



Australian Government

Department of Defence  
Science and Technology

UNCLASSIFIED

Approved for Public Release

# Cyber and Electronic Warfare Division DST Partnerships Week 2016

*Science and technology to understand and counter the threat using electronic means*

Connect, Partner,  
Collaborate, Innovate

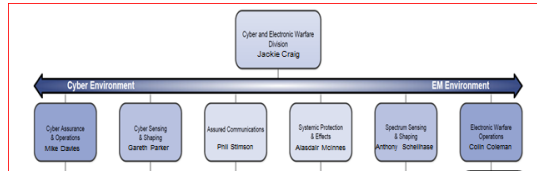
**DST**  
GROUP

Science and Technology for Safeguarding Australia

# Cyber & Electronic Warfare Division

*Mission: To understand and mitigate threats using electronic means*

## Major S&T Capabilities



- The Cyber-EW Continuum is the convergence of cyber, SIGINT, communications and EW.
- In accordance with national priorities outlined in the Next Generation Technologies (White paper), the Cyber Security Strategy, and increasing requirements from the ADF for cyber S&T, CEWD develops and applies technologies across the cyber-EW continuum to address threats in a data-driven, networked, cyber-physical future

## Program

- Strategic Research programs in both Cyber and Future EW, plus others under development), within the DST Strategic Research Initiatives program
- Support for the Defence IIP (Integrated Investment Program, formerly DCP) in transitioning technology developments to capability
- CEWD leverages our internal capability via strong international partnerships, including TTCP and bilateral agreements with other nations
- CEWD has an extensive history of collaboration with academia and Defence industry, and creates opportunities for future collaborative developments

## Partnership examples

- Data 61/CSIRO – trustworthy cyber (software)
- UNI NSW – trustworthy cyber (hardware)
- Northrup Grumman – Digital Video Guard (DVG) and EO Distributed Aperture System (EODAS)
- Ultra Avalon – RF sensing and analysis

## S&T highlights

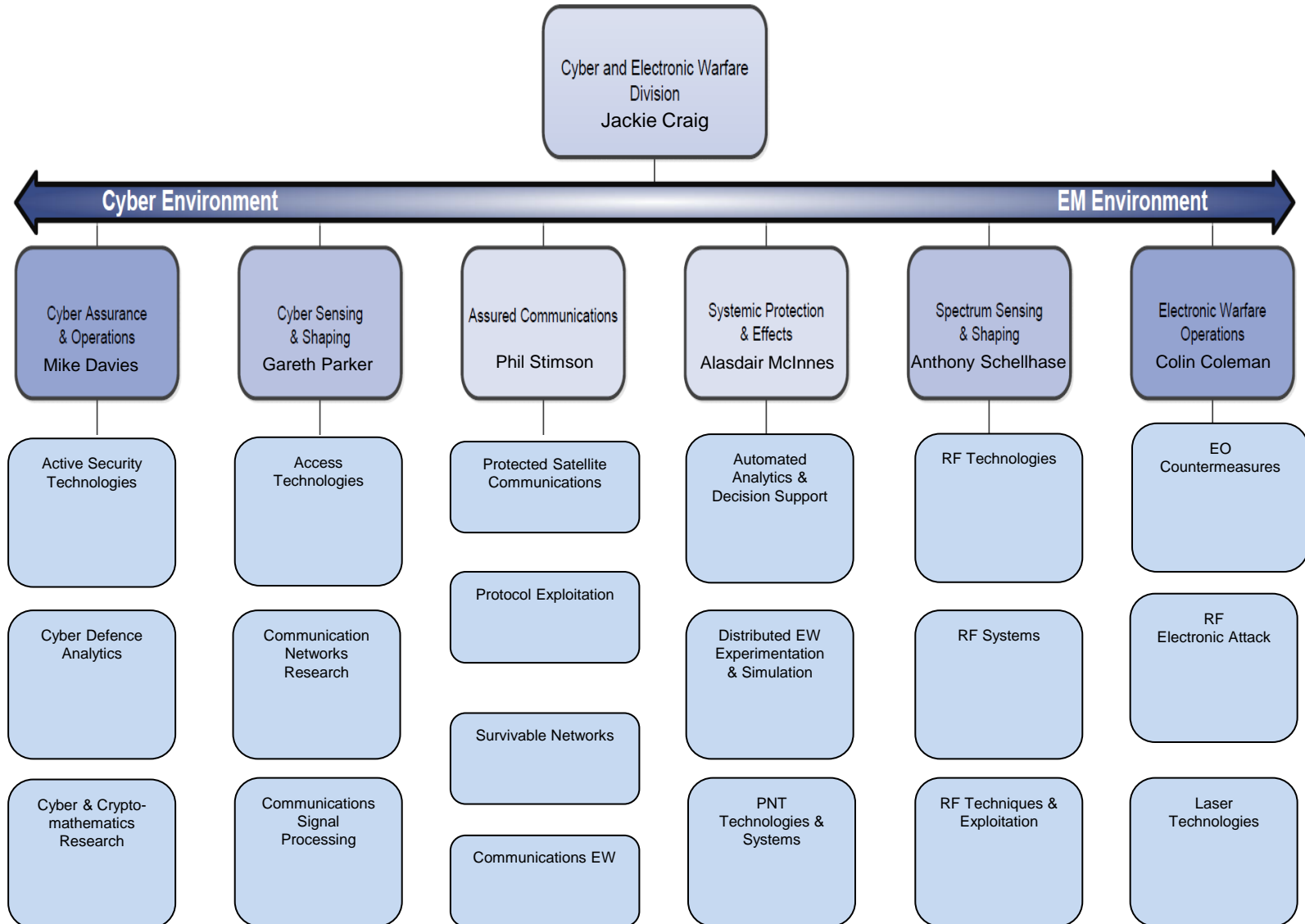
- Digital Video Guard (DVG)
- Wideband Global SATCOM Anchoring Monitoring System
- Redwing Program
- LIVE Maritime Situational Awareness
- DIRCM world leading laser research

## Opportunities to partner with CEWD

- **Hinder** – *Autonomous cyber defence*
- **SCADS** – Self-organising Communications and Autonomous Delivery Service  
*UAV-based resilient communications*
- **EODAS** – Electro-optic Distributed Aperture System  
*Airborne platform 360 degree threat sensing*

# Cyber and Electronic Warfare Division

## Structure





Australian Government

Department of Defence  
Science and Technology

UNCLASSIFIED

Approved for Public Release

# Cyber Assurance and Operations MSTC

*To enable autonomous, resilient and effective cyber capabilities with an operational edge*

Connect, Partner,  
Collaborate, Innovate

Dr Mike Davies

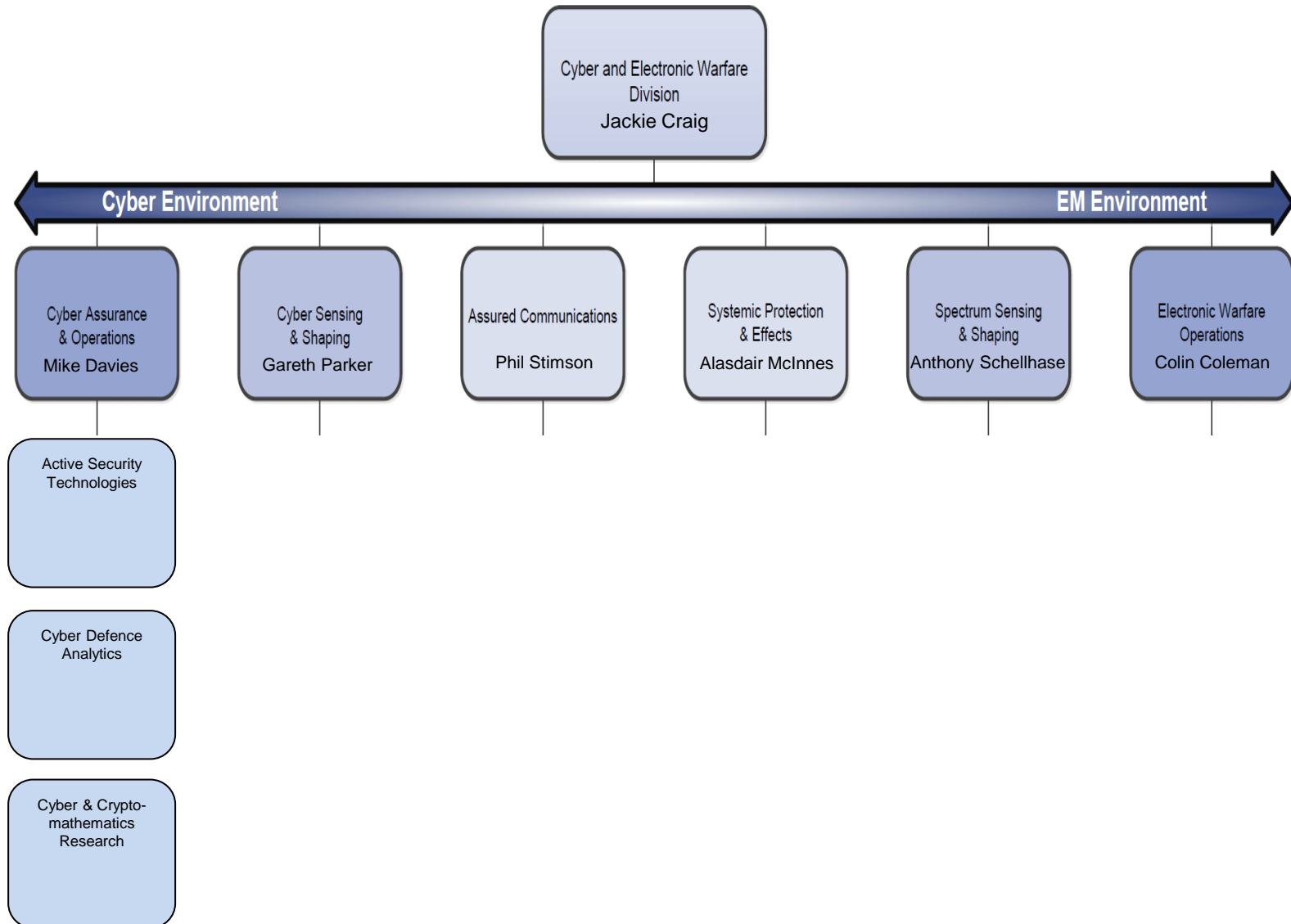
Research Leader

[michael.davies@dsto.defence.gov.au](mailto:michael.davies@dsto.defence.gov.au)

**DST**  
GROUP

Science and Technology for Safeguarding Australia

# Cyber and Electronic Warfare Division Structure



# Introduction

## Cyber Security Dilemma

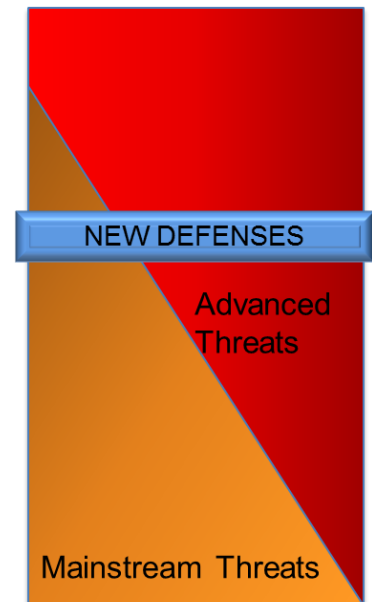
Defenders are losing (or at best playing catch-up), attackers are winning (or at least calling the shots)



We develop new measures through advancing our concepts, tools and techniques

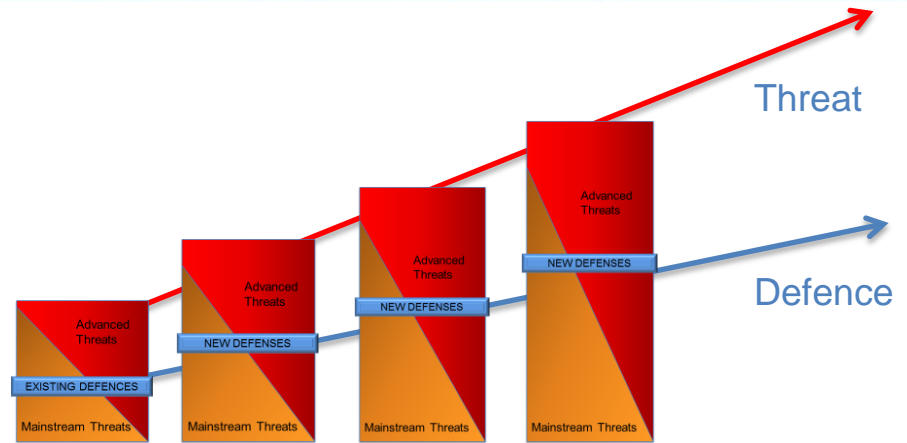


But then, however, so do the threat actors!

