Australian Government
Department of Defence
Defence Science and
Technology Organisation

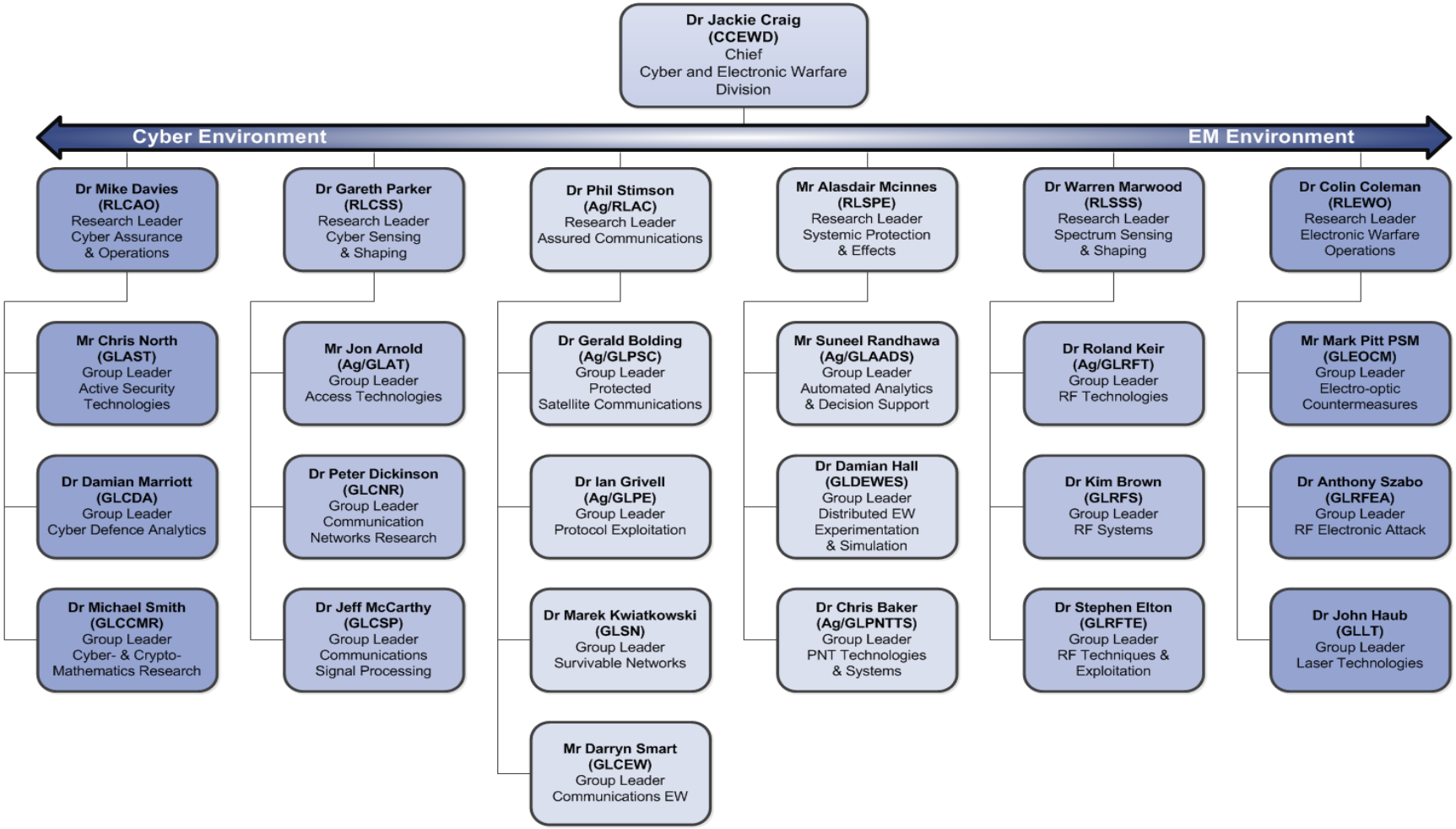
Cyber and Electronic Warfare Division
DSTO Partnerships Week 2015

