| Time   | Session 1.1 | Session 1.2 | Session 1.3 | Session 1.4 | Session 1.5a | Session 1.5b | Session 1.5c | Session 1.6a | Session 1.6b | Session 1.7a | Session 1.7b | Session 1.8a | Session 1.8b | Session 1.9a | Session 1.9b | Session 1.9c |
|--------|-------------|-------------|-------------|-------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|
| 08:00am |  | Welcome: Professor Michael Frater, Rector UNSW Canberra and Dr Peter Lawrence, Chief Information Officer, CIOG | Keynote Address: Mr Aiyaswami Mohan, Chief Technology Officer, CIOG | Keynote Address: Mark Loucks, Senior Data Scientist Advanced Data Analytics, Unisys; and John Kendall, Border Security Program Director, Unisys | (Dr Bernard Meyerson, IBM) | (LTGEN Robert M. (Bob) Shea, USMC (Ret.), President and CEO, APCEA International) | (Mr Kevin Zuccato, IBM) | (Mr Robert Kremer, Kinexus, formerly Kinetic Recruitment) | (Mr Kim Fritsche, Adobe and Mr Phil Cutforth, The Department of Internal Affairs) | (Mr Richard Brown, Cogito Group Pty Ltd and Mr Phil Cutforth, The Department of Internal Affairs) | Paper 2: Achieving the Single Information Environment | Paper 2: Performance Enhancement of LTE-HetNet utilizing Asynchronous ABSF Configuration Combined with Horizontal Sector Offset and Vertical Beam Forming | Paper 2: A Heterogeneous Software Defined Networking Architecture for the Tactical Edge | Paper 2: Introducing Tactical to Enterprise Integration |
| 10:00am | Morning Tea |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 11:00am |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 12:30pm | Lunch |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 1:30pm | Session 1.1 | Session 1.2 | Session 1.3 | Session 1.4 | Session 1.5a | Session 1.5b | Session 1.5c | Session 1.6a | Session 1.6b | Session 1.7a | Session 1.7b | Session 1.8a | Session 1.8b | Session 1.9a | Session 1.9b | Session 1.9c |
| 2:30pm |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 3:30pm |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 4:00pm |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 5:00pm | Welcome Networking Drinks |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

Exhibition runs from 7:30am to 6:30pm (open to exhibition-only registration from 1:30pm to 4:30pm) / IEEE Stream (Refereed papers) co-sponsored by IEEE
<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>07:30am</td>
<td><strong>Session 2.1</strong></td>
<td>Breakfast Session—Exhibition open and coffee available</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Product Brief (Ballroom): Social Media and Open Source Intelligence, Mr David Waxman, IBM Chief Architect: Project Aurora</td>
</tr>
<tr>
<td>09.00am</td>
<td><strong>Session 2.2</strong></td>
<td>Plenary Session: FYEY CIO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Keynote Address: Dr Peter Lawrence, AU CIO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Keynote Address: Mr Terry Halvorsen, US DOD CIO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Keynote Address: Mr Mike Stone, UK MOD CIO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Keynote Address: Mr Len Bastien, Assistant Deputy Minister Information Management</td>
</tr>
<tr>
<td>10.30am</td>
<td>Morning Tea</td>
<td></td>
</tr>
<tr>
<td>11.00am</td>
<td><strong>Session 2.3</strong></td>
<td>Plenary Session: FPR and GIS Joint Interoperability</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Moderator: AVM Andrew Dowse, HICTO, CIOG</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Keynote Address: BRIG John Gould, DG C4, VCDG Group</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Keynote Address: CAPT Stephen Dryden, RAN, DG Navy Communications &amp; Information Warfare</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Keynote Address: COL James Murray, Director Land C3 Program, G6 Army HQ</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Keynote Address: GPCAPT Glenn Nattrass, Director Networks, Air Force</td>
</tr>
<tr>
<td>12.30pm</td>
<td>Lunch</td>
<td></td>
</tr>
<tr>
<td>13.00pm</td>
<td><strong>Session 2.4</strong></td>
<td>Product Brief: Operational Information Management: What you need to know about security, data fusion, interoperability and future trends (Mr Scott Marshall and Mr Richard Armstrong, Berkeley IT)</td>
</tr>
<tr>
<td>1.30pm</td>
<td><strong>Session 2.5a</strong></td>
<td>Product Brief: C2 Solutions for the Warfighter: Latest Capabilities in Enterprise Information Management Across Multi-level Domain Environments Securely (Mr Phil Hawthorne and Mr Richard Armstrong, Berkeley Solutions)</td>
</tr>
<tr>
<td></td>
<td><strong>Session 2.6a</strong></td>
<td>Product Brief: Smart Battle Management Command and Control (COL Lynn Wills (Rtd), Ultra Electronics, ATS)</td>
</tr>
<tr>
<td></td>
<td><strong>Session 2.7a</strong></td>
<td>Update: Australian Land Vehicle C4I Specification Development (Mr Will Blake, Australian Department of Defence)</td>
</tr>
<tr>
<td></td>
<td><strong>Session 2.8a</strong></td>
<td>Product Brief: Transforming Defence Deployed Networks with the Cisco Digital Network Architecture (Mr Will Blake, Cisco)</td>
</tr>
<tr>
<td></td>
<td><strong>Session 2.9a</strong></td>
<td>Product Brief: Secure Replication Across Domains (Mr Perry Smith, Myriad Technologies)</td>
</tr>
<tr>
<td>2.30pm</td>
<td><strong>Session 2.5b</strong></td>
<td>Update: Airborne Mobile Broadband Communications (Mr Joseph Johnson, VisaSat)</td>
</tr>
<tr>
<td></td>
<td><strong>Session 2.6b</strong></td>
<td>Product Brief: Next Generation Mobile Intelligence: Tactical Field Applications (Mr Mark Vardy, Motorola Solutions Australia)</td>
</tr>
<tr>
<td></td>
<td><strong>Session 2.7b</strong></td>
<td>Update: The Next Generation Protected Mobility Vehicle (COL John McLean, LTCOL Steven Welsh, Mr Cameron Botterill)</td>
</tr>
<tr>
<td></td>
<td><strong>Session 2.8b</strong></td>
<td>Product Brief: High Performance Situational Awareness with LuciadLightspeed and LuciadRIA (Dr Bart Adams, Luciad)</td>
</tr>
<tr>
<td></td>
<td><strong>Session 2.9b</strong></td>
<td>Tutorial: Putting SharePoint at Sea (Mr Perry Smith, Myriad Technologies)</td>
</tr>
<tr>
<td>3.30pm</td>
<td>Afternoon Tea</td>
<td></td>
</tr>
<tr>
<td>4.00pm</td>
<td><strong>Session 2.5c</strong></td>
<td>Tutorial: Iridium NEXT – Vision for the Truly Global Satellite Communications (Mr Nihal Fernando, Arthur Otlet and Jeff Detwiler, Thales Australia)</td>
</tr>
<tr>
<td></td>
<td><strong>Session 2.6c</strong></td>
<td>Update: Extreme Profiling – Hunting for Bad Actors in Social Media Data (Mr Clement Fredembach, Teradata)</td>
</tr>
<tr>
<td></td>
<td><strong>Session 2.7c</strong></td>
<td>Update: Defence Spectrum Update (Mr David Murray, Defence Spectrum Office)</td>
</tr>
<tr>
<td></td>
<td><strong>Session 2.8c</strong></td>
<td>Product Brief: Defeating Insider Threats with Identity-Based Security (Mr Jon Green, Aruba)</td>
</tr>
<tr>
<td></td>
<td><strong>Session 2.9c</strong></td>
<td>Tutorial: Building Electronic Forms and Workflows to Streamline your Business Processes (Mr Nathan Pearce, Myriad Technologies)</td>
</tr>
<tr>
<td>7.00pm–11.00pm</td>
<td>Conference Dinner</td>
<td>(7:00pm for 7:30pm) Exhibition runs from 7:30am to 5:00pm (open to exhibition-only registration from 1:30pm to 5:00pm)</td>
</tr>
</tbody>
</table>
**Day 3—Thursday 10 November 2016**