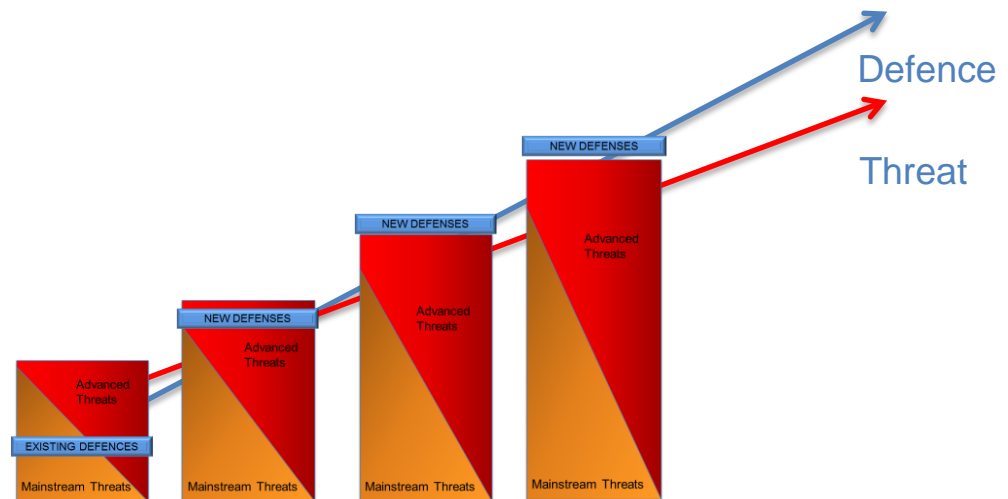


# A Challenge

How can we decrease the chance of just making incremental improvements which get outpaced?

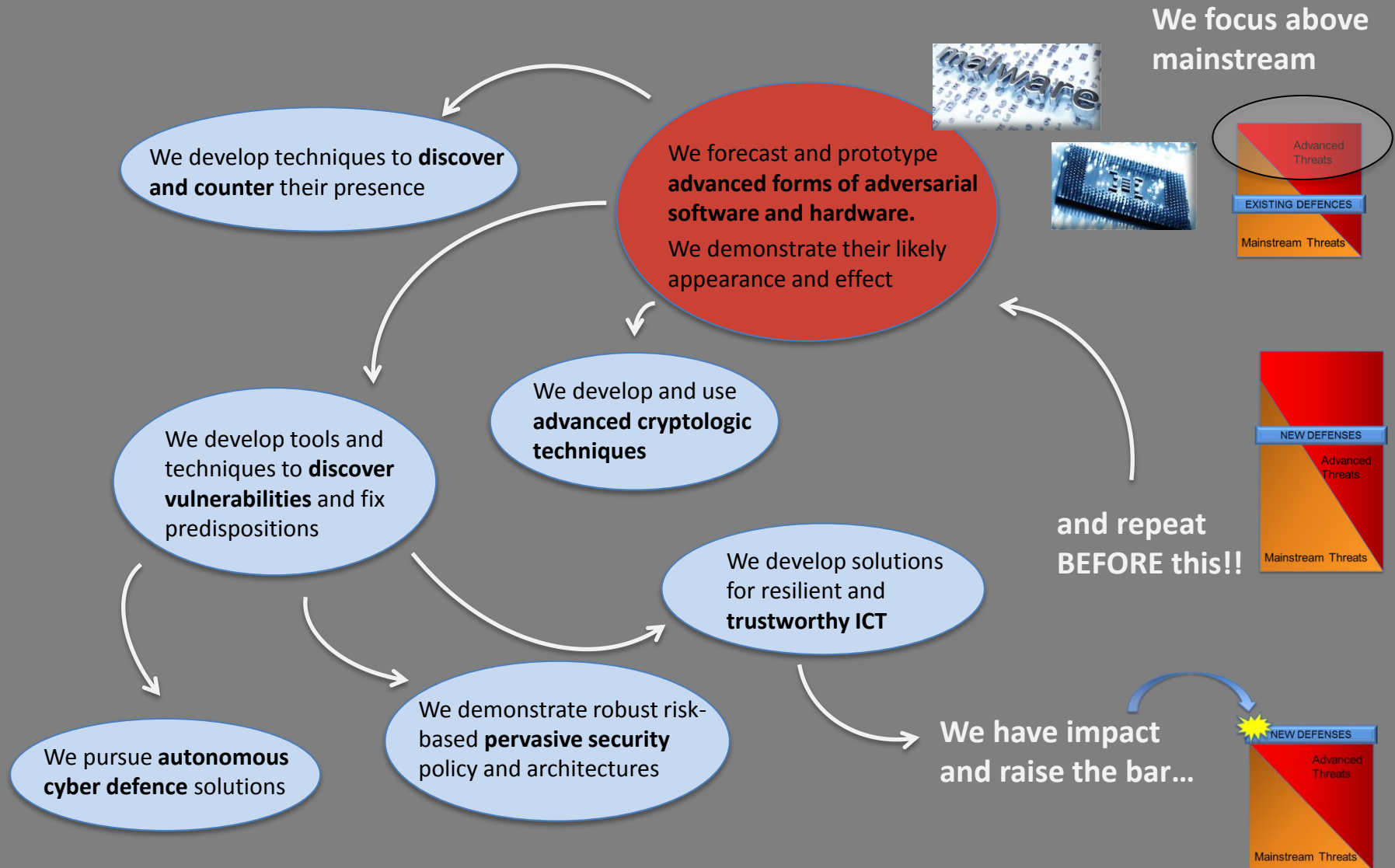


And increase the chance of producing a sustainable game-changer?



What qualities do we need from the Australian R&D community?...

# Modus Operandi in DST Group Cyber Assurance and Operations S&T





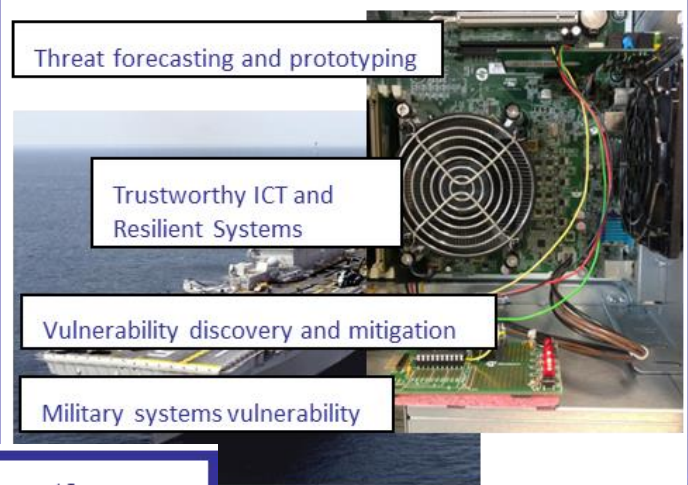
# DST Cyber Assurance and Operations Branch

*A critical enabler of effective cyber operations and resilient trustworthy systems*

## Cyber Defence Analytics



## Active Security Technologies



## Cyber- & Crypto- Mathematics Research



# Connect, Partner, Collaborate, Innovate

**DST**  
GROUP

## External Engagement: DST CYBER DEFENCE AND SECURITY R&D

May 2016

### RECENT HIGHLIGHTS

Apr 16: Led inaugural research stream at Australian Cyber Security Centre (ACSC) Conference

Dec 15: Invited keynote presentation at Edith Cowan University Security Congress

Nov 15: Invited presentation and panel member at GovInnovate, delivered with Data61

Nov 15: Collective briefings to/from Victorian academia through Defence Science Institute

Nov 15: Joint DST/ACCS Conference *Redefining R&D Needs for Australian Cyber Security*

Oct 15: Invited keynote presentation at Federation University *Malware Reverse Engineering* conference

Aug 15: Invited keynote address and panel member at Criterion Building *Cyber Resilience* conference

June 15: Invited presentation at Australian Defence Magazine Cyber Security Summit

Academia

Industry

Government R&D

DATA 61

**Data61 / CSIRO**  
Strategic research alliance; trustworthy ICT



**Cyber Security Growth Centre**  
Will support R&D prioritization, coordination and delivery



**AISA Aus Information Security Assoc**  
Exploring collective industry engagement



**CISCO**  
Discussing strategic alliance; trials with operational data



**Boeing Defence Aus**  
Exploring collaboration in trustworthy military systems



**SAAB**  
Strategic R&D Alliance in maritime systems



**Northrop Grumman**  
Licensed technology to support government trial



**Defence Science Institute**  
Collective engagement of academia and industry



**Federation University**  
Malware reverse engineering, research advisory committee



**Macquarie University**  
Malware analysis, autonomic computing



**Edith Cowan University**  
Strategic research alliance



**University of Adelaide**  
Collaboration in human aspects of cyber security



**Australian National Uni**  
Crypto-mathematics, National Mathematics Summer School, STEM outreach to schools



**Australian Centre for Cyber Security (ACCS)**  
Advisory committee member



**Deakin University**  
Co-supervising students in data analytics



**US Dept of Homeland Security**  
Australian PREDICT/IMPACT data authority, cyber physical systems security

**TTCP**

**AUS/CA/NZ/UK/US Defence S&T**  
Trustworthy systems, infosec, autonomous cyber defence



**US Defense: OSD/PACOM/MITLL/NRL**  
Mission assurance under cyber attack

**[dstl]**

**UK Defence S&T Laboratory**  
Collaboration in trustworthy systems



Trustworthy and Resilient Systems



Autonomous Cyber Capabilities



Crypto-mathematics



Vulnerability Discovery & Mitigation



Advanced Malware Analysis



Mission Assurance Analytics



Human and Social Factors

Contact: Dr Mike Davies, Research Leader, Cyber Assurance and Operations [michael.davies@dsto.defence.gov.au](mailto:michael.davies@dsto.defence.gov.au)





