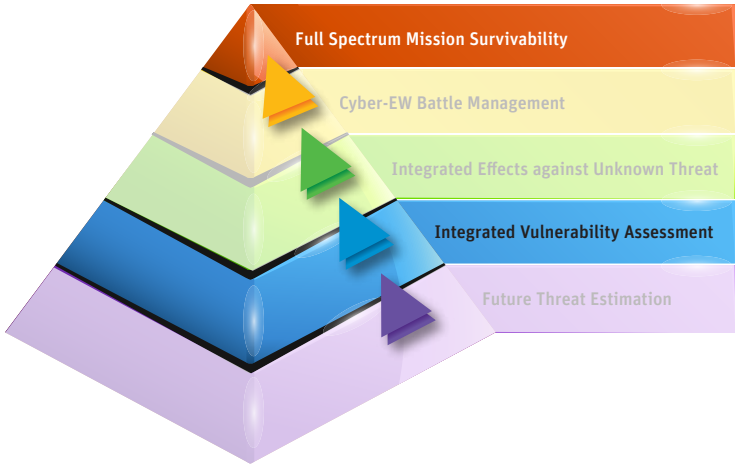
Future Threat Estimation

Understanding the threat to a mission is the initial step to achieving mission survivability. Historically threat assessment has been hardware centric, reactively assessing available threat assets. The future threat however will be predominantly software driven, with game-day characteristics and behaviours able to be changed dynamically rendering traditional threat assessment techniques less than viable. Future threat estimation will need to address this shortfall by considering science and technology trends that might impact future threat design and implementation, harnessing modelling, simulation and analysis integrated with flexible hardware surrogate development and experimentation to provide insight and understanding of potential future threats to the mission across traditional, networked, COTS derived and space-based systems.



Integrated Vulnerability Assessment

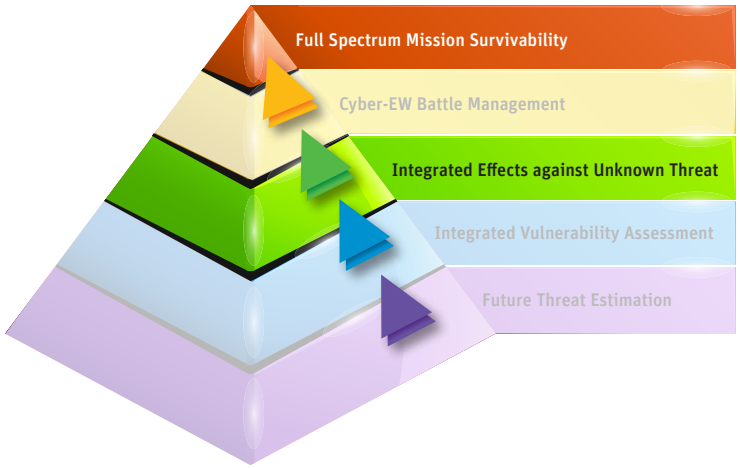
Understanding the vulnerability of the asset and mission to the future threat is the second step to achieving mission survivability. This includes assessing blue asset/system signatures that may be exploited by the threat, predicting likely attack vectors that might be utilised and identifying processes to mitigate this risk through such actions as asset/system signature management and system hardening.



CEWD S&T Themes

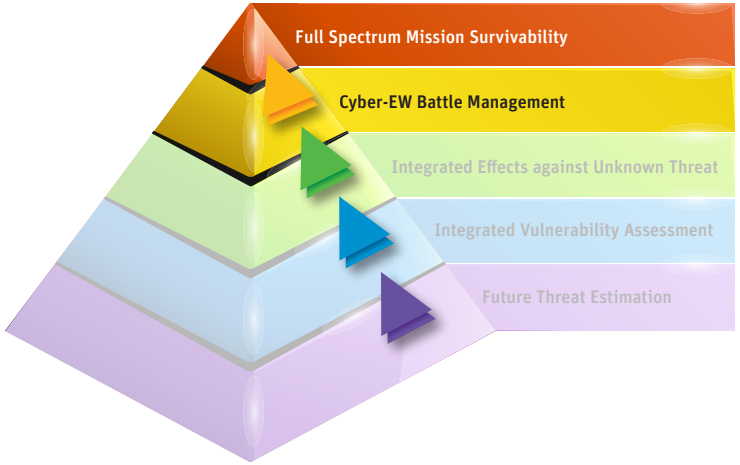
Integrated Effects against an Unknown Threat

Whilst the Future Threat Estimation sub-theme aims to provide insight into potential threats to the asset and mission, it is prudent to explore the worst case scenario where the threat is unknown and there is a requirement to prosecute the threat with the electronic capabilities available across the Cyber-EW continuum. Key to this is developing, verifying and validating both singular and integrated techniques and effects across the Cyber-EW continuum, performing battle damage assessment post prosecution, understanding the capability advantage of utilising integrated effects as distinct from the summation of singular effects and cognitively adapting integrated effects to maximise military outcomes.