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

Dr Jackie Craig
Chief
jackie.craig@dsto.defence.gov.au

UNCLASSIFIED

CYBER AND ELECTRONIC WARFARE DIVISION



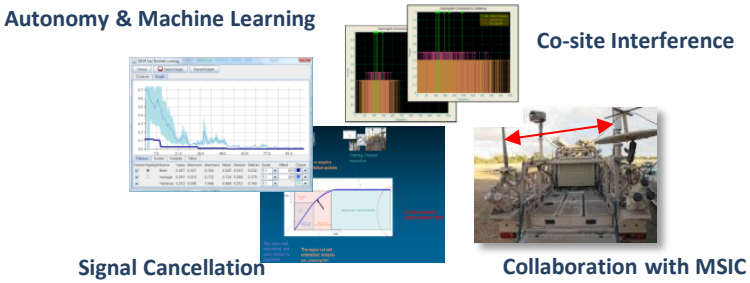
UNCLASSIFIED

CEWD Org Chart - February 2015

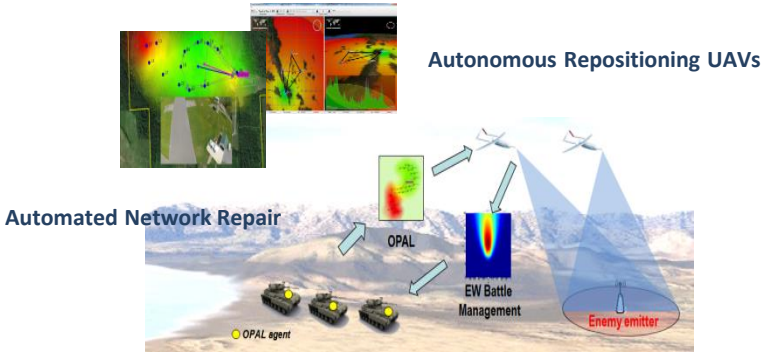
Assured Communications Branch

Develop survivable tactical communications and electronic warfare solutions for contested and denied cyber electromagnetic environments

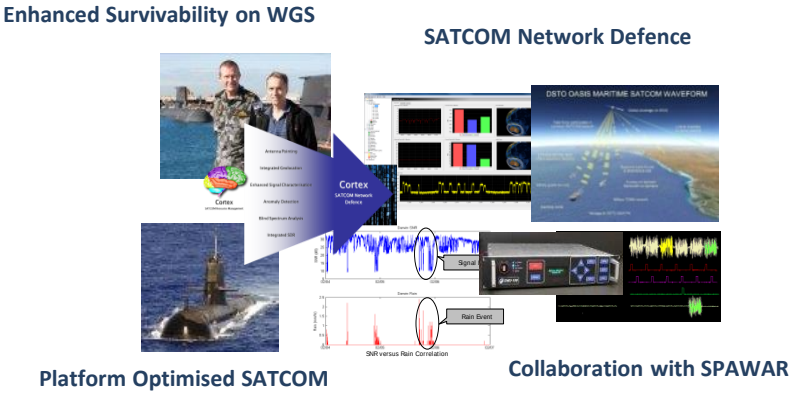
Communications Electronic Warfare Group



Protocol Exploitation Group



Survivable Networks Group

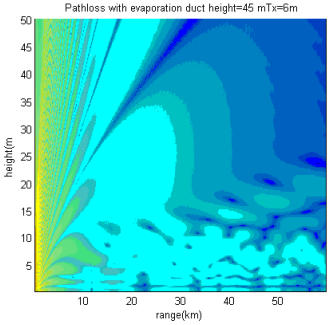


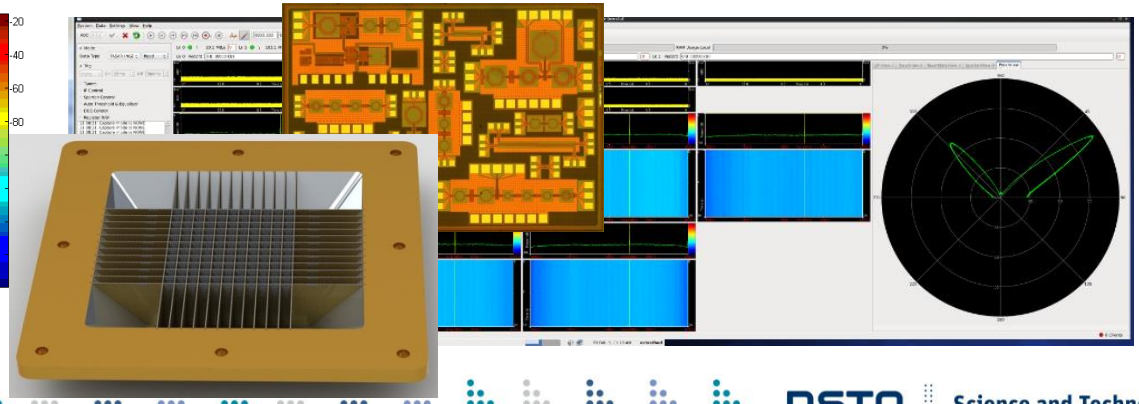
Protected Satellite Communications Group