Australian Government

Department of Defence  
Science and Technology

UNCLASSIFIED

Approved for Public Release

# Cyber Sensing and Shaping MSTC

*Sensing and shaping of communication networks for Cyber*

Connect, Partner,  
Collaborate, Innovate

Dr Gareth Parker

Research Leader

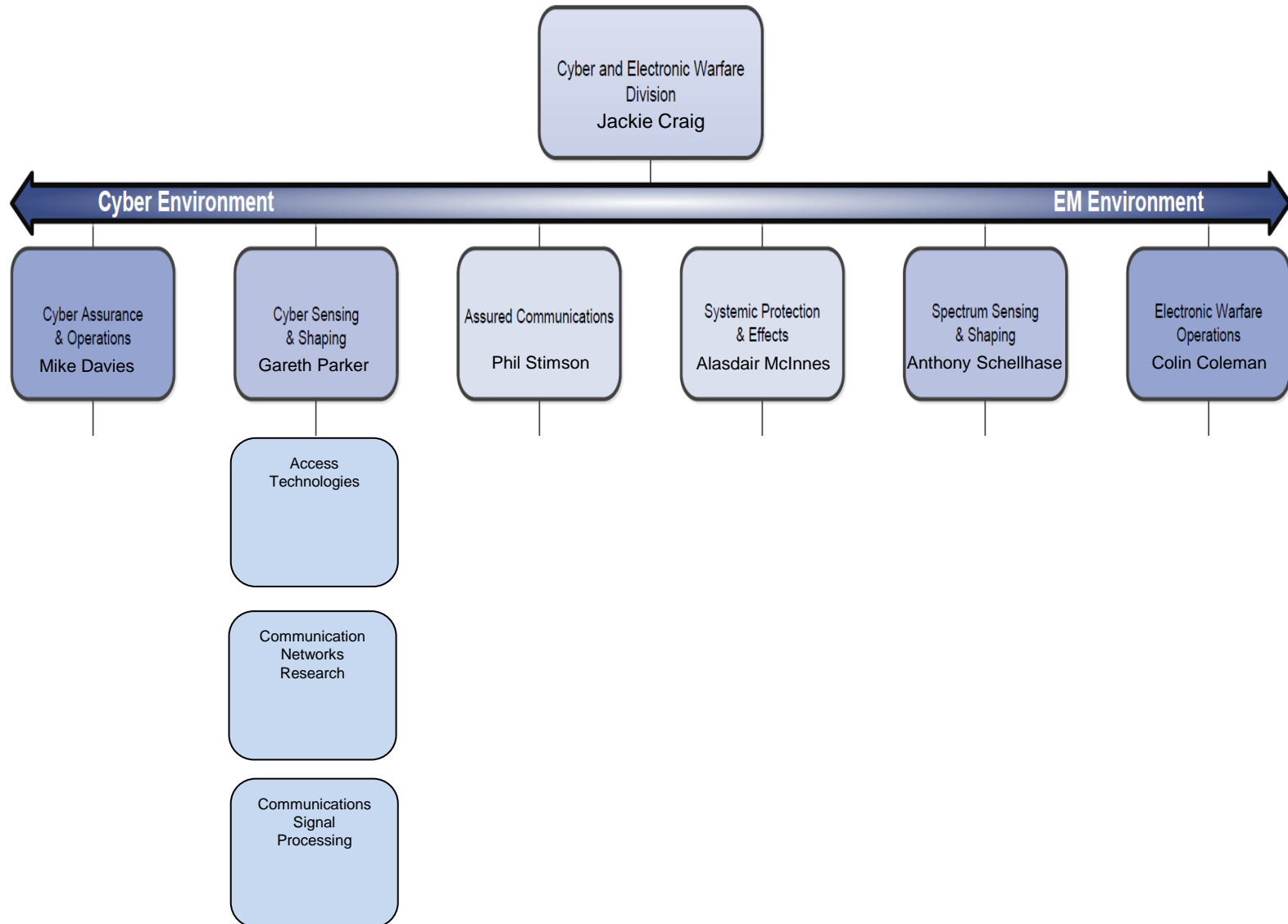
[gareth.parker@dsto.defence.gov.au](mailto:gareth.parker@dsto.defence.gov.au)

**DST**  
GROUP

Science and Technology for Safeguarding Australia



# Cyber and Electronic Warfare Division Structure



# Cyber Sensing and Shaping MSTC

*“Sensing & shaping of communication networks for Cyber”*

## Context

- Convergence of telecommunications and the internet
- Ubiquitous connectivity, mobile devices and the IOT
- Computers are connected via networks

## S&T scope: Communication networks

- Network characterisation & knowledge representation
- Network structures, protocols and behaviours
- Vulnerability discovery and treatment
- Communications technologies

## Domain: Intelligence and security



## Core knowledge and skills

- Telecommunications and internet architectures & protocols
- Communications and information theory
- Signal processing
- Data sciences
- Communications technologies – RF, digital systems, SDR, photonics

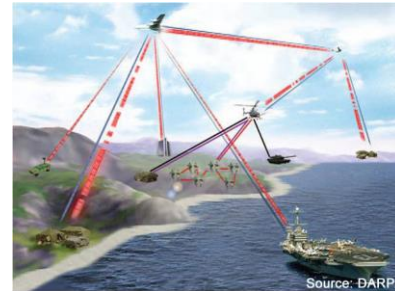
# Access Technologies

*“Technologies for cyber access and tailored communications”*

Group Leader: Mr Jon Arnold

## Bespoke wireless communications

- High data rate: mm-wave, FSOC
- Low probability of detection waveforms



## RF & photonic technologies

- Wearable and other specialised antennas and RF
- Size, weight and power constrained technologies
- Reconfigurable modem capabilities

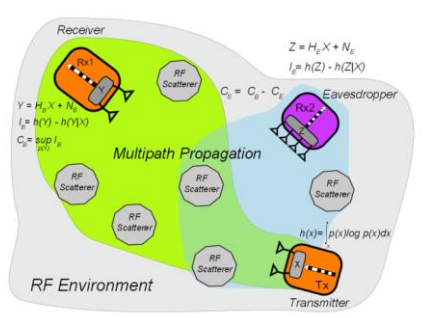
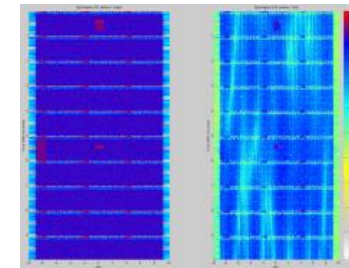
# Communications Signal Processing

*“Physical and cross-layer processing of wireless networks”*

Group Leader: Dr Jeff McCarthy

## Signals analysis

- Signal collection, enhancement and geolocation



## Waveform security

- MIMO, multichannel and diversity techniques

## Software defined radio solutions



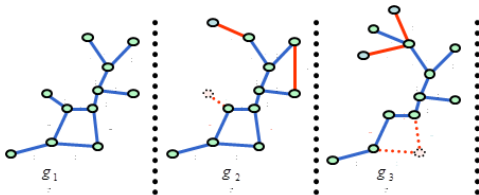
# Communication Networks Research

*“Telecommunications core networks and the internet”*

Group Leader: Dr Peter Dickinson

## Characterisation

- Topology, traffic flow, and temporal aspects



## Network knowledge representation

- Modelling and analysis of global multilayered communications networks

## Network vulnerabilities

- Understanding how routing protocol vulnerabilities can be exploited by an adversary
- Techniques and technologies for detection, protection and mitigation



## Specific Areas for Collaboration

# Body Worn Antennas and RF

## Aim

To develop new technologies for efficient antennas and RF that are safe for body worn applications in future tactical communications

## Current collaborations

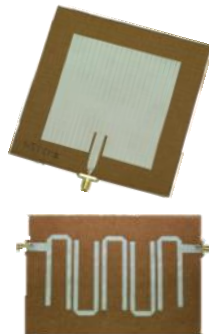
- University of Adelaide (via PhD research of Deshan Govender)
- CSIRO – battery technology & conducting fabrics

## Areas for expanded collaboration

- Mobile power technologies
- Flexible materials for RF and DC power distribution and antennas

## Our approach

- Fabric antennas
- ‘Metamaterials’
- Printed structures



## Contacts

Mr Adrian Caldow

[Adrian.caldow@dsto.defence.gov.au](mailto:Adrian.caldow@dsto.defence.gov.au)

(08) 7389 5861

# Wireless Security

## Aim

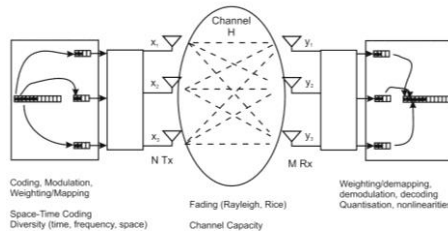
To explore vulnerabilities in wireless communications systems and develop physical layer approaches to enhancing security

## Areas for expanded collaboration

- Wireless network characterisation
- Cross-layer approaches
- Wireless sensor networks security

## Our approach

- Physical layer – LPD, MIMO, diversity



## Contacts

Dr John Kitchen

[john.kitchen@dsto.defence.gov.au](mailto:john.kitchen@dsto.defence.gov.au)

(08) 7389 6431

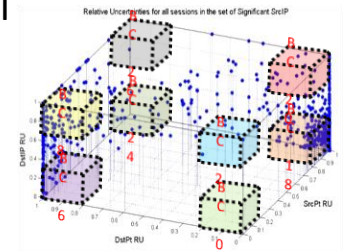
# Internet Traffic Profiling

## Aim

- Categorise high rate traffic
- Blind change and abnormality detection

## Areas for expanded collaboration

- Data science for network analysis
- Summarising bulk historical network data
- Algorithm development for distributed processing



## Our approach

- Characterisation of summarised data (i.e. NetFlow)
- Statistical and machine learning techniques to mathematically enhanced protocol-based network knowledge

## Contacts

Mr Darren Webb

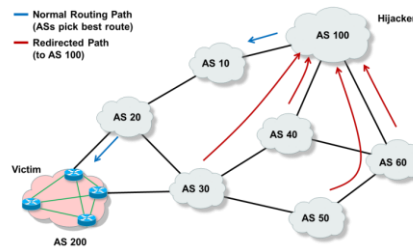
[darren.webb@dsto.defence.gov.au](mailto:darren.webb@dsto.defence.gov.au)

(08) 7389 4132

# Routing Security

## Aim

Secure critical infrastructure by protecting the internet control plane



## Current collaboration

US Dept Homeland security

## Areas for expanded collaboration

- Investigate the utility of route monitors to protect paths and network reachability.

## Our approach

- Assess threats using emulated models of computer networks
- Investigate effectiveness of emerging security measures

## Contacts

Mr Chris Wiren

[chris.wiren@dsto.defence.gov.au](mailto:chris.wiren@dsto.defence.gov.au)

(08) 7389 6572

# Network Emulation

## Aim

Develop sophisticated emulations of computer networks with a specific focus on the control plane (i.e. network routing)

## Areas for expanded collaboration

- Emulation of networks at scale
- Extension of emulator capability
- Develop traffic models that can be used to inject traffic into emulation

## Our approach

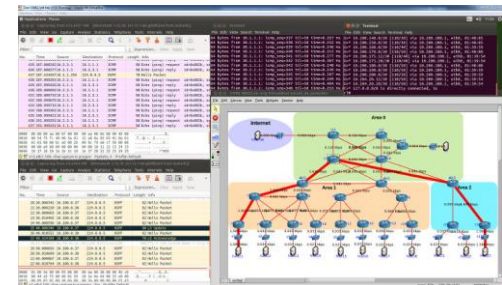
- Utilise the Common Open Source Research Emulator (CORE)
- Emulate networks of interest such as enterprise networks

## Contacts

Mr Shaun Voigt

[shaun.voigt@dsto.defence.gov.au](mailto:shaun.voigt@dsto.defence.gov.au)

(08) 7389 7527



# Emerging Communications Technologies

## Aim

Investigate future communications technologies that are likely to have a significant impact on Defence and National Security.

## Areas for expanded collaboration

- Software Defined Networking
- The Internet of Things
- Name data networking



## Our approach

Engage in regular technical exchanges with academia, and industry in areas of mutual interest.