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Title</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>07:30am</td>
<td>Session 3.1</td>
<td>Breakfast Session—Exhibition open and coffee available</td>
<td>Product Brief (Ballroom): The Role of Industry in Collaborative Cyber Security Threat Intelligence, Mr Gary Hale, Director, Cyber Security &amp; Innovation, Security &amp; Trust Organisation, Cisco, Australia and New Zealand</td>
</tr>
</tbody>
</table>
| 08:00am| Session 3.2| Plenary Session: Defence Cyber                                       | Keynote Address: Mr Michael Scotton, Assistant Secretary Cyber Security, Australian Cyber Security Centre  
|        |           |                                                                     | Keynote Address: Mr Chris Brookes, Assistant Secretary ICT Security, CIOG |
|        |           |                                                                     | Keynote Address: CDRE David Scott, RAN, DG Joint Environment Warfare, VCO Group |
| 10:30am| Morning Tea| Morning Tea                                                          |                                                                        |
| 11:00am| Session 3.3a| SecureCanberra Welcome Address: (ISO²)                               | Update: ABCA Armies CIS Update (ABCA representatives)                 |
|        |           | Presentations: Prisoners Immunity and Bees—How Collaboration Works in Information Security | Mr Craig Searle, CISSP, Chief Apiarist, Hivint, Australia |
| 12:00pm| Session 3.3b| SecureCanberra Cybersecurity—What Have We Missed?                   | Update: Evolving Core Communications Considerations for Planners     |
|        |           | (Mr Chuan-Wel Hoo, IBM Asia-Pacific)                                 | (LTCOL Michael King, HQ JOC)                                           |
| 1.00pm | Lunch     | Lunch                                                                |                                                                        |
| 2.00pm | Session 3.3c| Product Brief: Omni Channel Operator Engagement                       | (Mr David Lincourt, Vice President, Field Services – Global Defense Industry Business Unit, SAP) |
| 3.00pm | Session 3.3d| SecureCanberra Containment vs Prevention—Realistic Strategies for Dealing with Cybersecurity Threats | Update: Army’s Land Network Battle Lab (LNBL)                         |
|        |           | (Mr John Kendall, Unisys Global Public Sector)                       | (Mr Tom Schar, LNIC)                                                   |
| 4.00pm | Afternoon Tea| Afternoon Tea                                                       |                                                                        |
| 4.30pm | Session 3.3e| SecureCanberra Securing the IoT: Convergence of Anomaly Detection & Device Security | Update: Analysis of HAMEL 16 Data                                    |
|        |           | (Mr Nick Savvides, Symantec)                                         | (FLTLT Siti Ravindran, LNIC)                                          |
|        | Session 3.4a| SecureCanberra Product Brief: Linear User, Data, and Network Defence in a Multi-Level Environment | (Mr Steve Stratton, Forcepoint)                                       |
| 4.30pm | Session 3.4b| SecureCanberra Product Brief: Exploiting the Data Deluge with a Unified Data Architecture | (Mr Ross Farrelly, Teradata)                                          |
| 4.30pm | Session 3.4c| SecureCanberra Product Brief: Streamline User, Data, and Network Defence in a Multi-Level Environment | (Mr Simon Barker, Airbus Defence and Space and Ashley Neale, Speedcast) |
| 4.30pm | Session 3.4d| SecureCanberra Product Brief: How Skynet 5 Can Complement WGS with Military Grade X-Band, Enhancing Australia’s Operational Effectiveness | (Dr Suzette Johnson, Agile Center of Excellence, Northrop Grumman Corporation) |
| 4.30pm | Session 3.4e| SecureCanberra Product Brief: ISR Information Sharing: Data, Entities, and Objects in Context | (Mr William Sokol, MarkLogic and Mr David Eastman, Esri Australia) |
| 4.30pm | Session 3.4f| SecureCanberra Product Brief: Taking Text from Files to Actionable Information | (Mr Anthony Karkainen, Northrop Grumman) |
| 4.30pm | Session 3.5a| SecureCanberra Product Brief: How Skynet 5 Can Complement WGS with Military Grade X-Band, Enhancing Australia’s Operational Effectiveness | (Mr Simon Barker, Airbus Defence and Space and Ashley Neale, Speedcast) |
| 4.30pm | Session 3.5b| SecureCanberra Product Brief: Streamline User, Data, and Network Defence in a Multi-Level Environment | (Mr Simon Barker, Airbus Defence and Space and Ashley Neale, Speedcast) |
| 4.30pm | Session 3.5c| SecureCanberra Product Brief: How Skynet 5 Can Complement WGS with Military Grade X-Band, Enhancing Australia’s Operational Effectiveness | (Mr Simon Barker, Airbus Defence and Space and Ashley Neale, Speedcast) |
| 4.30pm | Session 3.5d| SecureCanberra Product Brief: How Skynet 5 Can Complement WGS with Military Grade X-Band, Enhancing Australia’s Operational Effectiveness | (Mr Simon Barker, Airbus Defence and Space and Ashley Neale, Speedcast) |
| 4.30pm | Session 3.5e| SecureCanberra Product Brief: How Skynet 5 Can Complement WGS with Military Grade X-Band, Enhancing Australia’s Operational Effectiveness | (Mr Simon Barker, Airbus Defence and Space and Ashley Neale, Speedcast) |

