A collaboration in Defence

Smart Base: Reimagining Network Security in Defence

Intent-Based Networking – Driving Digital Transformation in Defence

Purpose of the white paper

This white paper discusses a research project between Cisco and University of Adelaide intended to stimulate discussion about the future of Defence technology networks and to announce a broader investment by both parties to establish a special purpose Critical Infrastructure Lab aimed at exploring and testing new advanced networking solutions. The laboratory will be open to Defence personnel and Defence industries – as well as owners and operators of other critical infrastructure – and will be deployed at the Australian Cyber Collaboration Centre at the Lot Fourteen precinct in Adelaide.

Pillars of the Cisco and University of Adelaide collaboration

Research & innovation

The research project outlined in this white paper represents the start of a research collaboration around Defence.

Skills & Training

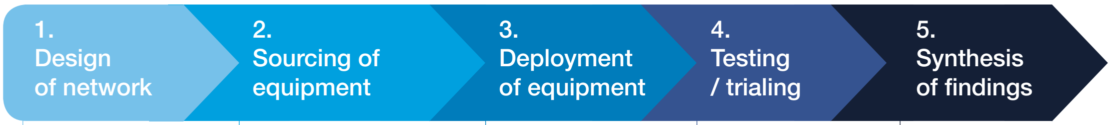
The university is exploring expanding the collaboration through the Cisco Networking Academy on specialist curriculum.

Campus infrastructure

Cisco provides underlying network technology and services to the university that underpin teaching, research and administrative functions.

Methodology and approach

This white paper presents findings from a limited scope trial of a software-defined network in a simulated Defence environment. The trial was based on a combination of technology deployed in a purpose-built lab environment. Our approach was as follows:



1. Design of network: Identification of relevant Cisco hardware and UofA software components.

2. Sourcing of equipment: Sourcing of firewall and related hardware (Cisco) and provision of a server to host standard Cisco utilities and UofA policy-defined networking software (UofA).

3. Deployment of equipment: Combined Cisco and UofA technical effort to deploy the equipment within laboratory environment.

4. Testing / trialing: Testing correctness of deployed policies via wired and wireless equipment within laboratory environment.

5. Synthesis of findings: Write-up of findings from trial and inclusion in UofA reporting.

Executive Summary

What is the Critical Infrastructure Lab?

The Cisco – University of Adelaide Critical Infrastructure Lab concept recognises that today's military environment is data-centric and that the network collects, aggregates, and acts on data at speed and scale to maximise operational advantage and increase efficiency. Data – and the network which underpins it – needs to be treated as a strategic asset operationalised to empower more lethal and effective military capabilities. It must be built upon a secure platform from the edge to the cloud and across multiple domains and in a way that enables the flexible and secure movement of sensitive information and communications anywhere, anytime, in any mission environment.

> "Cyber threats to Defence networks and mission systems have the potential to undermine the Australian Defence Force's ability to operate"[1]

The focus of this project

The objective of the Cisco and University of Adelaide collaboration was to better understand and investigate the benefits of Intent-Based Networks (Software Defined) in a Defence context. The initial focus of the collaboration was threefold:

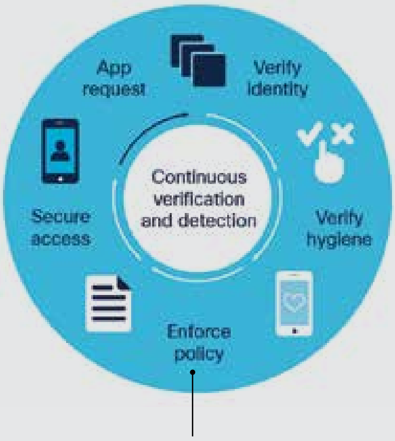
1. To design an operational, purpose-built lab environment (the Critical Infrastructure Lab) that can be used by other parties to develop and test solutions on a software-defined network. The Lab is underpinned by a combination of technologies, including smart network configuration management, traffic management and software-defined access.
2. Run a limited trial of a software-defined network in a simulated Defence environment.
3. Connect researchers and world-class engineers from Cisco to explore new and promising technologies that are of strategic interest to Defence. The collaboration aims to expand into new areas of research to maximise technology impact.

Zero-trust architecture: Designing a network assuming you can't trust anything it connects to

The Critical Infrastructure Lab incorporates a strategic approach to security that centres on the concept of eliminating trust from an organisation's network architecture and offers a comprehensive solution to secure all access across your applications and environment, from any user, device and location.