## Contacts

Peter Dickinson

[Peter.dickinson@dsto.defence.gov.au](mailto:Peter.dickinson@dsto.defence.gov.au)

(08) 7389 6158





Australian Government

Department of Defence  
Science and Technology

UNCLASSIFIED

Approved for Public Release

# Assured Communications MSTC

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

Connect, Partner,  
Collaborate, Innovate

Philip Stimson  
Research Leader

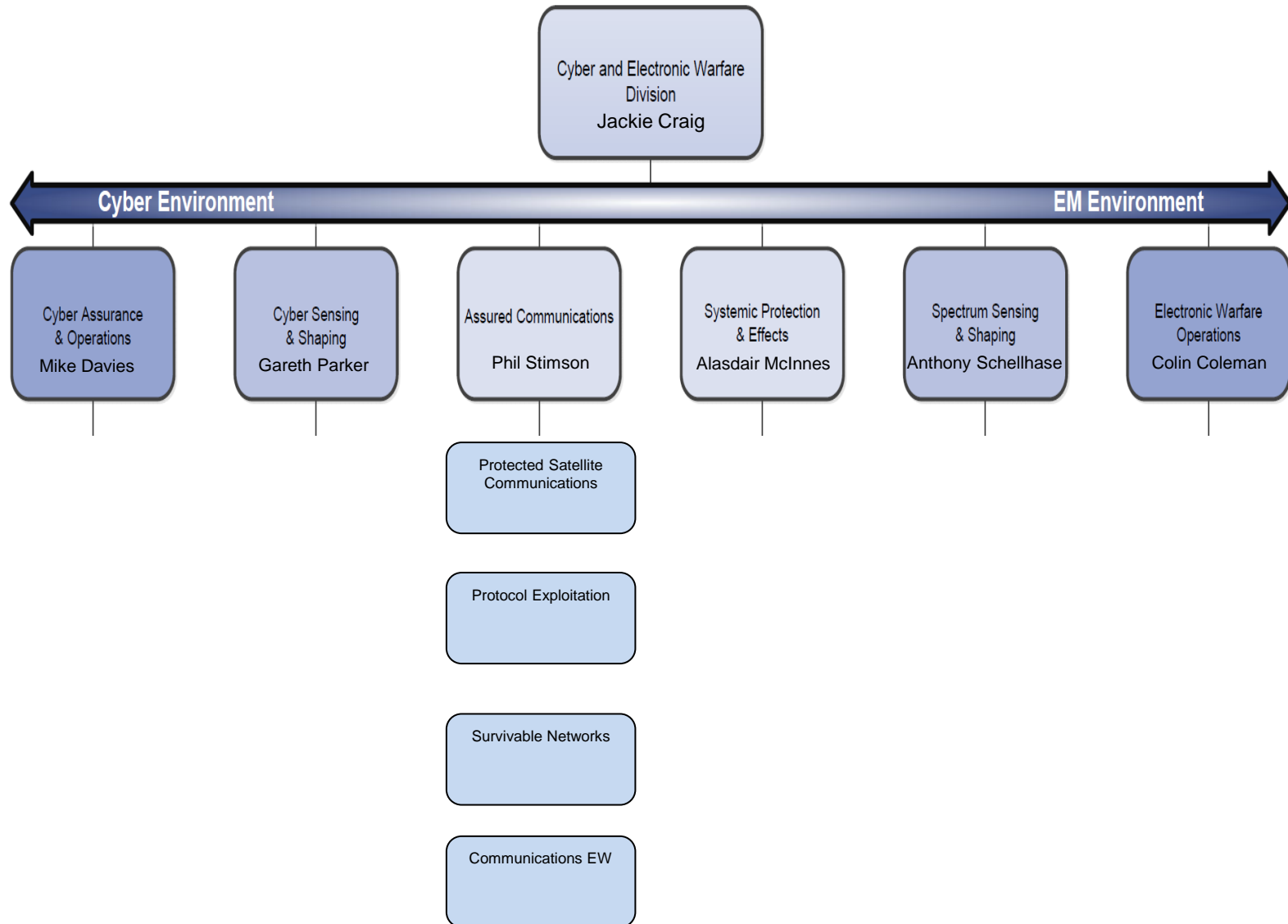
[philip.stimson@dsto.defence.gov.au](mailto:philip.stimson@dsto.defence.gov.au)

**DST**  
GROUP

Science and Technology for Safeguarding Australia



# Cyber and Electronic Warfare Division Structure



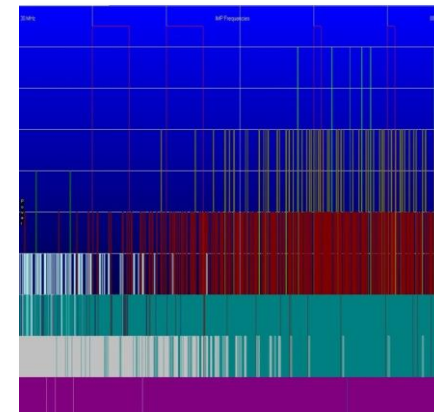
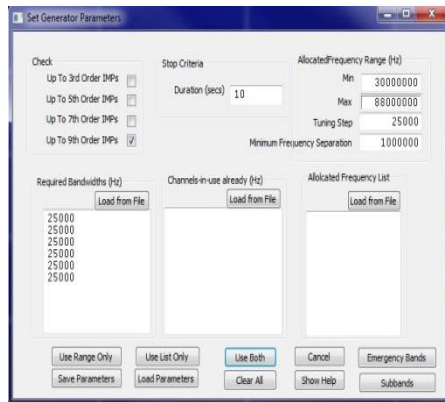
# Background

- Current ADF communications capability needs evolution.
- Threats to communications are increasing and evolving with time.
- Focus needs to be on operating in complex & dynamic behaviours.
- Commercial solutions do not offer the full capability.
- Collaboration with Allies is mutually beneficial and agreements call for enhanced mutual reliance. A substantial contribution from Australia is needed.
- Research in future protected military communications is required.

*We need to develop survivable tactical communications and electronic warfare solutions for contested and denied cyber electromagnetic environments*

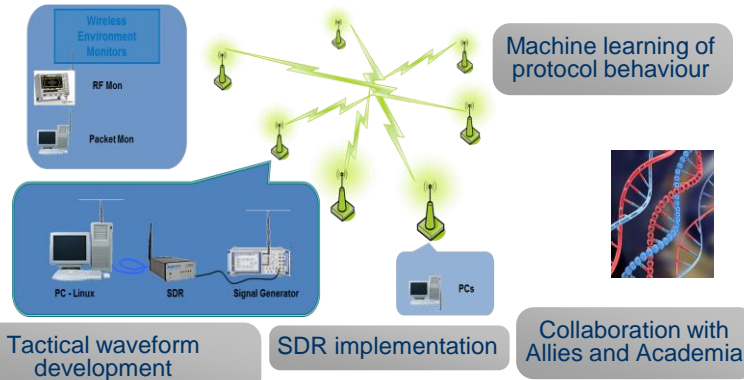
# Challenges

- Spectrum congestion
- Anti-satellite weapons
- Autonomous systems
- Software defined radios make it easy to create dynamic, zero-day, threats
- Widely available COTS electronics can now challenge MILSPEC systems



# Protocol Exploitation

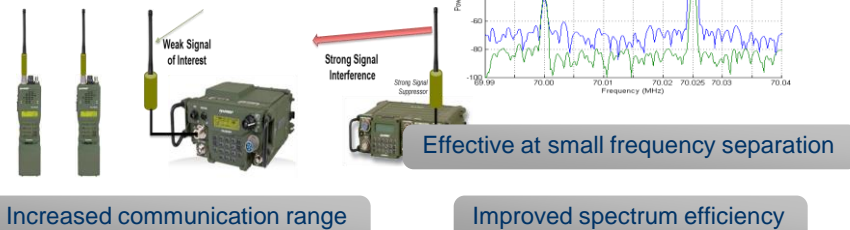
## Radio Network Protocols



## Interference Suppression Technology

Large suppression of strong interfering signals

Small impact on wanted signal



## Frequency Management

Minimise intermodulation interference

ClearView

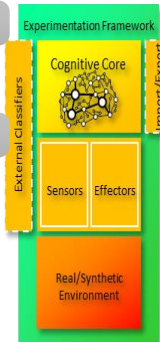


## Cognitive Networking

Network command & control

Learn, predict, respond

Increased resilience of tactical networks



## Support to Acquisition Projects

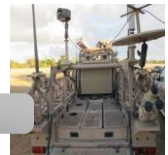
LAND 2072

LAND 400

SEA 1442

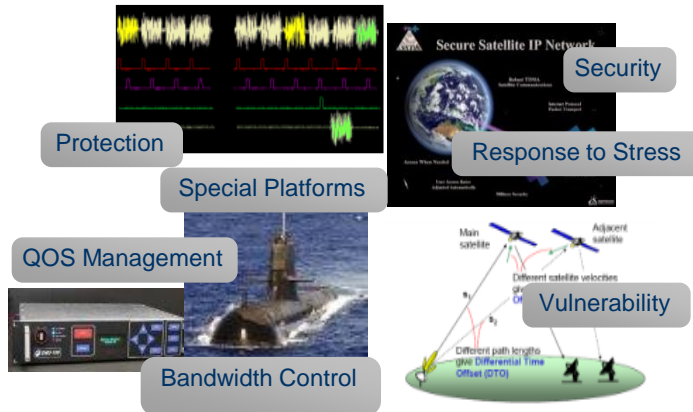
AIR 5397

JP 2097

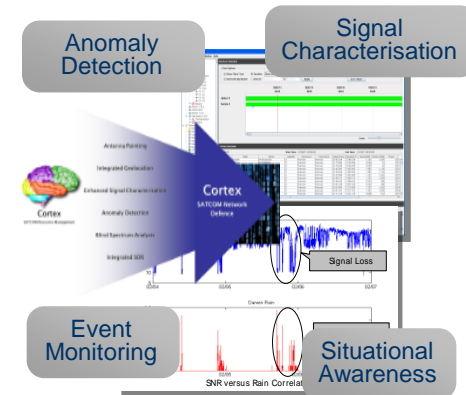


# Protected Satellite Communications

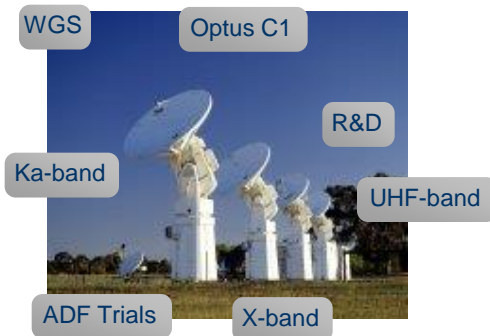
## Specialist SATCOM Waveforms



## SATCOM Network Defence



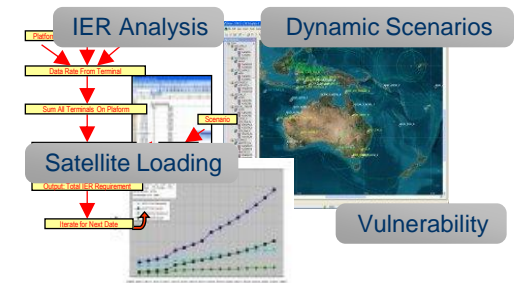
## DSTO SATCOM Facility



## Support to Acquisition Projects



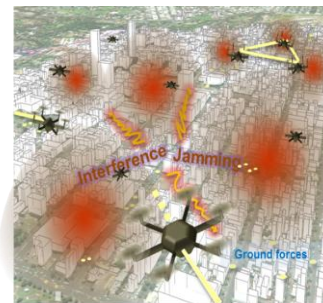
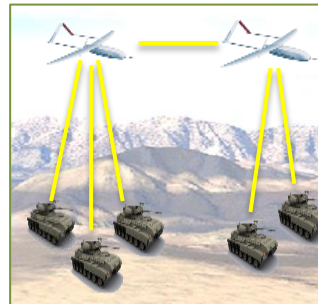
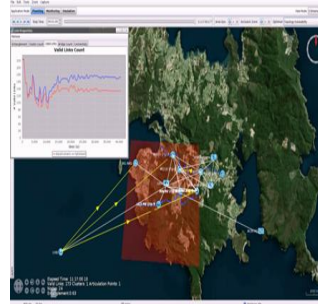
## SATCOM Modelling & Simulation