Exhibition runs from 7:30am to 2:00pm (NO exhibition-only registrations available)
Session Abstracts: Day 1—9 November 2016

1.1 Breakfast Session

The Exhibition is open and coffee is available in the Exhibition Hall.

1.2 Plenary Session—Opening Session

Welcome: Professor Michael Frater, Rector UNSW Canberra and Dr Peter Lawrence, Chief Information Officer, CIOG

Keynote Address: Dr Peter Lawrence, Chief Information Officer, CIOG

1.3 Plenary Session: CIO Session

Keynote Address: Mr Aiyaswami Mohan, Chief Technology Officer, CIOG

Keynote Address: AVM Andrew Dowse, Head ICT Operations, CIOG

Keynote Address: Mr Andy Start, Inmarsat

1.4 Lunch Session Product Brief: Overcoming the Challenges of Network Micro segmentation from Design to Execution and Management

Presented by: Mr Mark Loucks, Senior Data Scientist Advanced Data Analytics, Unisys; and Mr John Kendall, Border Security Program Director, Unisys

Network micro segmentation should be a foundational tool in minimising both internal and external malicious cyber threat risk. The concept is sound but the execution and management of network segmentation can be extremely challenging. Coming up with the correct segmentation is extremely challenging due to the complexity of even a simple network. Today advanced machine learning models are being utilized by Unisys to let the actual data tell the story of how best to segment your network. How network data is flowing and how endpoints utilise resources tells the most accurate story for determining the best segmentation strategy. The amount of data is overwhelming to apply standard analytics to answer the question. Advanced machine learning models applied to the problem provide a clear micro segmentation view for both the initial development as well as the ongoing management of your network segmentation. Since the model can continue to learn and provide dynamic output you can monitor and understand when and how to best adapt the network schema to reflect changes in the network.

Applying the rules with Unisys Stealth software which substitutes traditional hardware topology for software-based cryptography, Unisys Stealth micro segmentation solutions prevent unauthorised access to sensitive information and reduce the attack surface, thereby making endpoints invisible to unauthorised users (including DBA’s). The overall solution from modelling to cryptography provides the highest level of security for you network.

1.5a Update: Information Technology's Tectonic Shift

Presenter: Dr Bernard Meyerson, Chief Innovation Officer, IBM

Information Technology has followed a steady path over the past decades, powered in large part by the "engine" we recognize as Moore's Law. However, as technology elements have progressed below the dimensions at which quantum mechanical effects prevent their further use, no significant benefit is seen with each technology generation. At the same time, the explosive growth of data availability via the IoT, SigInt, and other sources, demands far more processing "horsepower" than ever before if one is to put such vast reservoirs of data to any useful purpose. This talk will cover the transformation that system technology, architecture, and "intelligence" must undergo to remain relevant to the challenges we now face.