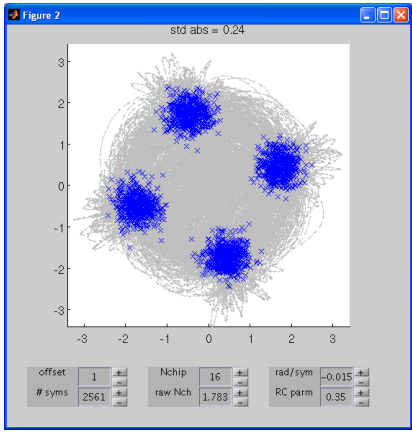
Spectrum Sensing & Shaping

To undertake S&T into RF technologies & techniques that provide situational awareness in a complex RF environment and to defeat the future networked EW, cyber and kinetic threat

Groups	Activities
RF Systems	Development of next generation systems & architectures for multi-function RF intercept systems
RF Techniques	Development of algorithms and implementations for signal detection & characterisation
RF Technologies	RF phenomenology and technologies for future RF sensors & effectors







Electronic Warfare Operations

Deny hostile use of the EM spectrum to engage ADF platforms using EW techniques against all elements of the adversary kill chain

Improving weapon and sensor technologies:

- Multiple redundant sensor modes
- Novel sensor technologies / new spectral domains

Advanced laser development and demonstration

Radar Target Generator

Threat guidance system testing and characterisation
Countermeasure development and validation

We are about denying the adversary **knowledge.**

Australian Government
Department of Defence
Defence Science and
Technology Organisation

Cyber Assurance and Operations MSTC

A critical enabler of effective cyber operations and resilient trustworthy systems

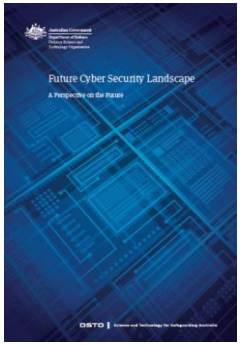
Dr Mike Davies

Research Leader

michael.davies@dsto.defence.gov.au

Strategic Context

Increasing national dependence on ICT: cyber-physical systems pervade



Lag in cyber security, increasing the vulnerability of government, industry and society

Mitigating this vulnerability necessitates that systems be **built**, **defended** and **operated** in a manner which maximises effectiveness within and through cyberspace

Australia's National Security strategy of 2013 highlights the 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 highlights the critical dependency that modern military capabilities have on information systems

Strategic Calls: 2014-2019

- Enhanced functionality, productivity and services will continue to drive developments ahead of cyber security
- 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 tailoring will not be a matter of research
- R&D needed 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 appeared which strike the right balance of cost, performance and security required for high-assurance
- Military deployed networks and more so platforms will continue to lag behind corporate Defence infrastructure in cyber security

CAO Branch Mission:

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

CAO Branch Vision:

A critical enabler of effective cyber operations and resilient trustworthy systems

To be by 2019: *An integrated major S&T capability in vulnerability discovery and mitigation, future threat estimation, crypto-mathematics, trustworthy systems and cyber autonomy with a critical role in the Australian Defence Organisation's ability to operate successfully within and through cyberspace*

Modus Operandi in Core Cyber Security S&T

DSTO

Mainstream Threats

We develop techniques to **discover and counter** their presence

We forecast and prototype **advanced forms of adversarial software and hardware.**

We demonstrate their likely appearance and effect

We develop and use **advanced cryptologic techniques**

We develop tools and techniques to **discover vulnerabilities** and fix predispositions