# Survivable Networks

- **HARLEQUIN** – optimisation planning tool for tactical networks
  - Research completed
  - Interested in commercialisation
  
- **OPAL** – distributed tool to support tactical networks during operations (end-to-end connectivity possible to maintain)
  - Research well advanced
  
- **SCADS** – distributed tool to support tactical networks during operations (end-to-end connectivity NOT possible to maintain)
  - Survivable Communications and Autonomous Delivery Service
  - Research recently started



# Electronic Countermeasures Development

- The ADF and OGAs operating in current operational theatres face extremely high level threats from Improvised Explosive Devices (IEDs)
  - Rely on a suite of counter IED systems to reduce their vulnerability.
  - e.g. Force Protection Electronic Counter Measures (FPECM)
- CEWD operates a world leading FPECM Countermeasures Development & Validation (CMD&V) program focussing on:
  - In-depth IED threat characterisation
  - Countermeasure technique development
  - Countermeasure device development
  - Hardware-in-the-loop validation testing
  - Over-the-air testing



*CMD&V  
Automated  
Test Benches*



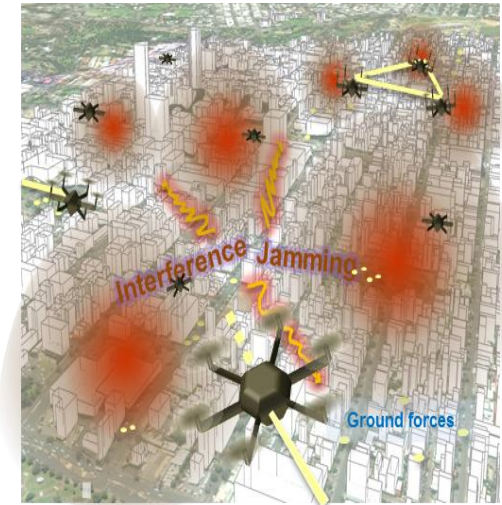
*Over-the-Air  
Trials*

- ***Directly Supporting Operations:***
  - ADF Theatres
  - Domestic Engagements

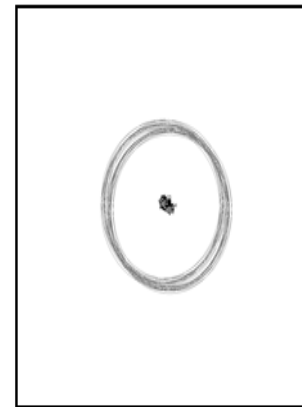
# Display - SCADS

- Survivable Communications and Autonomous Delivery System
- Self Organisation of multiple UVs to facilitate radio communications in a highly contested/denied RF environments
  - Currently, focus on UAVs
- Data ferrying
- Minimal to no communications required to achieve complex movement patterns

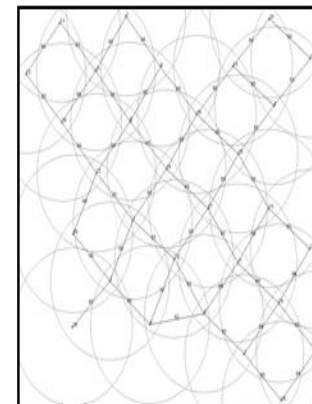
*Data ferrying UAV in an urban environment*



*Data ferrying nodes applying a simple local rule*



*Resulting emergent behaviour*







Australian Government

Department of Defence

Science and Technology

UNCLASSIFIED

Approved for Public Release

# Systemic Protection & Effects MSTC

*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*

Connect, Partner,  
Collaborate, Innovate

Alasdair McInnes

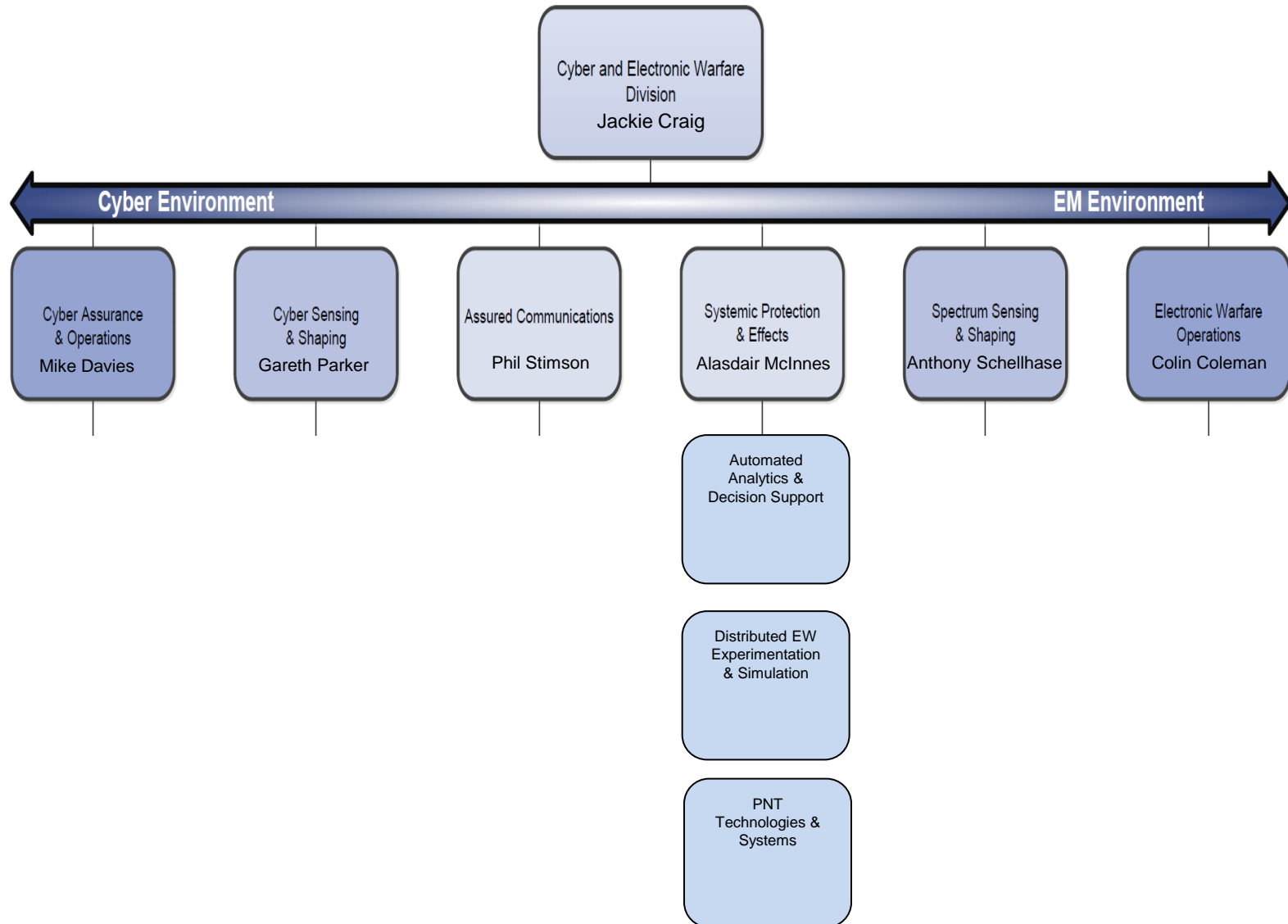
Research Leader

[alasdair.mcinnnes@dsto.defence.gov.au](mailto:alasdair.mcinnnes@dsto.defence.gov.au)

**DST**  
GROUP

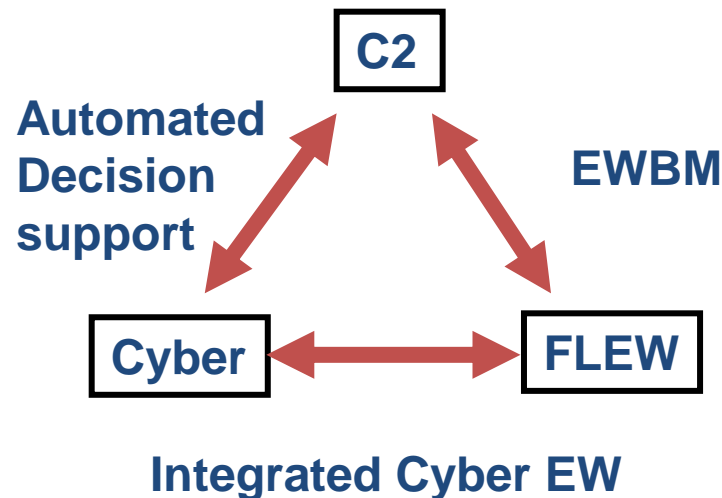
Science and Technology for Safeguarding Australia

# Cyber and Electronic Warfare Division Structure



## SPE Mission

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



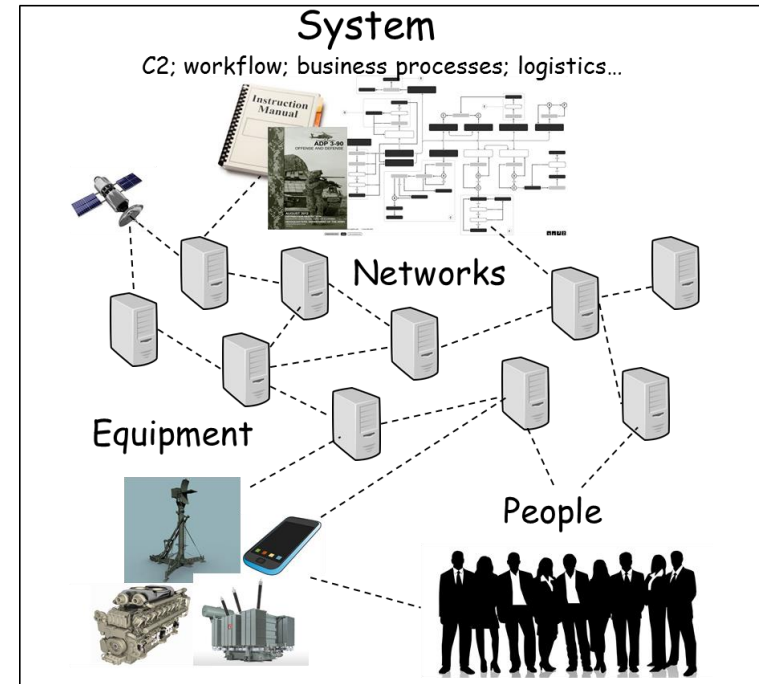
# Automated Analytics & Decision Support Group

## ■ Primary Impact Domains

- Military Platform Survivability
- Mission Assurance
- Critical Infrastructure Protection

## ■ S&T Focus Areas

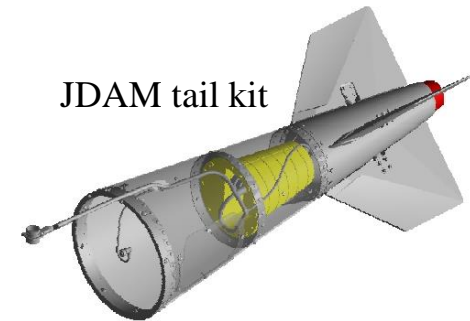
- Situational Awareness
- Threat Analytics
- Process Modelling & Mining
- Automated Reasoning, Planning & Execution
- Autonomous & Intelligent Systems



# Positioning Navigation and Timekeeping Technologies & Systems group major activities

## ■ Primary Impact domains

- Operate in GPS-denied conditions
- Deny satellite navigation to adversaries
- Alternative PNT technologies