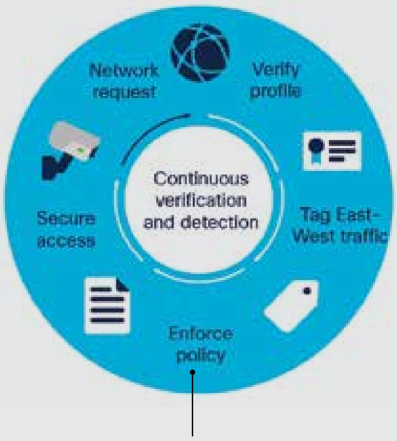
There are three pillars of zero-trust security:

Trusted Workforce
User-Device Access



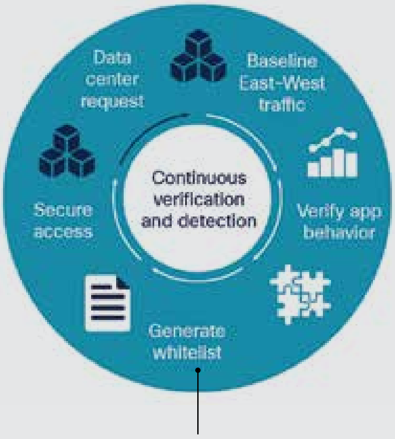
This pillar ensures only the right users and secure devices can access applications, regardless of location.

Trusted Workforce
IoT, Edge and Sensor Access



This pillar focuses on secure access when an API, a microservice or a container is accessing a database within an application.

Trusted Workloads
App and Data Access



This pillar focuses on secure access for all devices (including Internet of Things (IoT)) that connect to enterprise networks, such as user endpoints, physical and virtual servers, printers, cameras, HVAC systems, kiosks, infusion pumps, industrial control systems, and more.

The Critical Infrastructure Lab has a strong focus on network security and allows potential users to experiment with different tactics and methods of detecting changes in a network that might indicate a security breach. The testing of new tools and tactics is intended to augment a range of existing Cisco services that exist in this area. Users of the lab will have an opportunity to understand what's already possible in terms of detecting security issues in a network environment. Users will be able to test security of both IT and OT environments including networks that support industrial IoT applications.

Findings from the limited scope trial

The trial conducted as part of the collaboration focused on detection of changes in the network that might indicate a vulnerability. It intended to demonstrate how software-defined network architectures could potentially improve the speed to detection (and consequently limiting loss of both data and business continuity). The trial demonstrated the automated verification and deployment of firewall rules/policies to Cisco hardware via the University of Adelaide policy-based networking application.

What next?

Request a briefing to understand how the Critical Infrastructure Laboratory can be used to help develop, test and simulate cyber security investigations and responses.

How this project contributes to Australia's Defence agenda

The research that anchors this white paper is relevant to the Australian Defence Force's goal of securely operating and protecting military capability in and around its fixed base installations. Major learnings for Defence include the advantages offered by:

- A policy-based approach to securing users and endpoints
- "Provable network security" to guarantee that policies are secure and conflict-free
- Automation of network security orchestration
- Using a combination of tools to monitor changes in network performance
- Improved visibility into network operations.

The trial – and Lab environment – directly support and enable several specific information and communication technology (ICT) goals including:

- Protecting and securing Defence information and the information environment
- Providing accurate information for decision-making and military interoperability
- Standardising business processes, data and supporting applications
- Delivering reliable ICT services across fixed, deployed and mobile environments.

The Defence Context

> “While Joint Capabilities Group, CIOG and the individual Services focus on growing cyberspace capabilities, particularly Defensive Cyberspace Operations elements, manoeuvre commanders and their staffs must rapidly come to terms with the opportunities and threats inherent in cyber-enabled conflict if the Joint Force is to successfully face the security challenges of the 21st century.”[2]

Importance of secure networks in defence

The Australian Government has outlined three strategic objectives that are driving decisions and resourcing for Defence:

- **To shape Australia’s strategic environment**
- **To deter actions against Australia’s interests**
- **To respond with credible military force, when required**

These objectives are based on the requirement for Defence to maintain responsive and adaptable military capabilities in a complex technology environment that has a mix of legacy and new systems.

The network is the point at which all technologies coalesce in a Defence environment. Networks collect, aggregate and act on data at speed and scale to maximise operational advantage and increase efficiency. Data – and the network that underpins it – needs to be treated as a strategic asset that must be operationalised to empower more lethal and effective military capabilities.

Networks are increasingly at risk from a proliferation of cyber threats. With applications migrating to the cloud, defence systems coming online and a continually expanding threat landscape, networks are becoming increasingly vulnerable.

