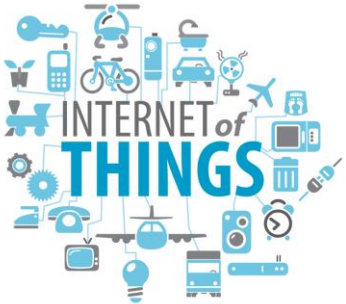
Australian Government
Department of Defence
Science and Technology

# Defence Cyber S&T

Dr Gareth Parker
Theme Leader, Next Generation Technology Cyber

# National Interest






# Defence

- Complexity
- Asymmetry
- Isolation
- Combined effects

# Defence's cyber S&T goals

## Platform cyber-worthiness and cyber security

Establish a trusted core and a quantifiable level of trustworthiness in Defence's networks and digital platforms.

## Defensive cyber operations

Maintain a dynamic understanding of complex military digital systems, autonomously identify and fix vulnerabilities, and defend against attack by a sophisticated, machine-assisted adversary.

## Intelligence

- *Through* cyberspace: Identify, locate, and exploit targets in a massively connected, virtualised world, using computer and communications information that may be voluminous, incomplete, heterogeneous and encrypted.
- *About* cyberspace: understand broader cyberspace, including the threat landscape.

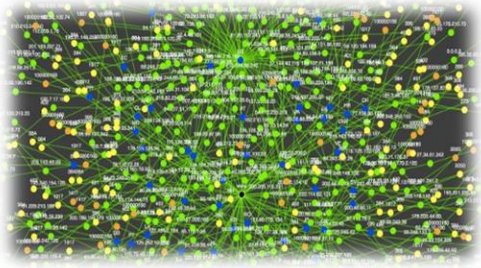
## Effects

Development of targeted effects against an adversary through cyberspace.