1.5b Update: 20 Years of Cyber Observation

Presenter: LTGEN Robert M. (Bob) Shea, USMC (Ret.), President and CEO, AFCEA International

Lieutenant General Shea is the President and CEO of AFCEA International, a global association with over 130 chapters and 32,000 members. AFCEA is dedicated to the ethical exchange of information between industry, government and academia on matters related to national security, with a focus on C4, intelligence, cyber, homeland security, and technology. Shea was the Director for Command, Control, and Communications, J6 for the United States Pacific
Command from 1995-98 and in that position he was a key player in the Exercise Terminal Fury ’97, which was one of first major U.S. government exercises focused on cyber. He later became the Director of C4I/CIO for the United States Marine Corps and in his final military position he served as the Director, J6 for the Joint Staff, the senior advisor to the Chairman of the Joint Chiefs of Staff on all C4 and defensive cyber related matters. While in that position, he was given the responsibility of writing the first United States National Military Strategy for Cyber Operations.

This presentation will focus on select key observations that Lieutenant General Shea has made and continues to make in matters related to cyber from the strategic to tactical level. Among the topics covered will be implications of policy or the lack of policy, the importance of information sharing between industry, government and academia and between governments, the need for education and training as well as the competition for human capital in cyber related disciplines. Shea will use his years of experience in cyber related matters to highlight some of the challenges he has observed over the years and continues to observe. He will also discuss his concern with the pace of change needed to address the cyber threat.

1.5c Update: Cyber Security Threat or Strategic Advantage?

Presenter: Mr Kevin Zuccato, National Cyber Security Executive, IBM

As we all know, the pervasiveness of the internet, ubiquity of technology and globalisation have combined to create a perfect storm with regards to cyber security challenges, which we are collectively being called to address in new and collaborative ways. That being said, all of these things are combining to drive rapid innovation and exciting new disruptive capabilities, which will enhance the way we live, play, relate and do business.

As Australians we are well placed to continue to develop a framework to ensure all industries participate in protecting our nation and its partners from cyber security threats.

In this session, based on his previous experience working for the Australian Federal Police (AFP) and in his current role as IBM’s National Cyber Security Executive, Kevin will share his unique insights, perspectives and observations with respect to what we should defend against and what we need to embrace as opportunities for enhanced collaboration in the future.

1.6a Update: Enterprise Applications in the IT Estate

Presenter: Ms Brenda Banning, Oracle

In a complex and dynamic Information Systems environment where both agility and reliability are fundamental the challenge is to design systems that will have a long and useful and secure life, while at the same time be resilient to change and accommodate the requirements of various diverse stakeholders.

A shift of technology selection away from application-focus to business-enablement as well as flexibility in delivery methods is required to resolve the current mismatch between the needs of the user community to make adjustments to the user interface, business logic and workflow, and the speed of the configuration management process for the enterprise applications. The technology to support the capability should be delivered through a collection of applications and tools that are used in concert to provide the right information to the right user (person or system) at the right time in the right format. From a delivery perspective a 2-speed ICT approach is required to balance reliability and agility.

1.6b Update: 2016 Military CIS Workforce, Supply & Demand

Presenter: Mr Robert Kremer, Kinexus, formerly Kinetic Recruitment

Since presenting at the 2015 MilCIS, there have been some important changes in the supply and demand of defence industry CIS skills sets. The 2016 presentation will review and analyse the most recent data available from the Kinetic Recruitment Defence Industry CIS Workforce Survey, offer insights from the last 12 months as well as provide predictions and recommendations for the future. Insights discussed within the presentation will include:

- Address and analyse some key factors in supply and demand
  - Demand Factors
    - What are the current and future project environments?
    - Structural changes to the market: CASG, ISP, etc.
    - What have the smart employers been doing?
  - Supply Factors
    - Who is/ will be competing for the CIS skills?
    - Demographics. Update on the age, experience levels, locations and gender split of the workforce.
    - What are the new generation of Graduates seeking?
• Salary Levels
  o What are the trends?
  o What skill sets have experienced the strongest/ weakest growth?

With the ADF embarking on programs to replace most major platforms and systems over the next few years, an understanding of the military CIS workforce is essential for any organization looking to attract and retain the workforce needed for successful project outcomes.

1.6c Product Brief: Link-16 Solutions for the Future

Presenter: Mr Doug Henderson, Data Link Solutions

DLS has provided more than 7,000 Link 16 terminals for more than 40 different platforms in more than 40 countries with product offerings that include the JTIDS, URC-138, MIDS LVT-1, MIDS-JTRS, MIDS LVT-2/11/12, MOS, FDL, TTR and High Power Amplifiers. In addition to the newest terminal, MIDS-JTRS, two featured products are the TTR and a High Power Amplifier (HPA). The TTR stands out as the smallest, most capable and cost effective Link 16 terminal in the market. With no cooling required, ease of integration and in-flight selectable power options, the TTR brings capabilities not possible before with small platforms desiring Link 16. The new HPA provides significant savings in weight (40%) and volume (50%) at a reduced cost, and in addition to being designed to be used with the MIDS-JTRS, is backward compatible with MIDS-LVT.

1.7a Update: Cloud Security: Constant Innovation Without Constant Capital Expenditure

Presenter: Mr Richard Brown, Cogito Group Pty Ltd and Mr Phil Cutforth, The Department of Internal Affairs

The ‘As a Service’ Model is allowing organisations to realise better and constant innovation at lower costs, enterprise level protection at costs that make it accessible to organisations of all sizes. You get the best solution through choice and less vendor lock in. Cloud security services for example are able to adopt new technologies such as improved threat protection quicker. No waiting for an upgrade cycle. NZ Government Case study explored.