Scale of the cyber threat facing defence networks

In June 2020, Australian Defence Minister, Linda Reynolds, declared that malicious cyber activity was "increasing in frequency, scale, in sophistication and in its impact". Between 1 July 2019 and 30 June 2020, the Australian Cyber Security Centre responded to 2,266 cyber security incidents at a rate of almost six per day.[4]

The cyber security threat to Australia is not limited to individuals or SMEs. Military cyber threats are growing, with defence forces increasingly acknowledging cyber as a new battlefield. Nation states and state-sponsored actors are becoming increasingly sophisticated and well-resourced in their attempts to steal sensitive data or achieve destructive effects to Australia's national security and economy.

The defence sector has particular vulnerabilities from a cyber security risk perspective:

- A growing number of defence systems rely on edge computing and IoT, which increases attack surfaces
- Modern force structures – which are organised with mobility in mind – increase the complexity of defence systems and people
- Defence holds a goldmine of highly sensitive information, including Five Eyes intelligence and intellectual property related to emerging and next-generation defence systems and innovation.

The growing cyber threat requires significant and sustained investment in new technology and analytical capability to guard the integrity of information and ensure the successful conduct of operations. This is particularly the case from a networking perspective. Despite the importance of networks, a device-centric management focus still tends to prevail, leading to vulnerabilities at overlooked points in the network where policies are not enforced.

Challenges for defence in creating secure networks

A range of technical, organisational and personnel challenges creates complexities for the Defence sector in building cyber capability and responding to cyber security threats.

Technical challenges

Serious security misconfigurations are a common occurrence in networks [5,6]. Network configuration is difficult to get right for various reasons, including:

- The network configuration process is often complex and largely manual, which leads to errors and inefficiencies. For example, a large organisation such as an Australian university will configure and manage millions of distinct network policies across its networking infrastructure. Maintaining consistency and error-free configuration at such a scale using a largely manual process is challenging and rarely achieved.
- Low-level details such as IP addresses and port numbers need to be manually configured, and are often entered incorrectly.
- Environments often have equipment from multiple vendors, each with proprietary and device-specific configuration requirements. This adds further complexity and opportunity for errors in configuration.
- A device-centric management focus tends to prevail, leading to vulnerabilities at overlooked points in the network where policies are not enforced or configured correctly.
- Most importantly, a single device can contain thousands of rules: with any errors these rules can be in conflict.

The final item above is key. Every network device contains thousands of lines of low-level code, implementing hundreds of network level rules – all configured manually.

Organisational challenges

Current Australian Defence Force (ADF) cyberspace operational responsibility lies with J6 staff, although this is not reflected in doctrine. Planning and executing cyber-enabled warfare is beyond the scope of the role and responsibilities traditionally filled by J6 staff.

Joint Capabilities Group, CIOG and the individual Services are currently focusing on growing cyberspace capabilities, particularly Defensive Cyberspace Operations elements [7]. However, deployed forces are not currently prepared for the threats in cyber-enabled conflict [2]. Issues include the lack of a detailed cyber terrain model in relevant planning, operations and intelligence doctrine, and various models of cyberspace actions across Joint and Single Services.

People challenges

The interplay between policies is extraordinarily complex, and not something that can be managed by people alone. Yet this is precisely what is demanded from network managers. Network managers need to be empowered to verify that policies are conflict-free, and their networks are secure. This is especially important for network security where vulnerabilities are often unknown and policies to guard against possible attacks are not available.

Australia's cyber response to threats in defence

The Australian Government has committed significant resources to tackling cyber-security threats in Defence in the fixed and deployed domains. This includes new strategies, creation of entities to address issues and implementation of defensive cyber projects.

Strategies

A number of strategies are creating new and expanded policy frameworks for preparing for and managing cyber-security threats in Defence. These include:

- **2020 Force Structure Plan:** The 2020 Force Structure Plan [8] sets out adjustments to Defence capability plans and builds on investments made in the 2016 Defence White Paper. The plan lists five key capabilities, one of which is "improved capacity to respond to grey-zone activities, including cyber and information operation, strengthened operational cyber capabilities." "Grey-zone" activities are described [9] as military and non-military forms of assertiveness and coercion aimed at achieving strategic goals without provoking conflict.
- **More, together:** More, together is the national Defence Science and Technology (S&T) Strategy to 2030 and introduces the "STaR Shot" concepts [10]. The eight STaR Shots represent a change in direction in the national S&T enterprise, by focusing on larger and fewer Defence objectives to deliver "leap-ahead" capabilities. The strategy provides a clearer pathway to take innovative ideas from the laboratory and into the hands of the war-fighter. One of the STaR Shots is Information Warfare, signifying that cyber security has the highest priority within Australian Defence S&T.
- **Defence ICT Strategic Direction 2016-2020:** The Defence ICT Strategic Direction 2016-2020 [11] from the Chief Information Officer Group (CIOG) outlines seven priorities, including: "Implement contemporary cyber security capabilities to protect the flow of information from threats."
- **Australia's Cyber Security Strategy 2020:** This strategy [12] outlines a spend of $1.67B over 10 years to achieve a number of aims, including protecting and actively defending the critical infrastructure that all Australians rely on, stronger defences for Government networks and data, greater collaboration to build Australia's cyber skills pipeline, and stronger partnerships with industry through the Joint Cyber Security Centre program.