# Research themes

System design for resilience

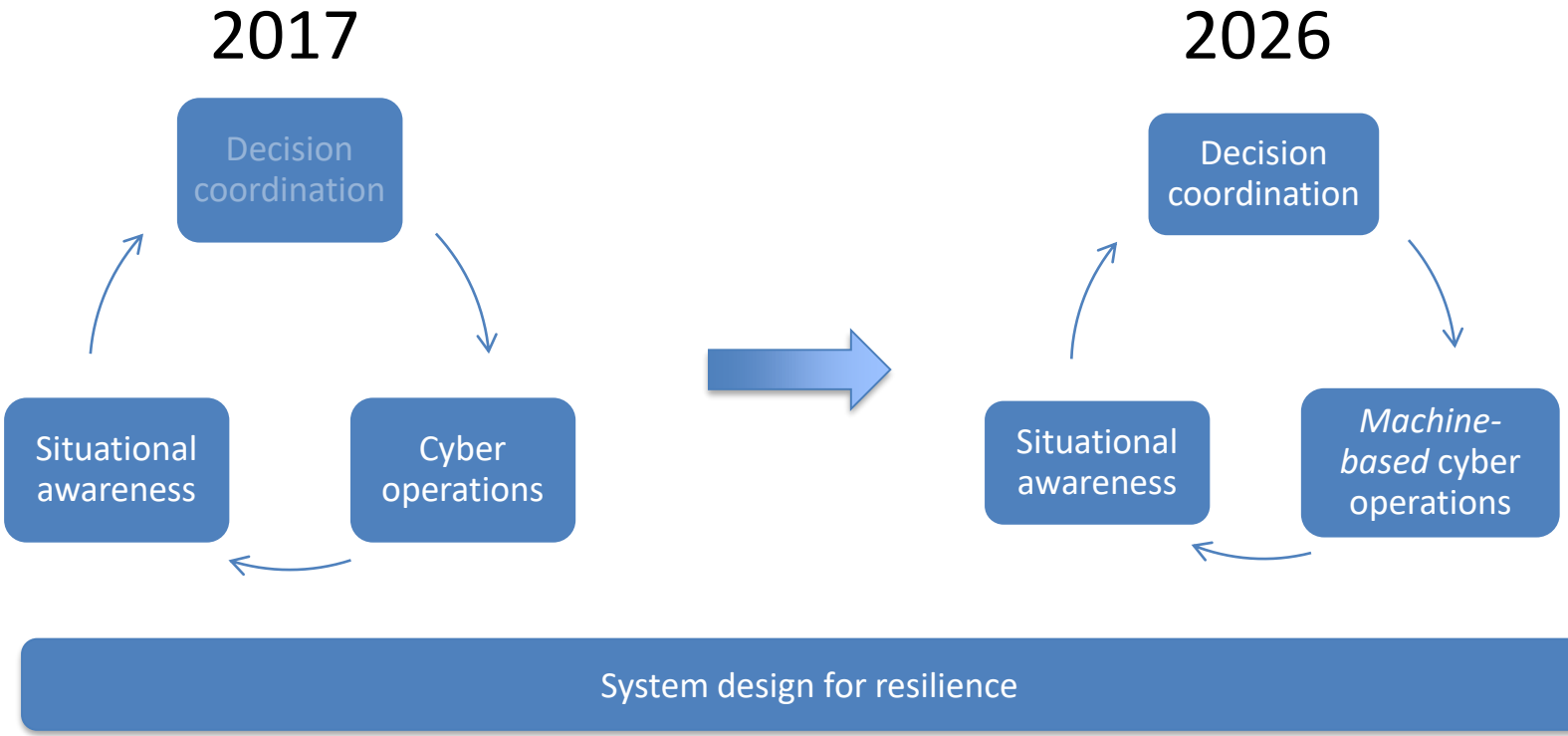
Situational awareness



Decision support

Machine-based cyber operations

# S&T for military cyber operations



# System design for resilience

*Building solid foundations into Defence's digital systems*

## Constituent research

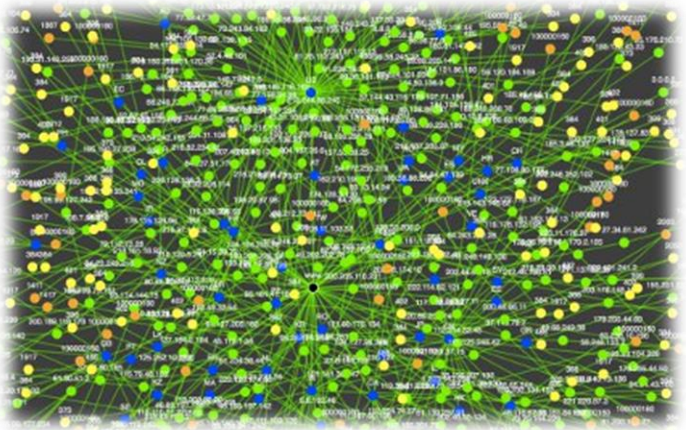
- Trustworthy underpinning for systems
- Hardening military applications and systems
- Vulnerability research
- Communications security
- Cryptography
- Human influence

# Cyberspace situational awareness

*Real-time understanding of a dynamic system through information that can be voluminous, incomplete, heterogeneous and encrypted*

## Constituent research

- Mapping of military mission to key cyber terrain
- Discovery of behaviours of interest in network traffic
- Representation and reasoning about computer and communication network information
- Battle damage assessment



# Cyber decision coordination

*Coordinating real-time decisions in a contested cyber environment*

Constituent research

- Decentralised cyber command and control
- Automated planning and decisions
- Cyber operations analysis

# Machine-based cyber operations

*Enable ADF cyber teams to train, exercise and deploy with inhuman speed and scale at the tactical edge with minimal resources*

## Constituent research

- Machine-assisted cyber defence
- Dynamic malware & vulnerability discovery
- Military autonomous cyber operations
- Robust machine learning-based network defence

# Next Generation Technology - Cyber Phase I: 2017-19


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

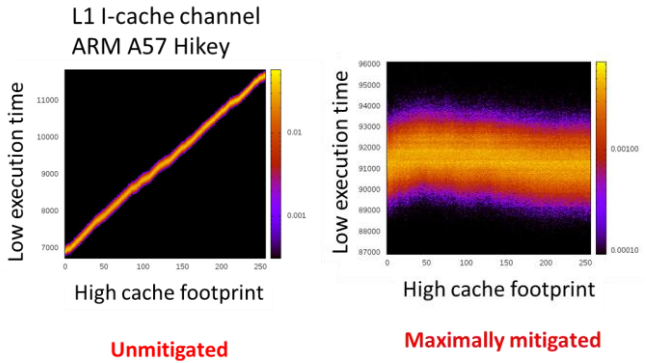
- 3-year agreement to partner with Data61 in shaping and leveraging the academic community in Cyber S&T
- Collaborative research projects with 13 universities
- Research community building events