1.7b Update: Adobe with Defence - Content Sharing Solutions, Mission Readiness and Online Training

Presenter: Mr Kim Fritsche, Customer Success Manager, Adobe and Mr Mark Samuels, Government Specialist Webqem

A cross section of Defence and its international partners have used Adobe Connect for their content sharing solutions, mission readiness and online training for more than a decade.

With more than 12,000 plus employees worldwide, Adobe has been revolutionising digital content, and providing federal government agencies with best-in-breed technology and solutions to rapidly create ground-breaking digital content, securely manage digital assets, enable collaborative workflows and deliver digital experiences across multiplatform environments.

Adobe and its partner Webqem will outline why Adobe Connect has been the principle collaboration service for the US Department of Defense, with at one point with more than a million registered users, spanning all over the globe in every operational environment.

Adobe Connect is a tactical, operational, virtual learning platform that was recognized as best in class by US DoD in 2007. More recently, Adobe’s research and development investment in Connect culminated in Gartner awarding top in class honors for Webinars, Learning & Training, and External Presentations workloads.

Webqem, an Adobe Training Centre and a full service digital agency, will demonstrate how to design and build best practice e-learning solutions, that can be fully integrated with existing Learning Management Systems. Demonstrated uses cases will include the efficiencies and cost savings and examples from:

- Mission Command
- HADR: Japan tsunami, Haiti earthquake,
- DC snow blizzard 2010, Midwest flooding
- Situational Awareness
- Education: Suicide prevention, pre-deployment
- Tele-maintenance
- Mission planning
- Training and elearning
- Exercise simulations
1.7c Product Brief: Achieving Information Superiority in Secure Command and Control Environments
Presenter: Mr Joe Pajer, Thinklogical

The proliferation of intelligence, surveillance and reconnaissance (ISR) information is radically changing the landscape of the military and intelligence community. Countries are now following a strategy of information superiority to defend against a broad range of threats, whether they be asymmetrical, nuclear or mass armies. A herculean effort has been directed at collecting data through satellites, unmanned vehicles and the monitoring of social media and other information sources.

The processing and analysis of this information mostly happens in a secure command and control operations centre, often with joint forces (across branches as well as countries) working together. The number and size of these centres is growing exponentially throughout the world. The current focus of the men and women who design and operate these command centres is “Instant Situational Awareness;” that is, “how can I use the ISR information sources available to me to give me a full and instant picture of the situation?”

In this session, you will learn how to:
• Achieve information superiority and instant situational awareness through and immediate access to critical video and data resources via “any-to-any” switching
• Simplify management of multiple classifications of information through a single IA (information assurance) approved secure infrastructure
• Increase the cyber security profile of command and control facilities while mitigating the threat of intentional or accidental breach, hack or data loss by insiders
• Future-proof your video, audio, and computer signal distribution system to support advances in technology, including 4K resolution and HDR
• Enable flexible and rapid reconfiguration of command and control resources to quickly adapt to dynamic mission requirements
• Reduce up-front IT and AV infrastructure expense while lowering long-term total cost of ownership

1.8a Refereed Papers—Industry Stream

Paper 1: AISR Missions on Intelsat EpicNG Ku-Band
Authors: Dennis Boiter; Gerry Jansson; Christopher Hudson; (Intelsat General, USA) Eric K Hall (L-3 Communications)
Abstract. Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) systems currently rely heavily on transponded satellites, both military and commercial at X-, Ku- and Ka-bands, for missions requiring beyond line of sight connectivity. Ku-band commercial satellites are the work-horse for both manned and unmanned Airborne ISR (AISR) operations today. In the future, C4ISR systems will require higher throughput, greater protection and improved affordability to align with future mission needs, mitigate threats, and fit within budgetary constraints. Intelsat EpicNG satellites provide cost-effective, next-generation, Ku-band capabilities including spot beams, higher throughput, improved efficiencies, and protection using deployed infrastructure. In this paper, the EpicNG architecture is described with comparisons to the legacy Ku-band systems and its application to the unique performance and mobility management needs of AISR systems. A detailed performance analysis is presented using representative AISR systems against a set of manned and unmanned mission/platform scenarios; with comparisons to legacy Ku-band and WGS Ka-band performance. It is shown that the EpicNG Ku-band satellite constellation, including H-3e, offers unique performance and affordability opportunities for AISR missions and enables the next generation military Ku/Ka-band C4ISR infrastructure.

Paper 2: Achieving the Single Information Environment
Author: Douglas Stapleton (Highlands Information Security Pty Ltd, Australia)
Abstract. The information environment at Australian Defence has traditionally spanned across different networks at different classifications. Bringing these disparate networks together into one Single Information Environment (SIE) is in the way of a grand challenge. This paper outlines the issues involved and plots one possible path towards accomplishing the grand challenge of finally achieving a Single Information Environment. That would mean that Defence could operate on one single network, not multiples as is the case today. It would also mean that Defence users would only have one set of credentials to login to the D-SIE (Defence Single Information Environment, as it will be known for the purposes of this paper).

1.8b Refereed Papers—Industry Stream

Paper 1: Design of a Mission System Interoperability Development Environment
Author: Andrew Coyle (Boeing Defence Australia)
Abstract. Over the past decade, the Royal Australian Air Force has seen the introduction of a significant number of new airborne C4ISR capabilities and an increasing commitment to coalition operations around the world. This has led to the need to enhance the overall interoperability of the RAAF and become a ‘Fifth Generation’ air force that is ‘truly joint’. This paper provides an overview of a project to design and establish a new mission system interoperability development environment capable of supporting interoperability prototyping and demonstration activities using a
mixture of live, virtual and constructive technologies and connection to existing platform engineering development environments.