Entities

The following organisations are working together to understand current threats and implement measures to prevent, detect and respond to those threats.

- **Australian Signals Directorate (ASD):** ASD defends Australia from global threats and advances our national interests through foreign signals intelligence, cyber security and offensive cyber operations. Australia's Cyber Security Strategy 2020 will invest $118 million to expand ASD's data science capabilities.[12]
- **Australian Cyber Security Centre (ACSC):** The ACSC – which is based within the Australian Signals Directorate – leads the Australian Government's efforts to improve cyber security, including by providing advice and information on emerging cyber threats and protections.
- **Joint Capabilities Group:** The Joint Capabilities Group – which consists of the Information Warfare Division and Joint Information Warfare Facility – is critical to ensuring the capacity and relevance of the ADF's defensive cyber options capability.

Defensive cyber projects

The following joint projects are focused on actively defending Australia from cyber threats:

- **Joint Project 9131:** This project aims to defend deployed networks and combat platforms against rapidly evolving cyber threats. Under Joint Project 9131, Minister for Defence Linda Reynolds said, in announcing the new allocation last year, the Government was funding the construction of a “modern, purpose-built” Joint Information Warfare Facility (JIWF), based in the ACT. That C4 (joint command, control, communications and computers) facility – billed as a “force multiplier” ¬– will support a range of training, tools, and infrastructure deemed “crucial to ensuring the capacity and relevance of the ADF’s defensive cyber operations capability”.
- **Joint Project 2068:** JP 2068 is a multi-phased proposal to progressively develop a survivable Defence Network Operation Centre capability, which will enable Defence to more effectively manage, monitor and secure its major communications networks and information systems.

While these responses are critical in the face of the growing cyber threat Australia faces, to date there has been less focus on the role of networks from a cyber security perspective. Ensuring Australia’s Defence forces have modern and secure networks is essential to accelerating the nation’s cyber resilience.

About this project

Context for this project

Today's military environment is data-centric and increasingly reliant on secure, robust and scalable networks. The network collects, aggregates and acts on data at speed and scale to maximise operational advantage and increase efficiency. Data – and the network that underpins it – needs to be treated as a strategic asset that must be operationalised to empower more lethal and effective military capabilities. It must be built upon a secure platform from the edge to the cloud, across multiple domains, and in a way that enables the flexible and secure movement of sensitive information and communications anywhere, anytime, in any mission environment in order to deliver a number of fundamental capabilities:

- **Data where it's needed at mission speed.** Mission-grade visibility, information access, enhanced situational awareness and security across the network operations platform.
- **Intelligent orchestration and automation.** Automated provisioning, monitoring and management (from a single platform) at scale for all users and devices aligned with Defence's business needs and current operational intent.
- **Resilience of critical infrastructure.** Proactive critical infrastructure monitoring, analytics and optimisation to execute actions at high velocity and support mission-critical services and resources at scale.
- **Comprehensive security.** Integrated, AI-driven, end-to-end security improving incident prevention/detection, automates/coordinates response and simplifies security operations.

Broad objectives of this project

To further accelerate Australia's response to growing cyber threats in the defence sector, Cisco and the University of Adelaide sought to better understand and investigate the benefits of software-defined networks in a Defence context.

Securing Australia's defence sector requires new intent-based networks that automate routine tasks, use analytics to help IT make informed decisions, and embed security into the network. Cisco and the University of Adelaide have developed the notion of a Critical Infrastructure Lab that describes exactly this: a Defence installation / operational environment that is underpinned by software-defined, secure network infrastructure that can be remotely configured and managed.