Cyber-EW Battle Management

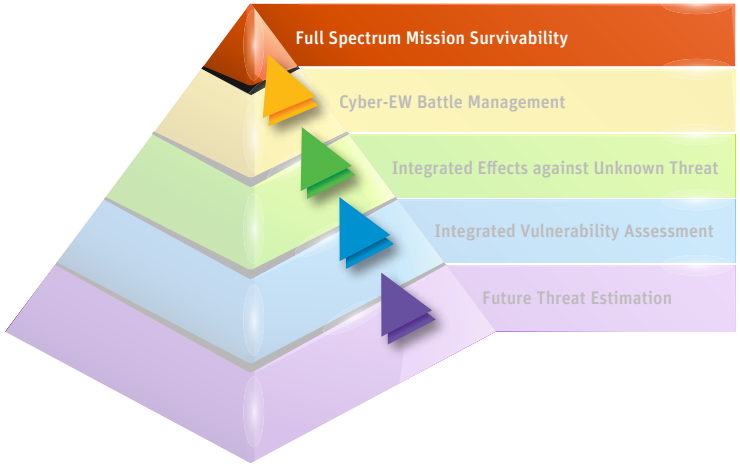
Effective electronic prosecution of a threat requires timely and responsive electronic battlespace awareness through the full sensing of the Cyber-EW continuum and the ability to efficiently coordinate and manage both centralised and distributed Cyber-EW resources for integrated electronic attack against a dynamically changing environment. This is embodied by the concept of Cyber-EW Battle Management and will include research and development of data processing, ultra-wideband signal processing, big data analytics, social influence and behaviour analysis, proactive EW, reasoning and command decision support tools.



CEWD S&T Themes

Full Spectrum Mission Survivability

Full mission survivability is an overarching theme that integrates the sub-themes identified below. Whether considering a Maritime, Air, Land or Space asset in a congested, contested and competitive environment, ensuring the survivability of not only the asset but also the mission is paramount for delivering the military response options that the ADF will want to pursue. Whilst historically both kinetic and non-kinetic threats to the asset and mission were electronically countered independently across the Cyber, Communications and EW domains, full spectrum refers to the holistic understanding and countering of the threat across the Cyber-EW continuum. Full Spectrum Mission Survivability includes research and development of sensor to effector concepts, techniques and technologies encompassing collection, exploitation and engagement of all signals across the Cyber-EW spectrum.



Developing our People

Part V

44

Principles

CEWD will have a focus on developing its people and fostering a safe, inclusive working environment. Pursuit of professional excellence, personal growth, a strong collaborative spirit, and commitment to achieving outcomes for Defence and National Security will be central to the CEWD culture. Staff development will be an on-going feature of Divisional business and will be carefully planned and resourced according to a 3-dimensional model of personal, professional, and leadership development. The senior executive management (SEM) of the Division as a team will take responsibility for nurturing and developing CEWD staff and as such will:

annually review the staff development plans;

provide resources for general and task-related WHS training

provide security guidance and training

demonstrate professional and ethical behaviours and values

support staff in taking ownership of their own professional and career development.

CEWD recognizes that development of Divisional Research Services (support) staff is as important as that of S&T staff. It is important to promote a culture that executive & support staff are an integral part of the Division's mission and ability to deliver S&T capability.

CEWD undertakes to provide appropriate development opportunities to executive and support staff, including the DST-specific courses such as SLEAD and GPSL.

In order to better acquaint executive and support staff with the technical work of the Division and its impact, a range of measures such as showcases, invitations to internal program reviews and inclusion on briefings and lab tours will be practiced.

Statements of Intent - PePLe

Personal Development

Everyone contributes to a safe, supportive, stimulating & inclusive work environment

CEWD will ensure that opportunities are made available to all levels, to create a culture of life-long learning and to actively manage talent within the Division. Development plans for all staff will be established to support career discussions between supervisors and staff members and to inform the training elements of Performance Feedback and Development (PFADS) agreements.

Professional Development

Everyone has recognised professional expertise they apply to achieving the CEWD mission

CEWD is committed to ongoing development of technical and professional skills. To assist the identification of appropriate training courses through the staff development plans, and to coordinate participation and gain any economies of scale, an online repository of relevant courses will be created, initially in CSS branch, but if successful will be expanded to CEWD as a whole.

A strategic approach to maximising benefits from the DIF program, DSTO fellowships and PhD training will be adopted, by taking a longer term view and forecasting where opportunities would potentially arise and of how they could be best taken advantage.

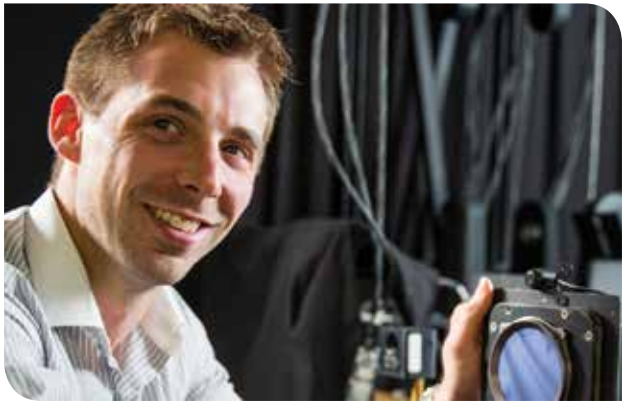
The potential for cross-fertilisation of skills by exchanges of staff between STC's will be considered. The benefits are clear but there are a number of constraints which reduce the flexibility and number of genuine opportunities.

Leadership Development

Everyone has the commitment, ability and opportunity to demonstrate leadership

Developing the future leaders of CEWD and enhancing the abilities of current leaders and managers is critical to the future health and morale of the Division. The range of development options available includes DST-specific programs, such as ISM, GPSL, SLEAD, LTTC and SLDP , and external options, such as the ADF staff college, and The Extraordinary Leader program.

Information from the staff development plans will allow the most effective use of these training options by allowing for informed consideration of requirements, balanced with availability of these programs.




SECURITY

For further information please contact:

Director S&T Program, Cyber and Electronic Warfare Division

Tel: (08) 7389 6937

Email: CEWDDirectorS&TProgr@dsto.defence.gov.au

Web: http://www.dst.defence.gov.au/