**Paper 2: Performance Enhancement of LTE-HetNet utilizing Asynchronous ABSF Configuration Combined with Horizontal Sector Offset and Vertical Beam Forming**

*Author: Fahim Salauddin (North South University, Bangladesh)*

**Abstract.** This paper inspects a heterogeneous network gathering macrocells and femtocells where macro users suffer significant downlink interference from femtocells due to frequency reuse across sectors of the same eNodeB and between eNodeBs. Earlier it has been shown that, a horizontal sector offset was combined with asynchronous ABSF to tackle this problem and it improved network performance significantly. In this paper, the idea of static vertical beamforming has been applied along with the concept of the combination of horizontal sector offset and asynchronous ABSF. Incorporating this additive idea with the existing improvement, the co-channel deployed network start functioning in both horizontal and vertical dimension. Simulation results show that, with the addition of vertical beamforming coverage probability increases by 40% and average user throughput increases by 30%. Moreover, the additional cell layer decreases the handover failure rates significantly, neither it increases cell boundaries per eNodeBs, and it is fully compatible with current channel dependent schedulers and gains scale with higher sectorisations.

1.8c Product Brief: Introduction to AWS Cloud Computing

**Presenter:** Mr Mark Fox, *Manager, AWS*

Amazon Web Services (AWS) provides on-demand computing resources and services in the cloud, with pay-as-you-go pricing. This session provides an overview and describes how using AWS resources instead of your own is like purchasing electricity from a power company instead of running your own generator. Using AWS resources provides many of the same benefits as a public utility: Capacity exactly matches your need, you pay only for what you use, economies of scale result in lower costs, and the service is provided by a vendor experienced in running large-scale networks. A high-level overview of AWS’s infrastructure (such as AWS Regions and Availability Zones) and AWS services is provided as part of this session.

1.9a Refereed Papers—IEEE Stream

**Paper 1: Towards Automatic Implementation of TDL Systems**

*Authors: Tobias Eggendorfer, Volker Eiseler (Universität der Bundeswehr München, Germany)*

**Abstract.** Military operations heavily rely on tactical data links to exchange command and control data allowing participants to gain an understanding of the operational situation. Since today most operations involve multiple nations cooperating on a mission these tactical data links are standardised e.g. as a NATO STANAG. However these standards are very complex and regularly updated to reflect technological advances. Therefore implementing TDL systems adhering to these standards is a very complex and error prone process. By supporting a NATO group developing an XML implementation of TDL standards and providing a toolset to implement a multi TDL capable system configured using these XML-TDL-specifications, the authors demonstrate how to shorten this process and allow for a completely automated implementation of TDL-STANAGs.

**Paper 2: Introducing Tactical to Enterprise Integration**

*Author: Christos Sioutis (DST Group, Australia)*

**Abstract.** This paper introduces a research program for investigating the technologies and challenges in achieving seamless integration between Defence's Tactical and Enterprise technology domains. The tactical technology domain encompasses the platforms, networks and supporting systems through which the Australian Defence Force (ADF) operates to achieve the commander's intent. Similarly, the enterprise technology domain encompasses the enabling business and information management aspects of the Defence organisation. Tactical to Enterprise Integration (TEI) is a complex problem which expands beyond simple network connectivity, or even information interoperability. There are many technical challenges and just as many potential solutions for achieving this integration. However, the operational effectiveness of the solutions varies depending on how they support the warfighter. With this in mind, the research program has four threads. Each thread is described in the context of a guiding warfighter vignette that depicts how a relevant tactical decision may be supported by the enterprise. Through preliminary research, the paper also identifies a number of key technology areas for initial investigation.

1.9b Refereed Papers—IEEE Stream

**Paper 1: Achieving Policy Defined Networking for Military Operations**

*Authors: Hung Xuan Nguyen, Michael Webb (The University of Adelaide, Australia); Sanjeev Naguleswaran (QSPectral Systems, Australia)*

**Abstract.** In the past few years, significant progress has been made in software defined networking in a quest to increase automation, improve network agility and security, simplify network configuration and reduce resources to establish and maintain the network. There are now a vast number of studies exploring how to utilise policies to achieve these goals. Applying outcomes of these studies to military networks requires a clear understanding of military applications and available mechanisms to implement the appropriate policies in a software defined networking
environment. In this paper, we identify several military networks where automatic policy defined networking is crucial. We further present a prototype policy defined networking solution that automatically translates high-level policies into device level implementations.

**Paper 2: A Heterogeneous Software Defined Networking Architecture for the Tactical Edge**

*Author: Ibrahim Elgendi; Kumudu S Munasinghe and Braden McGrath (University of Canberra, Australia)*

**Abstract.** The demand for real-time data in a modern battlefield is increasing exponentially. As a result, current military network paradigms and architectures are struggling to cope with increasing capacity demands at the tactical edge. Unfortunately, rescaling existing network architectures will not be a permanent solution to the problem. Therefore, in this paper, we propose a 3-tiered Software Defined Networking (SDN) architecture consisting of heterogeneous Dense Networks (DenseNets), which is a highly condensed deployment of relatively small, low-powered femtocells, at the tactical edge. The proposed 3-tiered SDN architecture abstracts the Land Tactical Network (LTN) as the Physical Layer, the Battlefield Tactical Network (BTN) as the Control Layer, and the Joint Task Force Headquarters (JTFHQ) as the Management Layer. The simulation and results confirm the architecture's capability for providing interoperability between heterogeneous communications equipment and supporting high capacity demands within limited and unreliable networking infrastructure in battlefield environments.