Specific focus areas for this Project

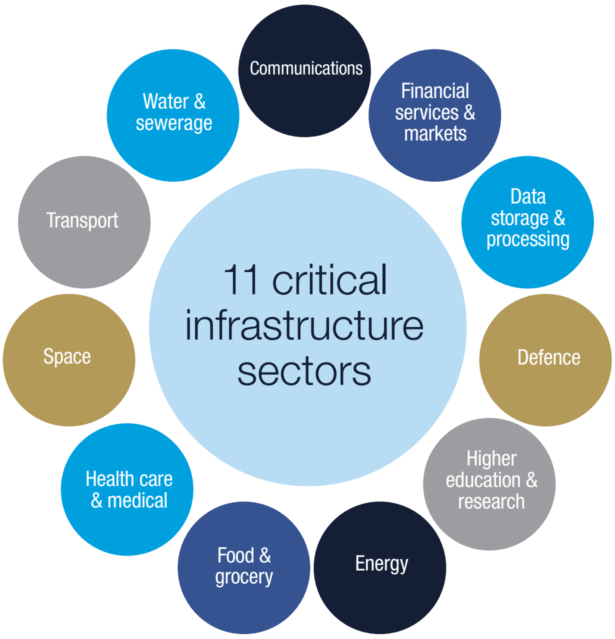
1. Design an operational, purpose-built laboratory environment for testing networks (the Critical Infrastructure Lab).
2. Conduct a limited trial of a software-defined network that mimics Defence characteristics.
3. Creating a platform for researchers to collaborate on.

Section 1: The Critical Infrastructure Lab

Purpose of the Critical Infrastructure Lab

The Critical Infrastructure Lab has been designed as a test facility for Defence and other critical infrastructure applications. The laboratory is built on a Cisco software-defined network infrastructure with potential for additional functionality to be added.

The Critical Infrastructure Lab focuses on network security and allows potential users to experiment with different tactics and methods of detecting changes in a network that might indicate a security breach. The testing of new tools and tactics is intended to augment a range of existing Cisco services that exist in this area. Users of the lab will have an opportunity to understand what's already possible in terms of detecting security issues in a network environment. Users will be able to test security of both IT and OT environments including networks that support Industrial IoT applications.



11 critical infrastructure sectors
Communications
Financial services & markets
Data storage & processing
Defence
Higher education & research
Energy
Food & grocery
Health care & medical
Space
Transport
Water & sewerage

Why Focus on Critical Infrastructure?

The Australian Government has committed to protecting the essential services all Australians rely on by uplifting the security and resilience of critical infrastructure. Critical infrastructure is "those physical facilities, supply chains, information technologies and communication networks, which if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic wellbeing of the nation, or affect Australia's ability to conduct national defence and ensure national security". [13]

Australia's critical infrastructure includes networks of electricity, communication, gas and water assets, as well as physical facilities such as maritime ports. It includes both public and private infrastructure. Only assets that are essential to the functioning of Australia's society and economy are deemed critical infrastructure. Disruption to Australia's critical infrastructure could result in a loss of operational continuity that threatens the availability and uptime of essential services. Now more than ever, owners and operators of critical infrastructure need advanced cyber protections and capabilities to automatically respond in the event of an attack.

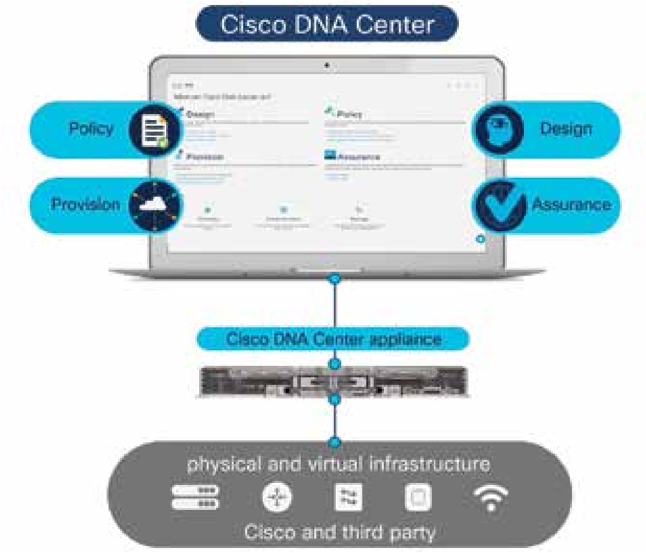
The Australian Government has defined 11 critical infrastructure sectors, including defence industries. Each of these sectors has unique challenges, threats and potential responses in terms of cyber security but share an interest in being able to test and validate security in a protected environment before moving to mass deployment.

Technologies deployed within the laboratory

A combination of technologies have been integrated to form the underlying platform for the Critical Infrastructure Lab. The laboratory is operated by the University of Adelaide with support from Cisco. The deployed network infrastructure is fully programmable, open to third-party innovation and integrates with cloud components.