We develop solutions for resilient and **trustworthy ICT**

We demonstrate robust risk-based **pervasive security** policy and architectures

We pursue **autonomous cyber security** solutions

and repeat…

We raise the bar…

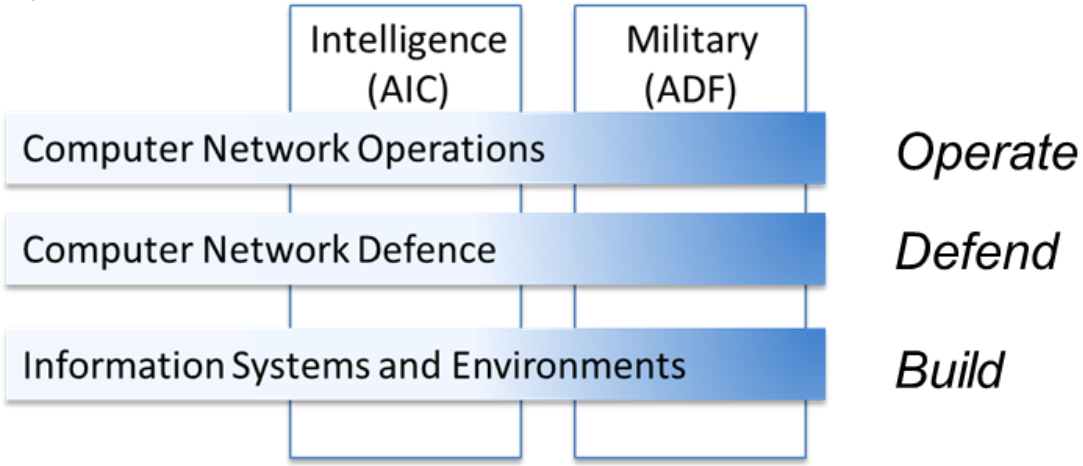
DSTO

Mainstream Threats

Core Impact Areas

CAO Branch engages a client community across the AIC and the ADF consisting of **designers, developers, trainers, managers and operators** of cyber capabilities. Impacting on

- Information systems and environments in general (reflecting the importance of security at *build*)
- Computer network defence (the need to *defend*) and
- Computer network operations (the need to *operate* within and through cyberspace)



Broad Strategic Directions

The strategy reflects the following broad strategic directions of S&T support:

- Increased impact on sovereign capabilities for computer network operations
- Increased impact on the ADF, focussing on trustworthy systems for military operations, and the defence of military platforms
- Increased national shaping to strengthen and partner with the cyber security S&T capabilities of academia and industry

Australian Government
Department of Defence
Defence Science and
Technology Organisation

Cyber Sensing and Shaping MSTC

Sensing and shaping of communication networks for Cyber

Dr Gareth Parker

Research Leader

gareth.parker@dsto.defence.gov.au

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

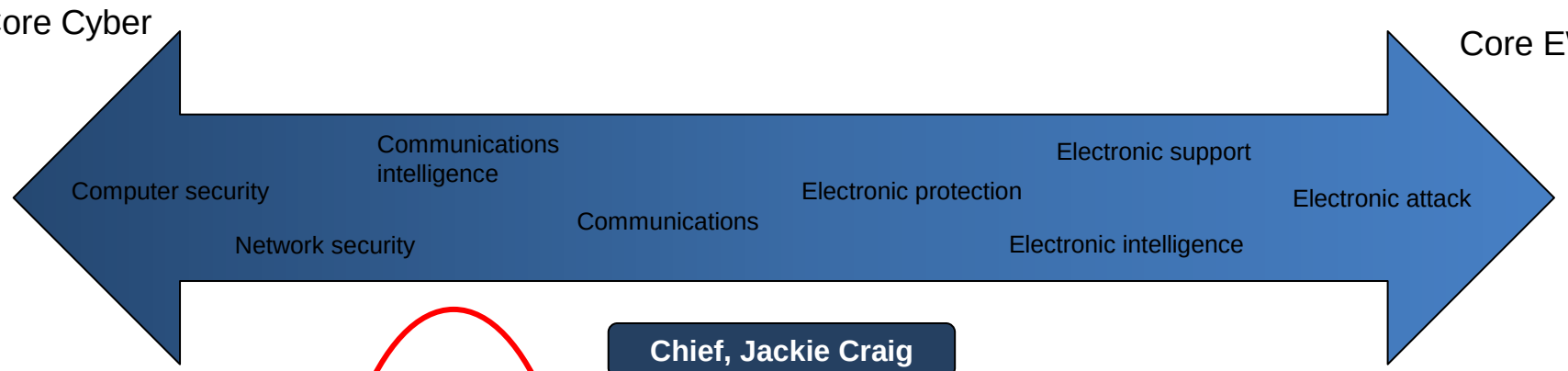
- Network characterisation & knowledge representation
- Network structures, protocols and behaviours
- Vulnerability discovery and treatment
- Communications technologies