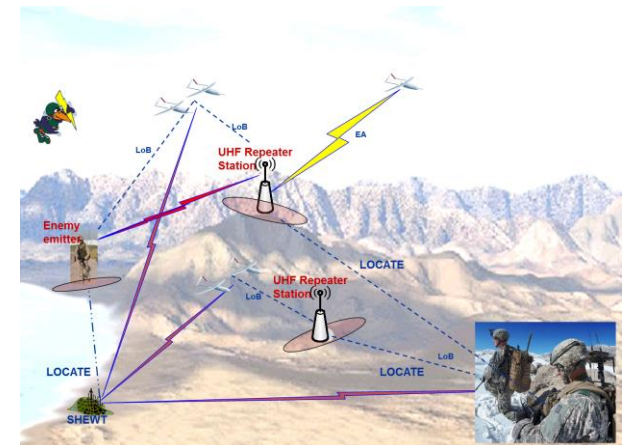
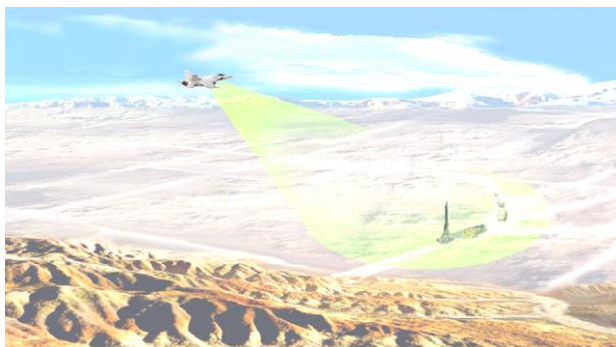
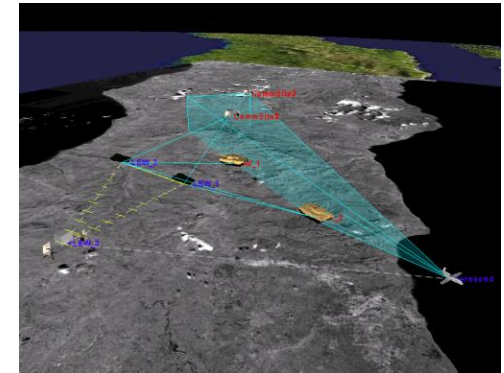
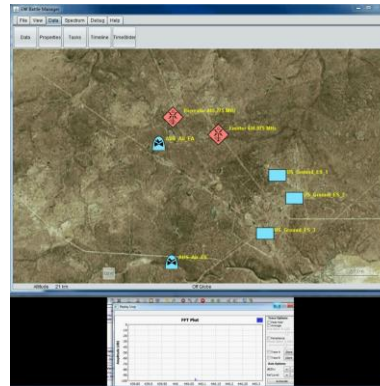
## ■ S&T focus areas

- International collaboration
- Anti-jam technologies & techniques
- Novel denial techniques
- Future technologies for accurate, stable timing



# Distributed EW Experimentation & Systems group main activities

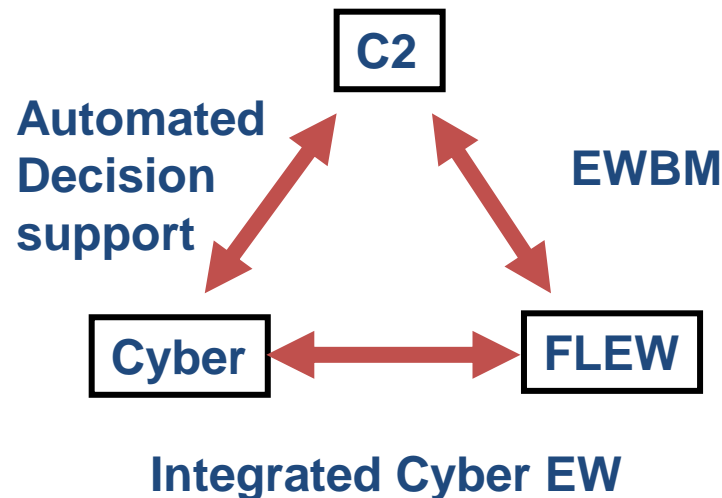
- Modelling, Simulation & Analysis
  - Force Level EW Synthetic Environment
  - Detailed Threat Modelling
- Experimentation
  - EW Battle Management
  - Shared EW Testbed
  - Tactical Networks
- Co-development
  - Advanced Passive Surveillance Capability
  - Geolocation





## Summary

- SPE branch is focused on force-level EW & cyber
- Developing and testing effective C2 tools & techniques





Australian Government

Department of Defence  
Science and Technology

UNCLASSIFIED

Approved for Public Release

# Spectrum Sensing and Shaping MSTC

*Sensing and shaping the RF Electromagnetic Spectrum*

Connect, Partner,  
Collaborate, Innovate

Dr Anthony Schellhase

Research Leader

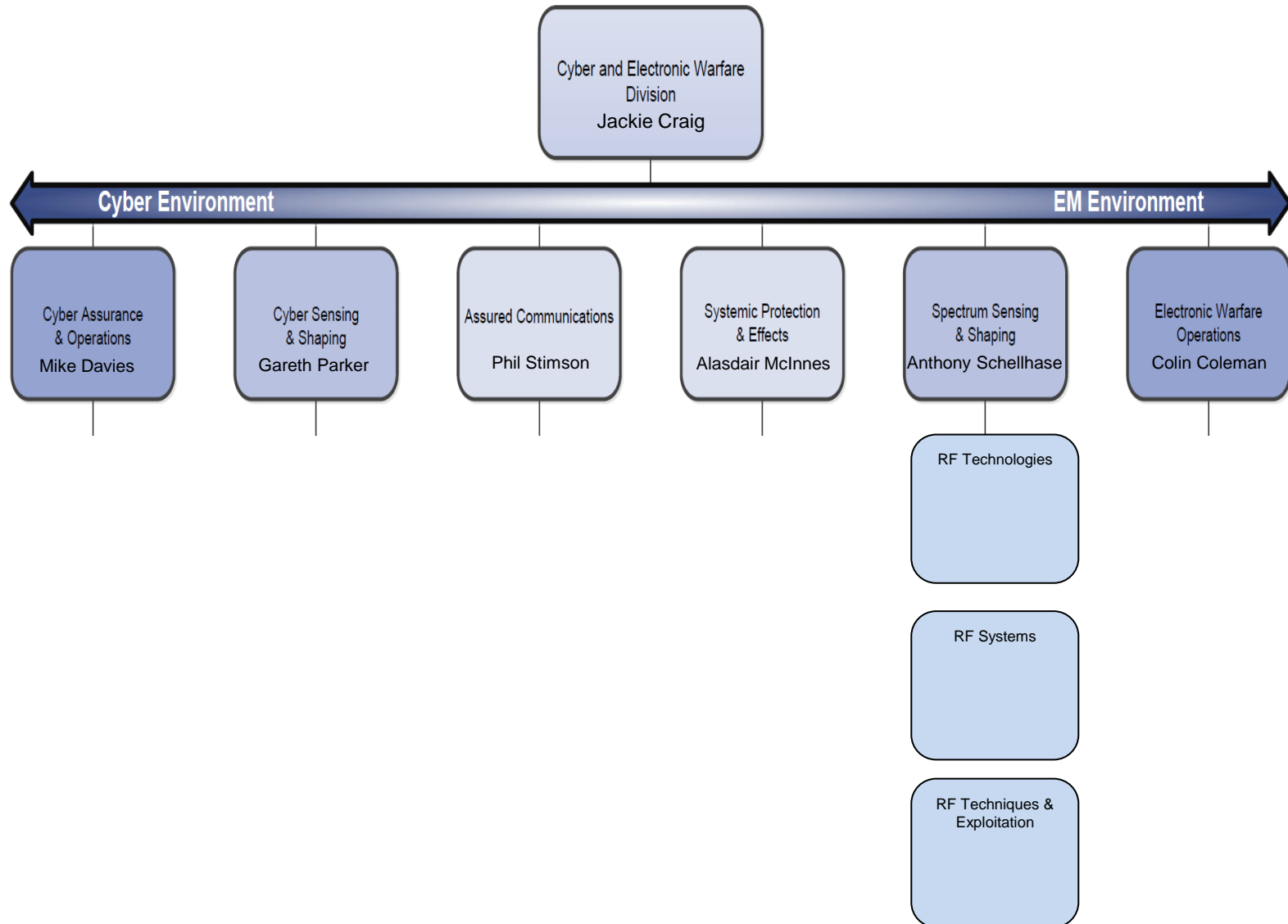
[anthony.schellhase@dsto.defence.gov.au](mailto:anthony.schellhase@dsto.defence.gov.au)

**DST**  
GROUP

Science and Technology for Safeguarding Australia



# Cyber and Electronic Warfare Division Structure



# Spectrum Sensing and Shaping MSTC

*“Sensing & shaping the RF Electromagnetic Spectrum”*

## Context

- Rapid evolution and global access to COTS
- Increasing complexity of EM spectrum
- Software-based systems
- Use of spectrum not used in the past
- Networked sensors & systems

## S&T scope: RF Electronic Warfare

- Wide-band RF digital sensors and effectors
- Multi-sensor and multi-channel processing
- MSA&E for EW Mission Survivability
- Low SWaP RF technology development
- RF SIGINT big data exploitation
- Cognitive ELINT

## Domain: Maritime, Aerospace & National Security



## Core knowledge and skills

- Mathematics, Physics
- Electronic engineering, RF engineering
- RFIC, FPGA, Antenna design
- Computer science
- Digital signal processing
- Numerical modelling, simulation & analysis
- Experimentation

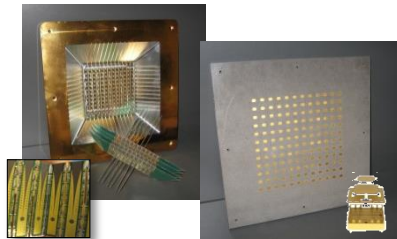
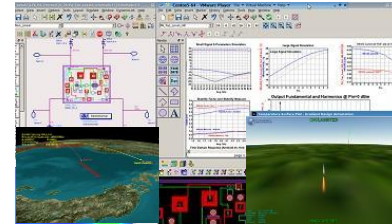
# RF Technologies Group

*“RF phenomenology, technologies and analysis for future RF sensors & effectors”*

Group Leader: Dr Roland Keir (roland.keir2@dsto.defence.gov.au)

## Modelling, Simulation & Analysis

- Chip to Ship modelling, simulation & analysis

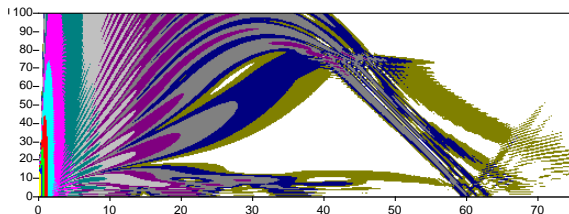
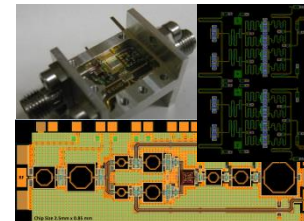


## Array Development

- Broadband, dual polarised array development suitable for active and passive EW systems

## RFIC/MMIC Development

- Miniature RF Technology development for next generation EW



## RF propagation Phenomenology

- Understanding RF propagation capabilities and impact on EW-ISR system performance