At the core of the lab is:

- **A Cisco Firepower 4110 next-generation firewall,** a security platform that supports flow-offloading, programmatic orchestration, and management of security services with RESTful APIs.
- **Dedicated Compute Node,** for hosting the University of Adelaide policy-defined networking application code as well as the Cisco Identity Services Engine (ISE) and the Cisco Secure Firewall Management Center (FMC).
- **Cisco Digital Network Architecture (DNA),** which facilitates simple, automated and programmatic deployment of network services. It brings the notion of user– and application–aware policies into the foreground of network operations.
- **Cisco DNA Center,** with four sections aligned to IT workflows:
  - *Design:* Ability to design network for consistent configurations by device and by site. Physical maps and logical topologies help provide quick visual reference.
  - *Policy:* Ability to translate business intent into network policies and apply those policies, such as access control, traffic routing and quality of service, consistently over the entire wired and wireless infrastructure.
  - *Provision:* Provisioning in a simple user interface once policies are created.
  - *Assurance:* Cisco DNA Assurance, using AI/ML, to enable every point on the network to become a sensor, sending continuous streaming telemetry on application performance and user connectivity in real time.



Through the combination of technologies deployed at the lab, users are able to investigate and test three important technology capabilities:

- **Smart network configuration management**
- **Smart network traffic management**
- **Software-defined access**

1. Smart network configuration management

Smart network configuration management enables automatic detection and correction of network configuration issues, and ability to demonstrate the provable properties of generated configurations. To support enhanced security, policy consistency and modern defence network deployment, Cisco and the University of Adelaide trialled two specific technologies in the Lab:

i. Cisco Digital Network Architecture (Cisco DNA): This is an intent-based networking approach that allows for end-to-end programmability at scale. This technology enables networking environments to react to changing mission requirements, whether event-driven, planned or strategic.

ii. Provable Network Security: This first-generation configuration tool models network policies in a "metagraph" [14] (a special type of directed hypergraph) and automatically analyses and generates provable secure network configuration code. This delivers two important capabilities to the Critical Infrastructure Lab:

- Formal verification of compliance with cyber-security best practices and guidelines: The Australian Government Information Security Manual (ISM), issued by the Australian Signals Directorate (ASD), provides agencies with a set of detailed controls that can be implemented to mitigate risks to their information and systems. The PNS approach provides a formal method to evaluate compliance with these cyber security best practices and guidelines.
- Continuous update of the network security implementation against security controls: Networks are not static. They dynamically change to service users' needs. For example, new applications require new privileges and open ports, and security group memberships change to accommodate business requirements. The PNS approach can continuously monitor the network for configuration change, check for correctness of the updates, and automatically roll out new verified changes.

These technologies offer a number of potential benefits to Defence including:

- Ability to audit network security configuration
- Ability to identify policy inconsistencies, conflicts and non-compliances
- Ability to locate the root causes of security configuration issues
- Auto-generating correct / compliant network configurations from high-level policies.

2. Software-defined access

The current rigid and largely manual lifecycle management approach to networking is not sustainable for deploying, maintaining and updating networks, particularly in complex environments such as Defence.

To provide for a more effective approach to networking, Cisco and the University of Adelaide deployed several capabilities at the Lab that work in unison with PNS and FLIMSY to enhance the security, policy consistency and deployment of modern defence networks:

- **Network automation:** Simplified network operations through a single point of automation, orchestration and management of network policy functions using Cisco DNA Center.
- **Single Network Fabric** SD-Access to free policy constructs from the underlying infrastructure such as IP addresses, VLANs, ACLs, etc. This divides the enterprise network into two different layers, each for different objectives.
- **Enhanced visibility** by using advanced analytics for user and device identification and compliance. This employed artificial intelligence and machine-learning techniques to classify similar endpoints into logical groups.
- **Policy analytics** that provide a thorough analysis of traffic flows between groups to define the right group-based access policies.
- **Secure segmentation** that automatically sets up both wired and wireless network devices for granular two-level segmentation for zero-trust security and regulatory compliance.
- **Trustworthy systems** that protect against counterfeit hardware and software modification. Key trustworthy technologies included image signing, secure boot, runtime defences, and security capabilities in the Trust Anchor module such as Random Number Generation (RNG) and crypto support, secure storage, and Secure Unique Device Identifier (SUDI).

These capabilities offer a number of potential benefits to Defence including simplified deployment of new network devices, automated network segmentation and group-based policy and contextual insights for fast issue resolution and capacity planning. The other advantage for defence is the capacity to create open and programmable interfaces for integration with third-party solutions. There is also potential to expand the focus of work to include smart network traffic management which looks to optimise the performance of the network through control of traffic rates and access control. This is especially important for forward-deployed personnel where small windows of network connectivity may occur. In these cases, careful control needs to be applied in order to maximise connectivity over these intermittent, contested or impoverished links. This technology offers a number of potential benefits to Defence including:

- Precise information management such that the value of the limited communications opportunities afforded to the deployed units is maximised
- An extremely lightweight solution that minimises space, weight and power (SWaP) impact, adds minimal complexity to the ICT infrastructure by being a largely independent, lightweight application running a deployed interface server
- A solution that is highly reconfigurable
- More responsiveness to changing requirements real-time reconfiguration
- A user-friendly interface that can be operated by a non-networking specialist.