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

Cyber and Electronic Warfare Division



Chief, Jackie Craig

- **Cyber Assurance & Operations** (Mike Davies)
  - Active Security Technologies (Chris North)
  - Cyber Defence Analytics (Damian Marriot)
  - Cryptomathematics Research (Michael Smith)
- **Cyber Sensing & Shaping** (Gareth Parker)
  - Access Technologies (Jon Arnold, Ag)
  - Communication Networks Research (Peter Dickinson)
  - Communications Signal Processing (Jeff McCarthy)
- **Assured Communications** (Phil Stimson, Ag)
  - Protected Satellite Communications (Gerald Bolding, Ag)
  - Protocol Exploitation (Ian Grivell, Ag)
  - Survivable Networks (Marek Kwiatkowski)
  - Communications EW (Darryn Smart)
- **Systemic Protection & Effects** (Alasdair McInnes)
  - Automated Analytics & Decision Support (Suneel Randhawa, Ag)
  - Distributed EW Experimentation & Simulation (Damian Hall)
  - PNT Technologies & Systems (Anthony Schellhase)
- **Spectrum Sensing & Shaping** (Warren Marwood)
  - RF Technologies (Roland Keir, Ag)
  - RF Systems (Kim Brown)
  - RF Techniques (Stephen Elton)
- **Electronic Warfare Operations** (Colin Coleman)
  - Electro-optic countermeasures (Mark Pitt)
  - RF Electronic Attack (Anthony Szabo)
  - Laser Technologies (John Haub)

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

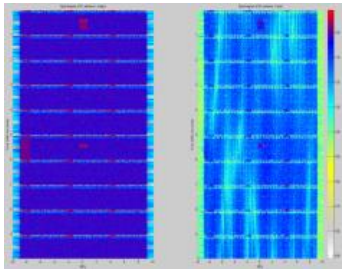
Communications Signal Processing

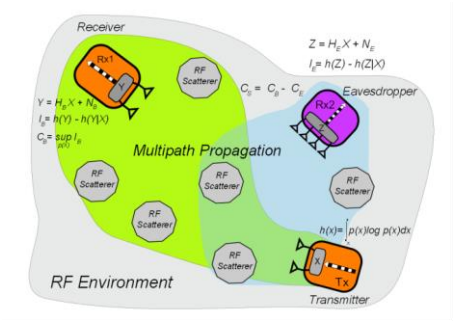
"Physical and cross-layer processing of wireless networks"

Group Leader: Dr Jeff McCarthy

Signals analysis

- Signal collection, enhancement and geolocation





Waveform security

- MIMO, multichannel and diversity techniques

Software defined radio solutions

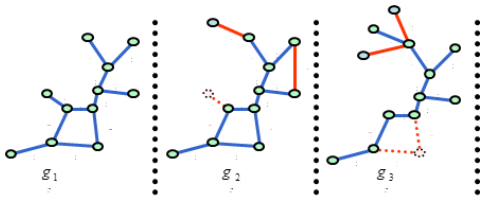
Communication Networks Research

"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)

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

(08) 7389 5861

Wireless Security

Aim

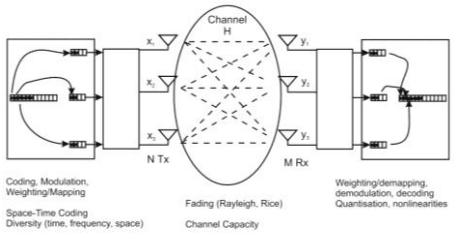
To explore vulnerabilities in wireless communications systems and develop physical layer approaches to enhancing security

Areas for expanded collaboration

- Cross-layer approaches
- Tactical communications
- Cryptography
- Wireless sensor networks security
- Protocol jamming

Our approach

- Physical layer – LPD, MIMO, diversity



Contacts

Dr John Kitchen
john.kitchen@dsto.defence.gov.au
(08) 7389 6431

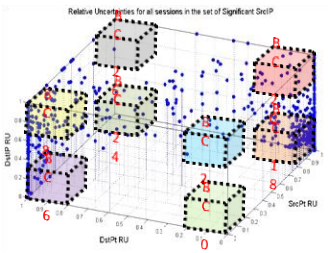
Internet Traffic Profiling

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

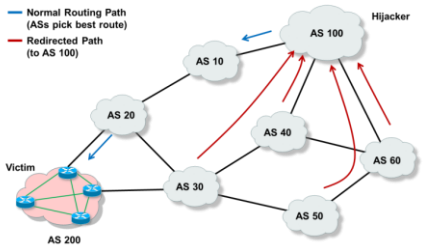
darren.webb@dsto.defence.gov.au

(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

(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

(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

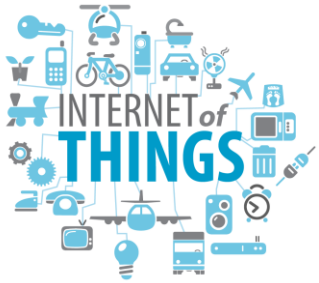
Engage in regular technical exchanges with academia, and industry in areas of mutual interest.