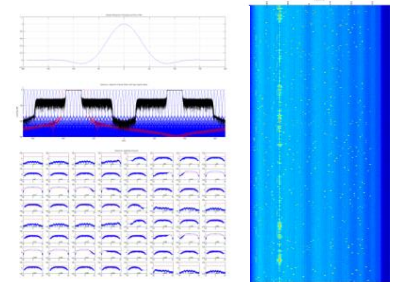
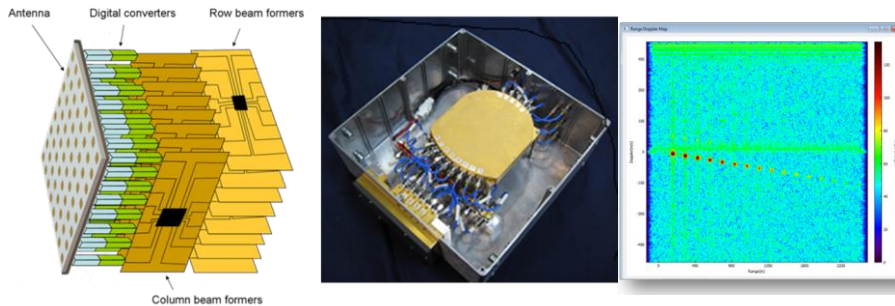
# RF Systems Group

*"Next generation systems and architectures for RF intercept systems"*

Group Leader: Dr Kim Brown ([kim.brown@dsto.defence.gov.au](mailto:kim.brown@dsto.defence.gov.au))

## UWB Digital RCVR system

- Improving the POI, sensitivity, fidelity, detection range, SA and threat warning against modern threat emitters

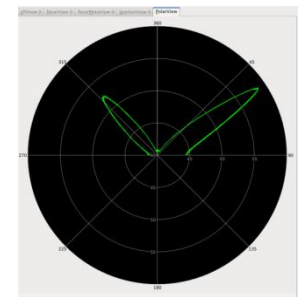
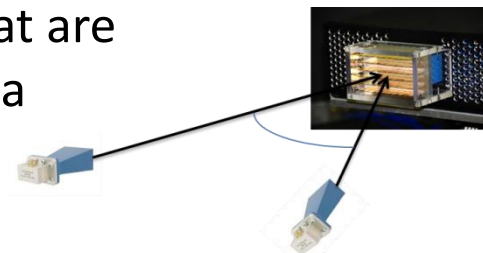


## UWB Digital EA

- Improving the capability against the modern wideband threat

## Multi-channel Spatial Processing Intercept Array

- Improving capability against emitters that are difficult to detect, locate and identify in a cluttered RF environment



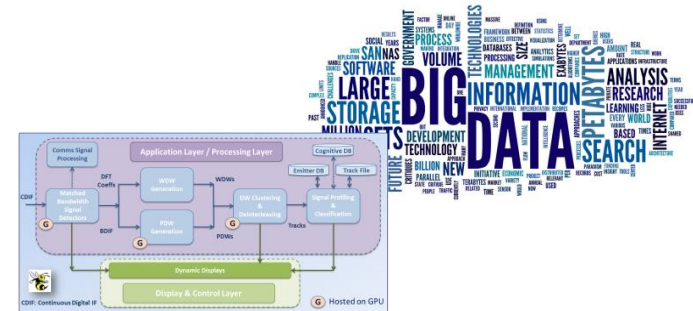
# RF Techniques & Exploitation Group

*"Algorithms and techniques for RF signal detection and characterization"*

Group Leader: Dr Stephen Elton (stephen.elton@dsto.defence.gov.au)

## TechSIGINT High Volume Data Processing

- Wideband Automated Signal Processor (WASP)
- Heterogeneous Processing Architectures

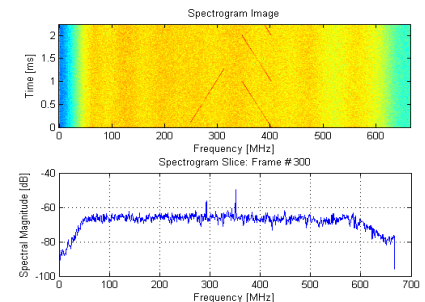


## TechSIGINT Analysis Tools & Decision Aids

- Off-line, operator in-the-loop analysis
- Automated mission planning and tactical decision aids for rapid SA & platform VA

## Signal Processing Theory & Algorithms

- RF waveform detection & characterisation
- LPI signal detection & exploitation
- Cognitive ELINT



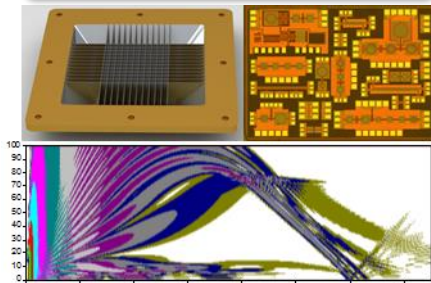


# Spectrum Sensing and Shaping MSTC

Comprehensive RF Sensing & Shaping

$\int$  (RFT+RFS+RFTE)

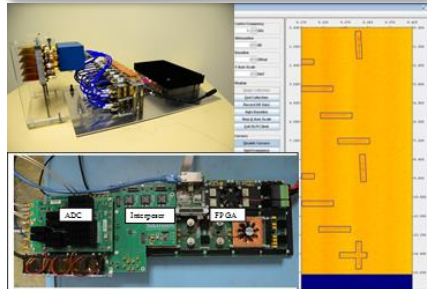
## RFT - Front End



### Environment Interface

- **Wide-band XMT and RCV multi-channel apertures**
- RFIC & SSPA
- Advanced Test & Measurement
- RF Phenomenology
- MSA&E

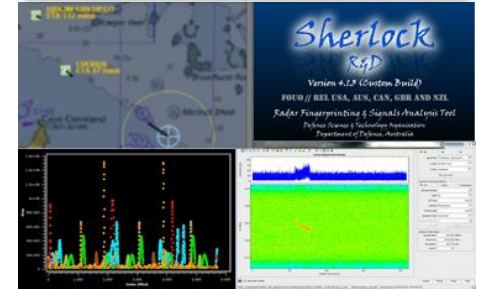
## RFS - Middle



### Real-time Intercept

- **Advanced RF to DIF RCVR systems**
- UWB HW/SW systems
- Multichannel systems

## RFTE - Back End



### Offline Processing

- **DIF to SA, I&W & INT**
- Offline DIF processing for characterization, identification & DF
- Math and stats based algorithmic techniques
- Analysis Tools & TDAs



# Spectrum Sensing and Shaping MSTC Successes

The Spectrum Sensing and Shaping MSTC works with industry and international partners to provide capability for the Australian Defence Organisation.

Examples include:

- the Nulka active decoy that, developed as a joint program with the US, is Australia's largest Defence export.
- the STARDUST series of ELINT augmentation processors that are integrated into ADO operations on maritime and air platforms.



# Spectrum Sensing and Shaping MSTC

## Existing Partnerships

### National

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



### International


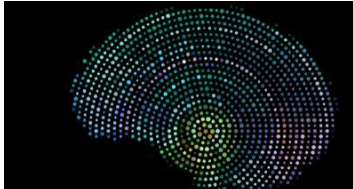
- ONR/NRL, NUWC, NSWC Crane, NSWC Dahlgren
- USN TENCAP, SPAWAR
- Dstl, DRDC, DTA
- TTCP, SD, ABCANZ, Nulka, PFSD MOUs
- Arizona State University

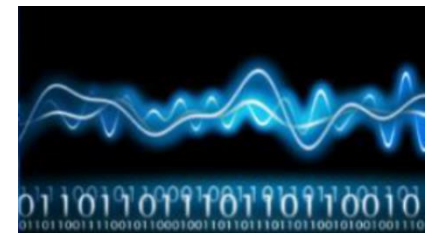
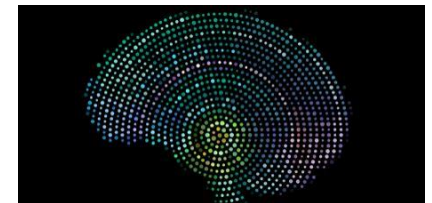


## Partnership Opportunities<sub>1</sub>

We are interested in partnerships that assist with the transition of advanced spectrum sensing and shaping technologies into next-generation capabilities for both Australia and its allies.

## RF Spectrum Sensing in the Maritime & Aerospace Domains

- The ability to provide Threat Warning, Indications & Warning and enhanced Situational Awareness of the electromagnetic environment by providing timely information and intelligence. Example technology areas of interest are:
    - Passive ultra-wideband RF digital sensing systems;
    - Passive multi-channel multi-sensor systems; &
    - Cognitive signal processing and analysis.
- 
- 



# Spectrum Sensing and Shaping MSTC

## Partnership Opportunities<sub>2</sub>

### RF Spectrum Shaping in the Sea Domain

- The ability to determine and shape the electromagnetic environment to increase the possibility of platform survivability. Example technology areas of interest are:
  - Advanced modelling, simulation and analysis tools for EW mission survivability
  - Manufacturing technologies for packaging microwave and millimetre wave electronics
  - Advanced mathematical models for determining the propagation environment for microwave and millimetre wave frequencies.





Australian Government

Department of Defence  
Science and Technology

UNCLASSIFIED

Approved for Public Release

# EW Operations MSTC

*Conceive, develop and validate effective EW technologies  
and techniques for the ADF*

Connect, Partner,  
Collaborate, Innovate

Dr Colin Coleman

Research Leader

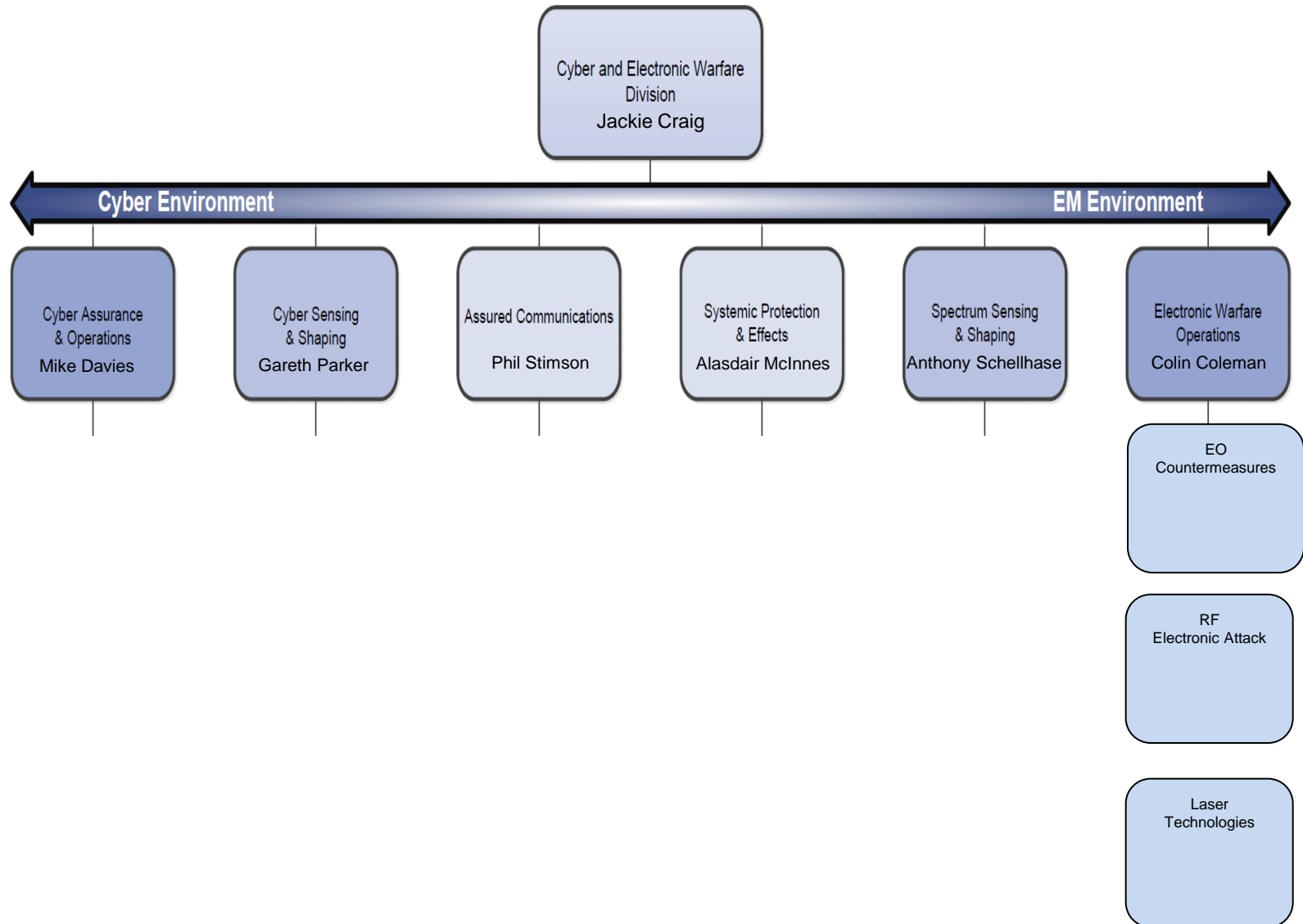
[colin.coleman@dsto.defence.gov.au](mailto:colin.coleman@dsto.defence.gov.au)