Services offered in the Critical Infrastructure Lab

The lab will offer a range of potential services to operators of critical infrastructure and ecosystem partners. The services are divided into three categories:

1 Ideation and scenario planning

The lab will be available to organisations to assist in understanding their current risks, potential solutions and exploration of a range of potential scenarios related to their specific context. These services would target executive and technical staff and involve subject matter experts from the University of Adelaide, Cisco and other specialist organisations as required. Not all organisations would move to Stage 2.

2 Deep dives and validation of specific network and security solutions

The lab's greatest value is the capacity to replicate an organisation's technology environment and test potential solutions. A similar service is currently offered by Cisco through its Customer Experience Centres (known as the CPOC program). The process for validating specific solutions at the Lab would be as follows:

- Diagnostic of the organisation's challenges and risks. This is generally done through a combination of surveys and interviews and culminates in a workshop
- Options mappings as part of the discovery process. Once the potential vulnerabilities and gaps have been identified a range of potential options would be developed including architectural responses and potential point solutions
- Replicating the organisation's current technology environment. The lab is designed to allow potential solutions to be tested in a simulated environment. This includes simulating current network infrastructure in place, cloud services (and even individual providers of those technologies) currently used by an organisation and a range of other relevant equipment including end points that need to be supported. The lab would then stand up a simulated version of that environment.
- Testing in real time. Organisations would visit the lab and test solutions in the simulated environment and better understand how it works in practice, what issues arise and whether the approach is likely to generate intended benefits. This process would culminate in a formal test report and next steps.

3 Bespoke solution development

The lab would be capable of designing, developing and conducting research into bespoke solutions that do not currently exist in the market. These solutions would be co-developed with industry partners and government agencies that have a requirement for highly customised solutions. These solutions would be nested within and be designed to interoperate with the Cisco technology environment.

Section 2: Research Trial

Overview of the trial

The project involved conducting a trial within the Critical Infrastructure Lab, with a focus on detecting changes in the network that might indicate a vulnerability. It demonstrated how software-defined network architectures could potentially improve the speed to detection (and consequently limit loss of both data and business continuity).

The trial focused on automated verification and deployment of firewall rules/policies to Cisco hardware via the University of Adelaide policy-based networking application. Our testing of deployed policies was performed using wired and wireless equipment/devices within the Critical Infrastructure Lab environment.

Findings from the trial

The results from the trial revealed that software-defined networking creates a range of benefits for defence organisations that contribute to higher order strategies:

Security

The Critical Infrastructure Lab environment is based on a zero-trust architecture and recognises that protection of data and business continuity are non-negotiable. The University of Adelaide provable network security algorithms built into the policy-defined networking application allow a network manager to perform continuous verification of policy consistency and compliance. This is a first-generation configuration tool that models network policies in a "metagraph" [14] (a special type of directed hypergraph) and automatically analyses and generates provable secure network configuration code.

Speed of deployment

The technologies deployed in the Critical Infrastructure Lab offer the prospect of improved speed of deployment. The University of Adelaide policy-defined networking application can bulk-import, analyse, verify and deploy network policies via simple interactions with a web interface, removing many manual steps in the deployment and verification process.

> "Defence needs to ensure it is alert and adaptable to opportunities presented by new technology" [8]

Simplicity to configure, manage and make dynamic changes in the network

As indicated in the context section, the configuration and management of networks has become increasingly complex. This complexity is driven by a number of factors including multi-vendor environments, legacy applications and an increased number of rules and policies that need to be applied. The software-defined access technologies allow security to be driven at a policy level. The University of Adelaide policy-defined networking application provides a mechanism to perform consistency and compliance checks automatically without the need for manual inspection of complex and large configuration files, hence greatly simplifying the process of configuring and validating firewall settings and reducing security risks associated with manual ad hoc interventions.

Improved visibility and awareness

If you can't **see** it you can't measure it, respond to it or manage it. A range of tools were used to assist in providing greater visibility into the network environment. By observing changes in the network – and earlier – Defence organisations can introduce threat tactics and minimise potential losses or vulnerabilities. Cisco management interfaces provide visibility into the deployed configurations and the University of Adelaide policy-defined networking application provides automated visibility on the correctness and compliance of the configurations with respect to the security management intent.

Section 2: Implications

While Defence owns and operates highly secure networking infrastructure using high-end encryption technology, Defence networks suffer the same problems of error-prone approaches to configuration and management of network infrastructure that all organisations experience because of the sheer complexity of today's networks.