Contacts

Peter Dickinson

Peter.dickinson@dsto.defence.gov.au

(08) 7389 6158



Australian Government
Department of Defence
Defence Science and
Technology Organisation

Systemic Protection & Effects MSTC

Force-level Cyber and Electronic Warfare with effective command and control

Mr Alasdair McInnes

Research Leader

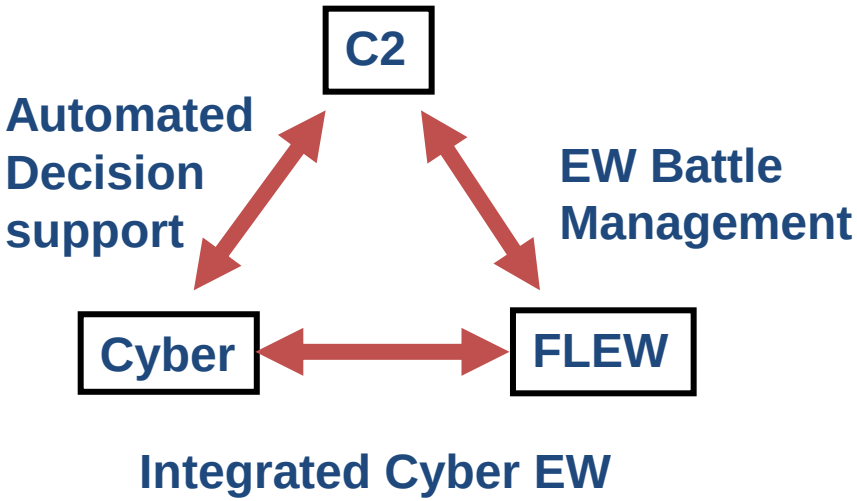
alasdair.mcinnes@dsto.defence.gov.au

Outline

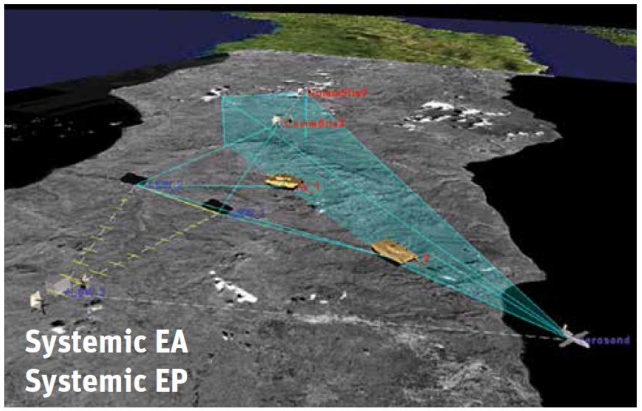
- MSTC mission
- Where we fit
- Strategic context
- Key challenges and responses
- Main activities
- Summary