**1.9c Refereed Papers—IEEE Stream**

**Paper 1: A Novel Efficient Signal Processing Approach for Combined Acquisition of GPS L1 and L2 Civilian Signals**

*Author: Sana Qaisar, Craig R Benson and Michael J Ryan (University of New South Wales, Australia)*

**Abstract.** L1-L2C is the first dual-frequency pair of civilian GPS signals, expected to become available over the full constellation by 2019. Pre-operational CNAV broadcast is made available to support development of L2C signal processing capability in modernised GPS receivers. The transmission of synchronised L1 C/A and L2C codes by Block IIR-M and follow-on generations of GPS satellites allows GPS receiver designers to develop correlators for combined acquisition of the two signals to achieve additional detection sensitivity when compared to processing an individual signal. One of the key challenges in this joint acquisition is the processing complexity or cost of Doppler search to be conducted over the synchronised data-bit intervals of 20 milliseconds in each of the L1 and L2C channels. To date, researchers have addressed this problem by limiting the coherent correlation interval to a 1ms period, thereby reducing the Doppler search space while combining the outcomes of 20 coherent correlations through non-coherent and differentially-coherent processing techniques to compensate the effect of residual Doppler appearing across the data-bit interval in each of the L1 and L2C channels. These solutions however compromise the signal-to-noise-ratio when compared to fully coherent processing of signals over 20 milliseconds. In this paper, we propose complex-averaging of L1 and L2C signals at the IF stage to reduce the sampling rate of the Doppler signal, and accomplish the Doppler search at a low processing cost without compromising the detection performance of individual channels. The scheme is evaluated theoretically as well as validated through experiments on real GPS signals broadcast by Block IIR-M satellites. The proposed processing approach allows GPS receivers to detect weaker signals through low-power processors.

**Paper 2: Minimising Paradoxes when Employing Honeyfiles to Combat Data Theft in Military Networks**

*Author: Ben Whitham (UNSW, Australia)*

**Abstract.** The application of deception has been instrumental to the success of military operations for thousands of years. Cyber deception offers similar potential to detect, delay and confuse a dedicated and trained digital adversary. Honeyfiles are cyber deception technique utilised by advanced network defenders to combat data theft. In practice, the accessibility and applicability of honeyfiles to military networks has been limited by designs that are over-complicated, require Internet access and/or create protection paradoxes by reproducing the very classified material that they are attempting to protect. This paper presents three new honeyfile designs, based on the transposition and substitution of content from the target environment through parts of speech tagging. The new designs minimise the replication of classified material, yet still remain enticing to malicious software or user driven searches. The main advantage, however, is that their construction can be automated, enabling their employment by personnel without cyber deception qualifications.
Session Abstracts: Day 2—9 November 2016

2.1 Breakfast Session Product Brief: Social Media and Open Source Intelligence

Presenter: Mr David Waxman, *IBM Chief Architect: Project Aurora*

Information does not have to be secret to be valuable. Open Source Information is unclassified, available and one of the largest sources of information available, but in many cases not leveraged to its full potential. During this session, David will address a number of key topics including, Social Media, Search Techniques for the Surface Web, Peer to Peer Networking, and Darkweb Intelligence. David will also discuss some of the key OSINT challenges (volume, veracity, structured/unstructured, multilingual) as well as discussing some practical applications of OSINT and how some of those challenges have been addressed.

2.2 Plenary Session: *FYEY CIO*

- **Keynote Address:** Dr Peter Lawrence, *AU CIO*
- **Keynote Address:** Mr Terry Halvorsen, *US DOD CIO*
- **Keynote Address:** Mr Mike Stone, *UK MOD CIO*
- **Keynote Address:** Mr Len Bastien, *Assistant Deputy Minister Information Management*

2.3 Plenary Session: *FPR and CIS Joint Interoperability*

- **Moderator:** AVM Andrew Dowse, *Head ICT Operations, CIOG*
- **Keynote Address:** BRIG John Gould, *DG C4, VCDF Gp*
- **Keynote Address:** CAPT Stephen Dryden, RAN, *DG Navy Communications & Information Warfare*
- **Keynote Address:** COL James Murray, *Director Land C3 Program, G6 Army Headquarters*
- **Keynote Address:** GPCAPT Glenn Nattrass, *Director Networks, Air Force*

2.4 Lunch Session Product Brief: Operational Information Management: What you need to know about security, data fusion, interoperability and future trends

Presenter: Mr Scott Marshall and Mr Richard Armstrong, *Berkeley IT*

Scott and Richard will discuss some of the latest emerging trends in best practice Operational Information Management, with specific reference to the often unique needs of Defence. They will note some of the key challenges in adapting and securing various solutions to enable them to comply with AGSCS and ISM requirements, and note emerging trends that we are seeing both in Defence and broader Government information security practice both in Australia and overseas. They will also provide some key checks that you can make of your information management solution to determine its fitness for purpose.

2.5a Product Brief: C2 Solutions for the Warfighter: Latest Capabilities in Enterprise Information Management Across Multi-level Domain Environments Securely

Presenter: Mr Phil Hawthorne and Mr Richard Armstrong, *Berkeley Solutions*

Having delivered Secure Multi Level - X Domain solutions in the ADO since 2011 Richard and Phil will update attendees on some major new capabilities which have recently been introduced on Defence networks to enable an integrated, properly secured delivery of information across dissimilarly classified networks with complete data security. Richard will demonstrate with reference to recent operations and major activities how innovative new approaches have allowed information held in multiple environments, including Nexus, SharePoint, Objective, Mercury and specialist Intelligence applications to be delivered to stakeholders in an integrated view. These new solutions are able to operate over degraded networks, providing reliable and effective solutions for the Warfighter.