The technology deployed in the Critical Infrastructure Lab offers a solution to this conundrum through the use of mathematically provable policy configuration and automated control of network infrastructure. The technology is vendor agnostic, scales seamlessly, and can be used to rapidly adapt a network's security posture in response to evolving threats.

Relevance of the findings to specific Defence organisations and projects

The research is particularly relevant to the Defence Terrestrial Communications (JP2047) project and other core network infrastructure programs in DSTG (Defence Science and Technology Group) and the Intelligence agencies. There is potential that research will extend to the deployable infrastructure projects such as JP 2072 (BCS-L), Sea 1442, Sea 2273 and others. Getting these foundational infrastructure projects aligned to the research is also a critical enabler for all of the C2, ISREW, Logistics, Personnel and Corporate applications that transcend the Cyber and Information domain. Given that JP 2047 is closing on full operational capability and therefore coming to an end in terms of its initial contractual phase, the research should help to inform core communications project planning and execution. An example of a project that could leverage the research is the Defence Secret Network (DSN) refresh next-gen warfighting network program.

Implications of the research

Operations

- The importance of an end-to-end view of all networks.
- Updating all Joint and Single Service planning, operations, intelligence and communications with a singular domain model to enable visualisation of actions in and through the cyberspace.
- The inclusion of a detailed cyber terrain model in relevant planning, operations and intelligence doctrine, and the inclusion of cyber domain planning considerations across all relevant Joint and Single Service Doctrine.

Technology

- The importance of software-defined networks that are highly automated, remotely configurable and policy-based.
- Architecting for cyber security rather than relying on endpoint security.

Skills, people and training

- A strategic approach to cyber security skills involving collaboration between government, industry and education providers.
- Implementation of a sovereign Cyber Operations Planning Course into all joint professional military education and office training continuum courses.

Request more information or a briefing

Prof. Michael R Webb

Director, Defence & Security Institute
Academic Coordinator, Defence, Cyber & Space
The University of Adelaide
m.webb@adelaide.edu.au

Chris Miles

Chief Architect, Federal and Defence, Cisco
chmiles@cisco.com

References

1. Australian Government media release, *Stronger cyber defences for deployed ADF networks*, 12th August 2020; Available from: https://www.minister.defence.gov.au/minister/lreynolds/media-releases/stronger-cyber-defences-deployed-adf-networks
2. Wardrop, C., *Victory in the Age of Cyber-Enabled Warfare*, 11th March 2021; Available from: https://theforge.defence.gov.au/publications/victory-age-cyber-enabled-warfare#ftnt30
3. Available from: https://www.theguardian.com/australia-news/2020/jun/19/australia-cyber-attack-attacks-hack-state-based-actor-says-australian-prime-minister-scott-morrison
4. Available from: https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf
5. Wool, IEEE Computer, 2004.
6. Ranathunga D., Roughan M., Nguyen, H., Kernick P. and Falkner N., SCADA *Firewall Configurations and the Implications for Best Practices*, IEEE Transactions on Network and Service Management, 2016, 13(4), p. 871-884.
7. Braue, D. *Defence Consolidates cyber capabilities*, Information Age, August 2020; Available from: https://ia.acs.org.au/article/2020/defence-consolidates-cyber-capabilities.html
8. Australian Government, *2020 Force Structure Plan*; Available from: https://www1.defence.gov.au/sites/default/files/2020-11/2020_Force_Structure_Plan.pdf
9. A. Coyle and H. Nguyen, P. Boyd, G. Judd, *Improving the Performance of Land Tactical Digital Networks Using Measures of Network Capacity*, http://www.milcis.com.au/s/2018-1-8c1.pdf
10. Australian Government, *Science, Technology and Research (STaR) Shots*; Available from: https://www.dst.defence.gov.au/strategy/defence-science-and-technology-strategy-2030/science-technology-and-research-star-shots
11. Australian Government, *Defence ICT Strategic Direction 2016-2020*; Available from: https://www.defence.gov.au/CIOG/_Master/docs/Defence-ICT-Strategic-Direction-2016-2020.pdf
12. Australian Government, *Australia's Cyber Security Strategy 2020*; Available from: https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf
13. Available from: https://www.homeaffairs.gov.au/reports-and-pubs/files/protecting-critical-infrastructure-systems-consultation-paper.pdf
14. *Clear as MUD: Generating, Validating and Applying IoT Behaviorial Profiles*, Hamza A., et al. (2018), accepted to appear in ACM SIGCOMM 2018 Workshop on IoT Security and Privacy (IoT S&P), August 2018