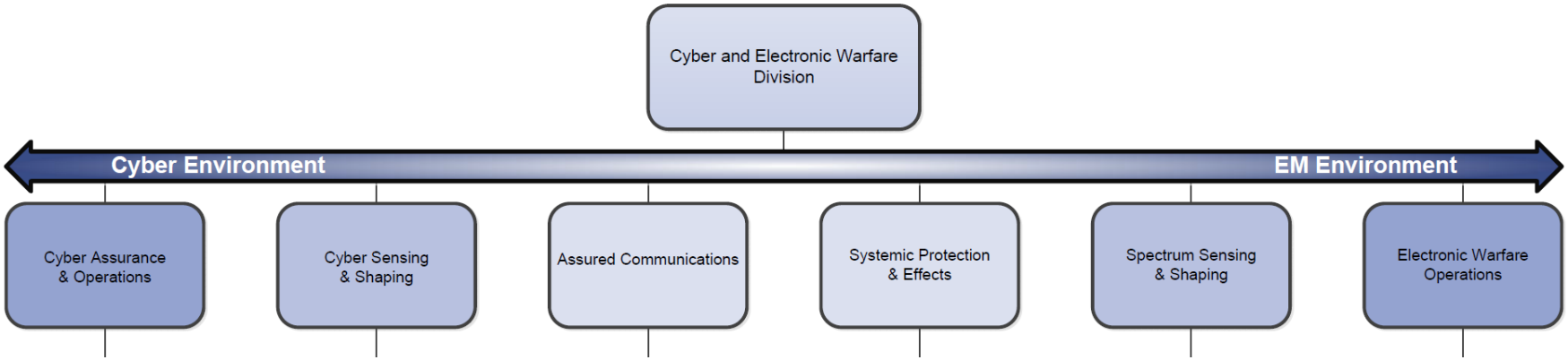
SPE Mission

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



Cyber-Electronic Warfare Continuum





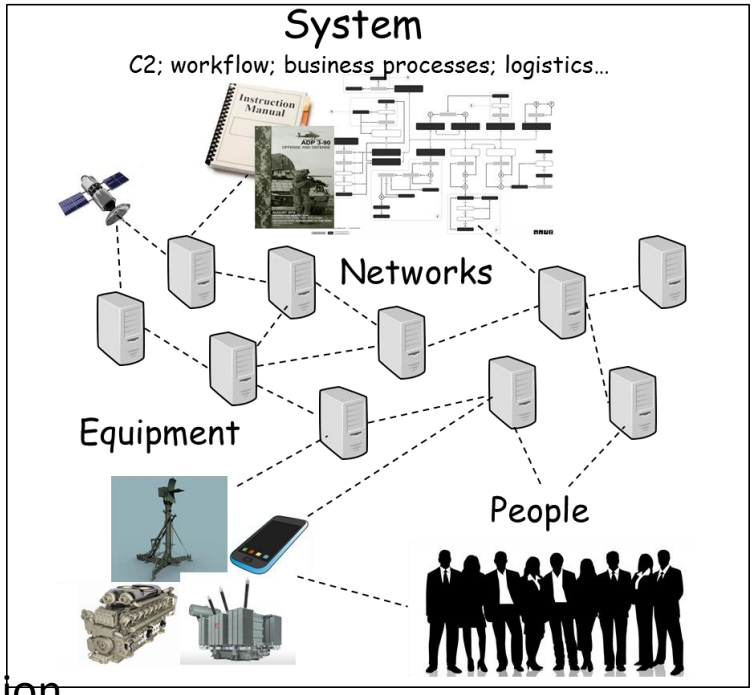
Key External Trends – and Objectives

- Increasingly numerous, networked, EM-capable platforms
  - An effective complex adaptive C4ISTAREW capability
- Increasingly complex EM environments
  - An effective EW Battle Management capability – a step towards the above
- Threat evolution – networked, software-driven
  - Comprehensive threat M&S capability
  - Effective experimentation capability
- Emergence of Cyberspace as an operational environment
  - Mission Assured Cyber Dependent Operations
- Critically reliant on cyber-physical systems
  - M&S and experimentation capabilities for cyber aspects
- Increasingly reliant on PNT
  - Assure own PNT, deny adversary PNT
  - Protect civilian PNT

Automated Analytics & Decision Support Group

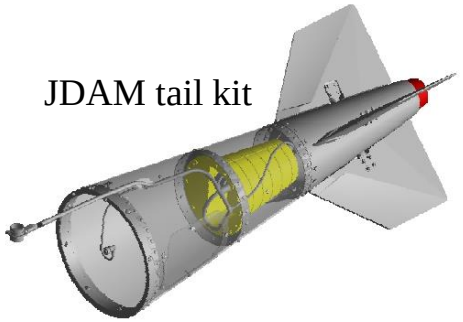
- Primary Impact Domains
  - Military Platform Survivability
  - Mission Assurance
  - Critical Infrastructure Protection

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

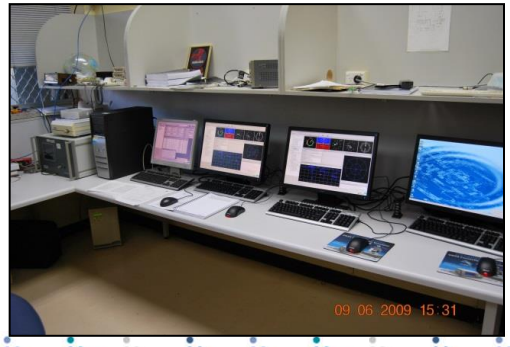


Positioning Navigation and Timekeeping Technologies & Systems Group Major Activities

