



Australian Government

Department of Defence

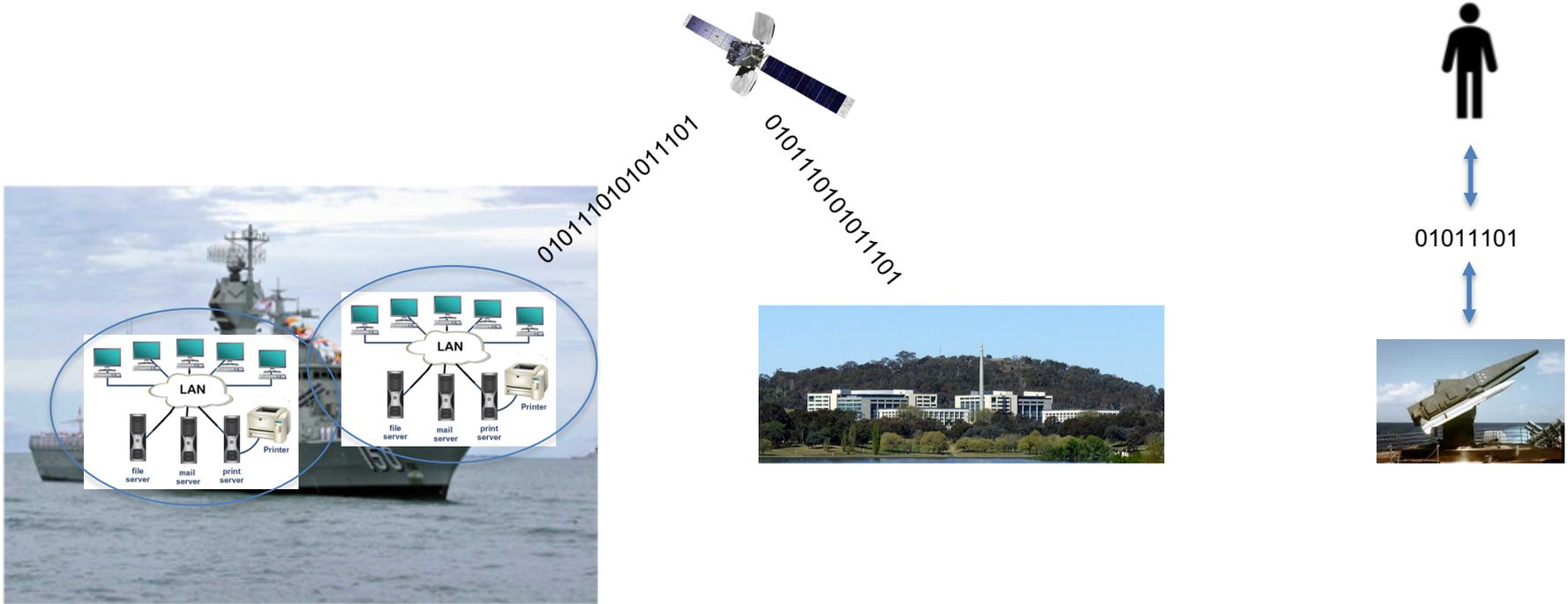
Science and Technology

Next Generation Technology Cyber

Dr Gareth Parker

Research Leader, Cyber Sensing and Shaping
(Theme Leader, Next Gen Technology – Cyber)

Modern military systems



Stuxnet



Ukraine



Fundamental technological challenges

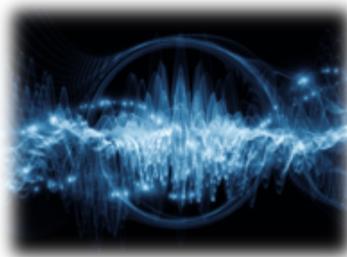
Increasing dependence on an increasingly unknown system



Speed of technological change



Data-to-decision reflex



An unknown and persistent threat



Mitigation of untrustworthiness

Military Differentiating Factors

Life or death consequences



Risk that vulnerabilities are only realised at critical times



System complexity



Military Differentiating Factors

Combined effects



Speed differential



Deterrence and offence



Asymmetry



DST Cyber Strategy

Challenges

- Prevent environment surprise
- Counter and unknown and persistent threat
- Mitigate untrustworthiness
- Data-to-decision reflex
- Evolve Cyber-EW concepts

Fundamental requirements

- Threat assessment
- Intelligence
- Situational awareness
- Information assurance
- Planning and shaping