# Outcomes to date

# Phase I Outcomes – System Design for Resilience

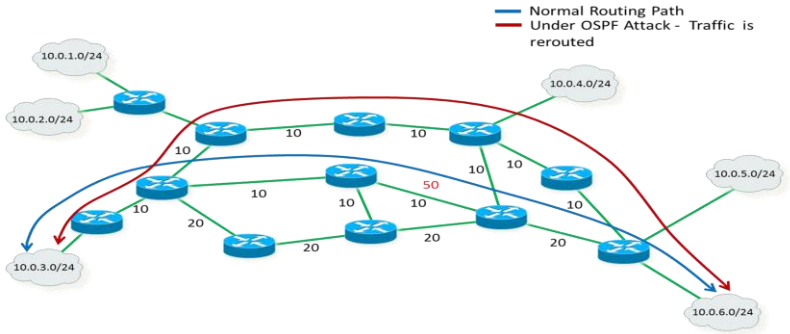
## Micro-architectural vulnerabilities

- Mitigation of covert timing channel between concurrent processes




## Cross-domain desktop compositor

# Phase I Outcomes – System Design for Resilience

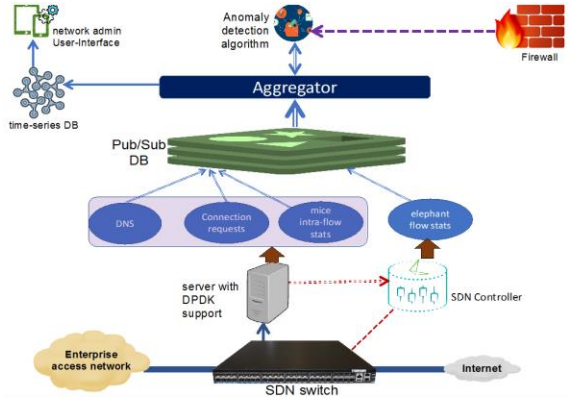



## Vulnerabilities in network control

- Detection of anomalous behaviour in OSPF network protocol

## Software defined network security

- Architecture developed to capture, analyse and forward network traffic
- ML analytics to detect adversarial data exfiltration via DNS



# Phase I Outcomes – System Design for Resilience

## Deep learning for code vulnerability analysis

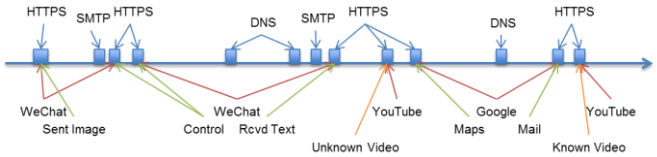
- Identifying function scope in software binaries
- Transferring learning models to domains in which few vulnerabilities are available for training



## Phishing mitigation

- Researching the user and environmental factors that influence phishing susceptibility

# Phase I Outcomes – Situational Awareness

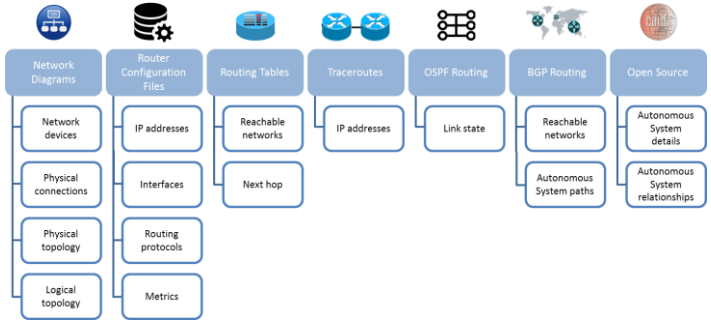



## Deep learning for encrypted network traffic characterisation

- Successful identification of WiFi message content using an ‘open world’ assumption
- Deep learning solutions based on temporal, ever evolving, and sparsely-labelled data

## Network knowledge representation, fusion and reasoning

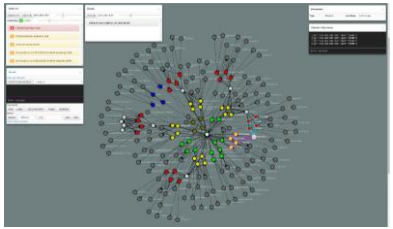
- Development of an appropriate ontology for network related information
- Developed a framework for incorporating provenance information



# Phase I Outcomes – Machine-Based Cyber Operations

## Autonomous penetration testing

- Demonstration of the utility in applying decision processes from robotics to design optimal strategies for adversarial cyber games



## Adversarial machine learning

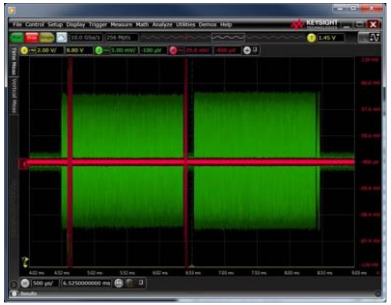
- Demonstration of network defence compromised through both manipulation of reward mechanism as well as poisoning of training data

## Autonomic computing

- Distributed Self-Management of Resilient Cyber Systems

## High Speed Machine Learning

- Successful FPGA implementation and comparative assessment of ML-based spectrum monitoring algorithms
- Planned extension to EW application



# Phase I Outcomes – Cyber Decision Support

## Automated planning tools

- Extension to cyber security application of planning approaches for problems with time constraints