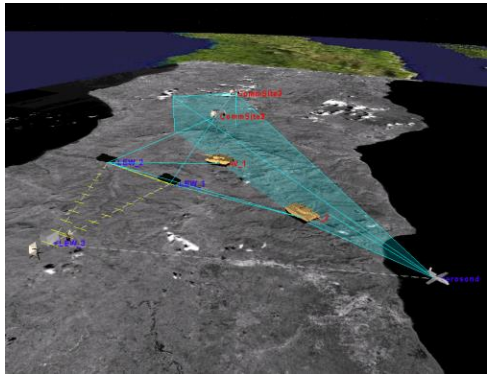
- Primary Impact domains
  - Operate in GPS-denied conditions
  - Deny satellite navigation to adversaries
  - Alternative PNT technologies



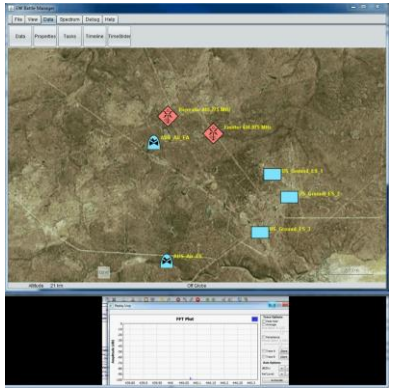
- S&T focus areas
  - International collaboration
  - Anti-jam technologies & techniques
  - Novel denial techniques
  - Future technologies for accurate, stable timing



Distributed Electronic Warfare Experimentation and Systems Group Main Activities

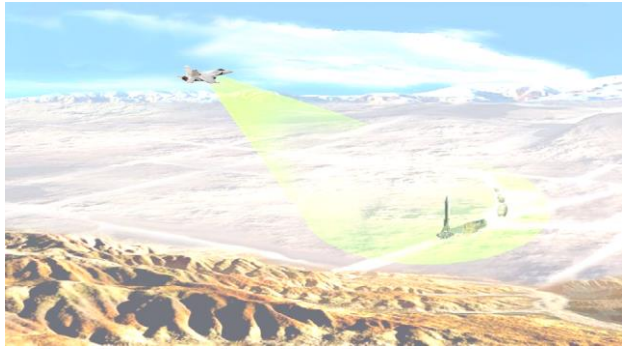


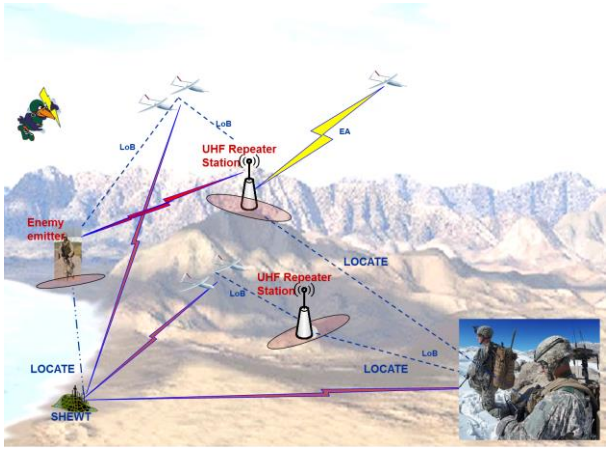
- Modelling, Simulation & Analysis
  - Force Level EW Synthetic Environment
  - Detailed Threat Modelling



- Experimentation
  - EW Battle Management
  - Shared EW Testbed
  - Tactical Networks

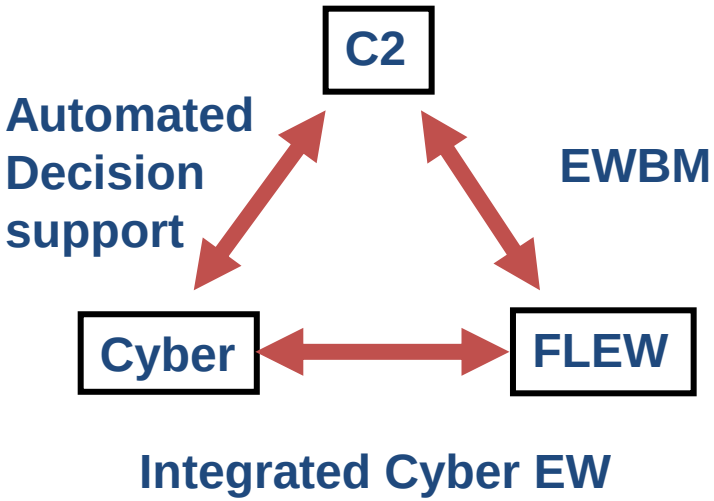
- Co-development
  - Advanced Passive Surveillance Capability
  - Geolocation





Summary

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



Australian Government
Department of Defence
Defence Science and
Technology Organisation

Divisional Wrap-up