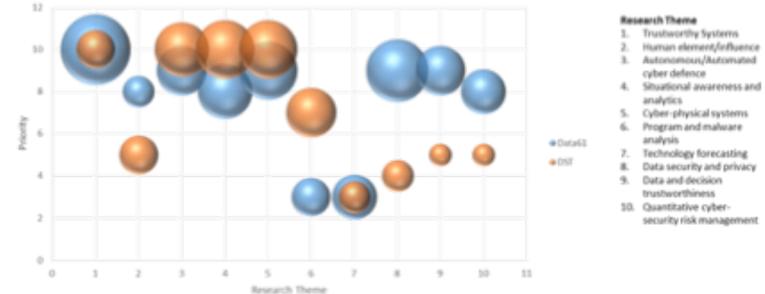


Foundational research themes

- System design for resilience
- Autonomous systems
- Sensing to effects
- Cyber influence and data analytics
- Technology forecasting

Partnering with Data61

- Considerable S&T synergies
- Complimentary responsibilities, Influence and Partnering communities
- An opportunity to
 - Leverage dual use research and technology
 - Develop deeper collective S&T expertise - opportunity for knowledge exchange, peer review and support
 - United academic interface with Government research agencies
 - Expanded and strengthened international partnerships
 - Leverage Data61 specialized commercialisation expertise
 - Share research infrastructure



Cyber Collaboration



- 3-year agreement to partner with Data61 in shaping and leveraging the academic community in Cyber S&T
- Includes:
 - Collaborative research projects across 4 foundational research themes
 - Growing the national talent pool - PhD supervision/scholarships
 - Outreach – cyber event support



System design for resilience

Trustworthy systems

- Trusted core components
- Secure design practices
- Scalability – circuits to platforms
- Verification and vulnerability analysis



System design for resilience

Communications and data security

- Advanced cryptography
- Secure waveforms



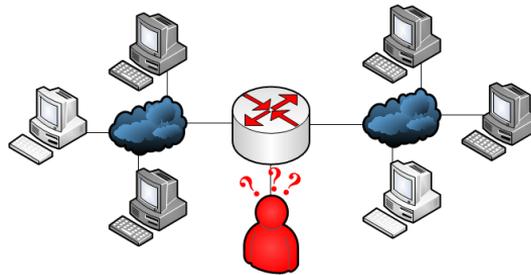
System design for resilience

Agile networks

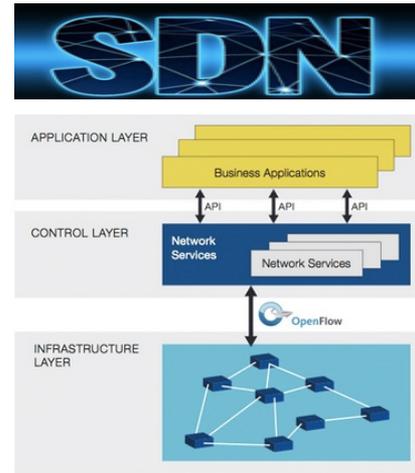


Virtualisation

Moving target defence

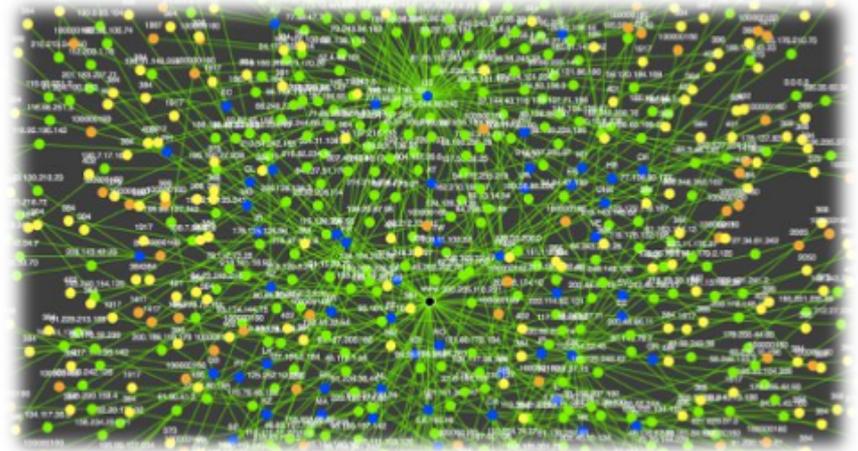


Software defined networking



Situational Awareness

- Mission system dependencies
- Mapping to cyber terrain
- Threat awareness
- Dynamic understanding of systems and networks
- Anomaly detection



Sensing to Effects

- Proximal cyberspace
- Combined effects development
- Validation and battle damage assessment



Artificial intelligence and autonomous cyber

- Automated and autonomous planning and response
- Machine learning for discovery and situational awareness



The Human Element

- Operator vulnerabilities
- Influence