**DST**  
GROUP

Science and Technology for Safeguarding Australia

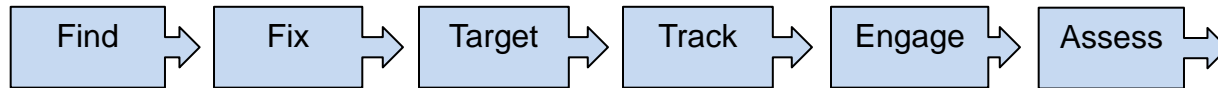


# Cyber and Electronic Warfare Division Structure





# Knowledge is the key element of a kill chain



- Avoid being **Found** or... Know that something **exists**
- Avoid being **Fixed** or... Know **where** it is
- Avoid being **Tracked** or... Know **where continuously**
- Avoid being **Targeted** or... Know **what** it is
- Avoid being **Engaged** or... Know with **weapon precision**
- Avoid being **Assessed**... Know the **result**

EW Operations seeks to deny **knowledge** to break the kill chain.

# RF Electronic Attack

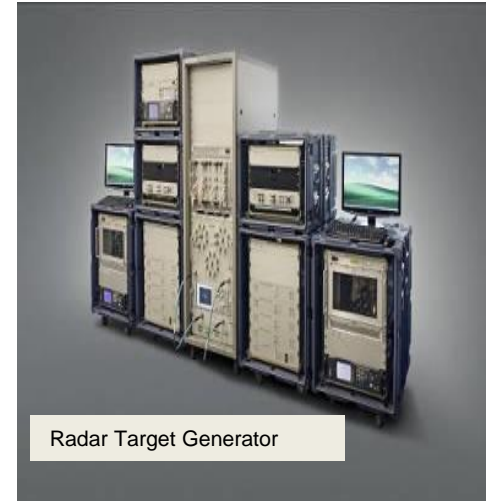
Dr Anthony Szabo

## Task: Counter adversary sensors in the RF domain

Challenges: Agile and adaptive radar  
Passive and networked sensors  
New operating bands: MMW, VHF

Research: Cognitive EW techniques  
Advanced threat emulation  
Counter-Counter LO

Partnership: EW applications of machine intelligence  
RF system development (eg. radar decoys)



# EO Countermeasures

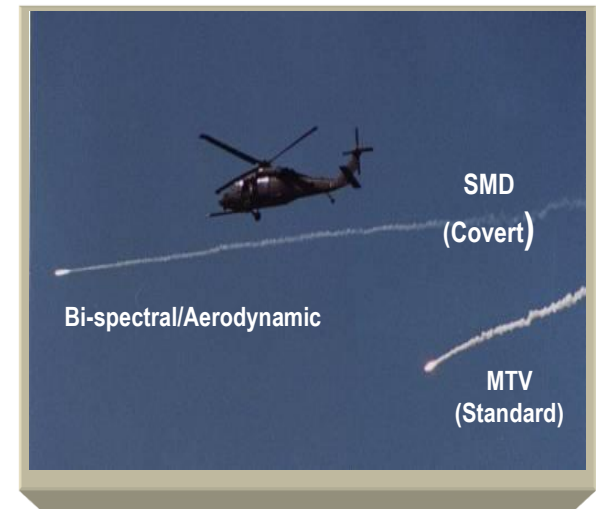
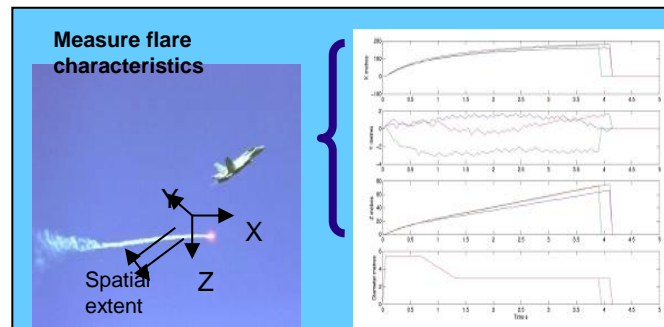
Mr Mark Pitt

**Task:** Know, detect and defeat threats in the EO domain

**Challenges:** Multi-band and imaging sensors (IR/visible/UV)  
Elaborate sensor processing  
Short timescales

**Research:** Missile and hostile fire detection algorithms  
High fidelity simulation for CM development and validation  
Novel methods of threat assessment

**Collaboration:** Omnidirectional image processing for TW/SA



## How a DIRCM (sort of) works:



# Laser Technology

Dr John Haub

## Task: Develop novel laser technology for defence applications

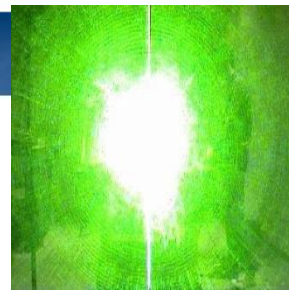
**Challenges:** Produce lasers with the desired power, wavelength, beam quality modulation in a compact, robust and efficient package.

**Research:**

- Fibre laser design and fabrication
- DIRCM laser system development
- High power directed energy lasers
- Laser effects testing
- Laser sensing and response

**Collaboration:** Novel laser systems research

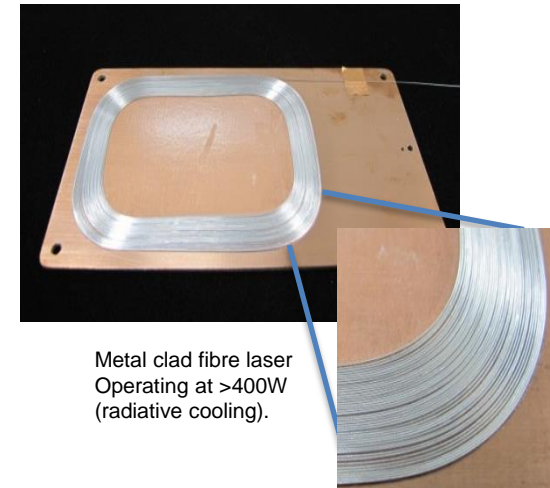
- Advanced DIRCM lasers
- Laser retro-reflection systems
- Eye safe laser attention gaining



Sensor dazzle



LAWS Laser  
Weapon System



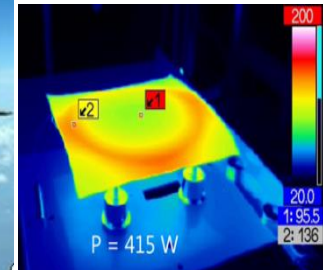
Metal clad fibre laser  
Operating at >400W  
(radiative cooling).



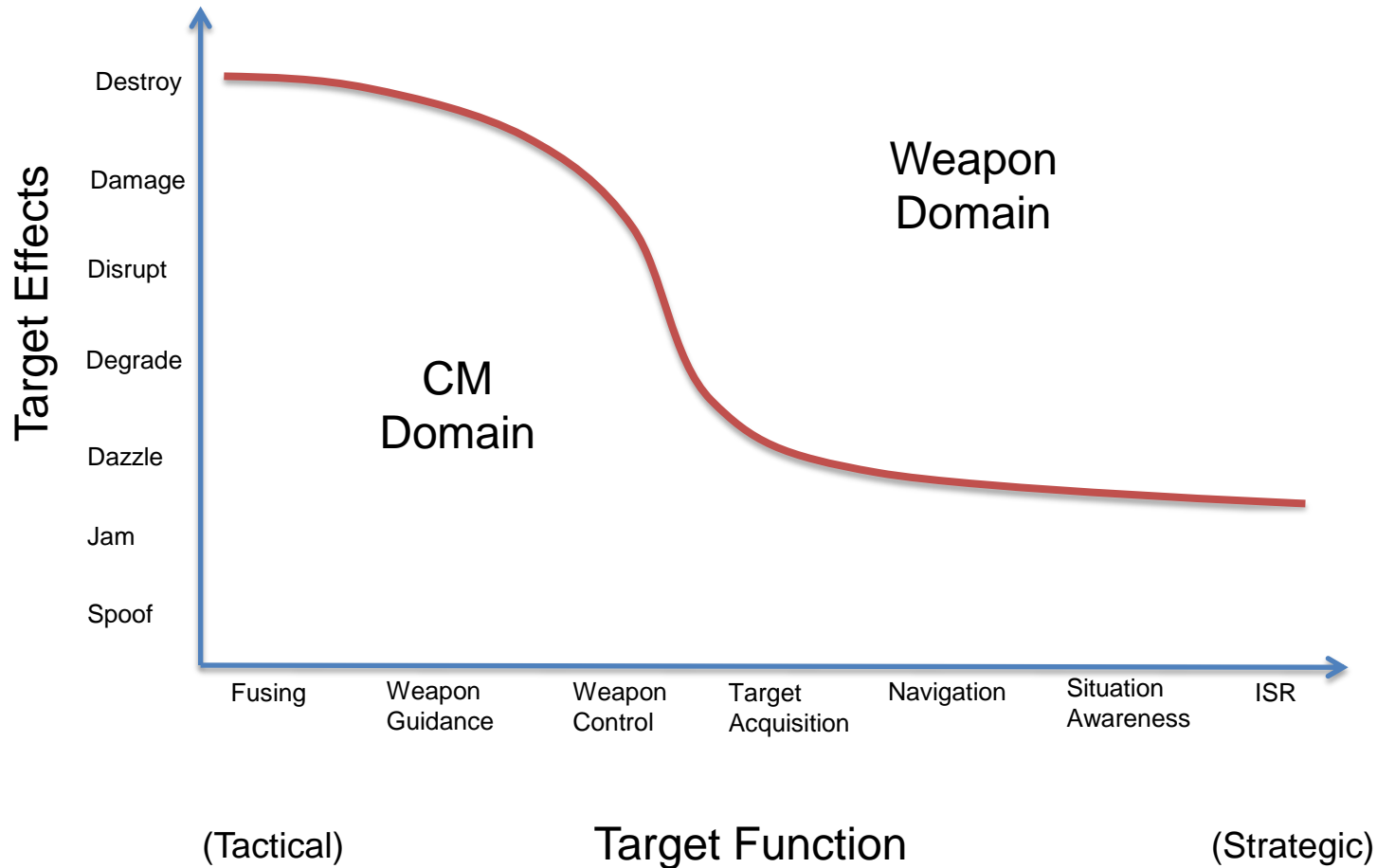
EAGLE



DIRCM: Mid IR 3 – 5μ



# Laser Weapon or Countermeasure?







Australian Government

Department of Defence  
Science and Technology

UNCLASSIFIED

Approved for Public Release

# Discussion

Connect, Partner,  
Collaborate, Innovate

**DST**  
GROUP

Science and Technology for Safeguarding Australia