2.5b Update: Airborne Mobile Broadband Communications

Presenter: Mr Joseph Johnson, *Business Development Director, ViaSat*

Today’s military and government missions require high-throughput, reliable; secure communications that enable leadership and operators to share information anywhere within moments. Airborne missions for Intelligence, Surveillance, and Reconnaissance (ISR), Command & Control, and en-route mission planning require connectivity with true broadband capability.
The Royal Australian Air Force (RAAF) has equipped its C-17A Globemaster III strategic transport aircraft with a new advanced satellite communication (Satcom) and imagery display system for its crew and passengers to address this capability need providing a significant increase in the utility of the airlifter.

During Jericho Dawn series of capability demonstrations in Canberra, the system was used to stream full motion video on large screens in the aircraft from a Heron remotely piloted unmanned aircraft system operating 2000km away over Woomera Test Range in South Australia.

This brief is intended to provide an update to the current operations and the growth of air mobility capabilities over Australia, the region and globally. The initial series of demonstrations performed over the past year are the tip of the iceberg in this capability. Senior leaders can have office like connectivity while in the air; deploying soldiers will have the latest situational awareness while en–route to their mission; ISR platforms can disseminate intelligence in real-time; and medivac missions can have real-time connectivity to medical experts.

2.5c Tutorial: Iridium NEXT – Vision for the Truly Global Satellite Communications

Presenter: Mr Nihal Fernando, Mr Arthur Ollett and Mr Jeff Detwiler, Thales Australia

Satellite communications have evolved in many different ways in the last few decades to support critical communication needs in defence, emergency management and disaster recovery. The latest and most advanced service platform is the Iridium CertusSM powered by the $3 billion Iridium NEXT satellite constellation. This new service platform is expected to deliver a wide range of service offerings together with innovative terminals providing enhanced solutions in Maritime, Aviation, Land Mobile, M2M and Government communications.

Iridium NEXT will consist of 66 cross-linked Low-Earth Orbit (LEO) satellites delivering truly mobile voice and data coverage over the entire earth surface. The launch of the first set of satellites is scheduled to occur in late 2016. The complete constellation is expected to be operational by end of 2017.

This tutorial will provide an overview of the Iridium NEXT Satellite Constellation, and the various service offerings and terminals. Further, this tutorial will present number of capability use cases applicable to Australian Defence Forces.

2.6a Product Brief: Smart Battle Management Command and Control

Presenter: COL Lynn Wills (USAF Retired), Ultra Electronics, Advanced Tactical Systems

Smart BMC2: Revolutionizing Real Time Decision Making: Computers have been used to assist Battle Management Command and Control (BMC2) operators since the 1960s when the massive Soviet bomber fleet threatened to overwhelm the day’s air defence systems. Early systems like the USAF Semi-Automated Ground Environment (SAGE, AN/FSQ-7) and USA Guided Missile Air Defense System (Missile Minder, AN/TSQ-73) leveraged early computing power to either assist the operator (semi-automated system) or completely take over (automated) the BMC2 decision making functions.

It is common to find automated functionality in BMC2 systems today assisting the surveillance, identification, weapons assignment, weapons control, and battle management task sets. Automatic track initiation, flight plan correlation, Identification By Origin, intercept guidance, and Threat Evaluation and Weapons Assignment are examples of software applications enabling more accurate and efficient decision making, while simultaneously improving operator reaction times:

- **Accuracy.** Machine to machine transactions reduce “fat finger” errors.
- **Efficiency.** Computer assistance accomplishes mundane decision making, freeing operators to focus on higher order problems.
- **Speed.** Computing solves problems faster than the operator can think, particularly when the operator is faced with an overwhelming number of simultaneous tasks.

Just as computers addressed the problem of an overwhelming Soviet bomber fleet in the 1960’s, we must solve the “deluge-of-data” challenge brought about by the Information Age. The ability to move data between sensors, shooters, and BMC2 nodes has resulted in today’s operators being inundated with data. Our Smart BMC2 (S-BMC2) system will collect, organize, analyse and act on huge volumes of data and present actionable information and courses of action to the operator.

S-BMC2 combines the robustness of our existing BMC2 system with the power of data analytics, or “Big Data”. The BMC2 component processes input data such as radar and tactical data link messages and hands off the processed data to the data analytics component. The data analytics component then analyses the data and returns alerts to the BMC2 when it finds anomalies in normal patterns of life. Based on the alerts, the BMC2 component takes pre-programmed actions using an “Operator-On-The-Loop” paradigm. Since data analytics learns over time, S-BMC2 not only operates in real time, but also becomes a predictive situational awareness tool as well.
The concept of S-BMC2 is simple: apply the same data analytic processes proven effective in the intelligence, medical, and marketing domains to collect, organize, analyse, and act on the deluge of data facing today’s BMC2 operators.
2.6b Product Brief: Next Generation Mobile Intelligence: tactical field applications

Presenter: Mr Mark Vardy, Motorola Solutions Australia

Rapid advances in technology are creating revolutionary capabilities for defence and public safety agencies. For these agencies, the ability to dynamically collaborate in real-time, capturing and securely sharing intelligence across agencies can mean the difference between mission success and failure.

Motorola Solutions’ Next Generation Mobile Intelligence strategy focuses on putting intelligence into the hands of agencies over a choice of networks, devices and applications. As part of this new direction, Motorola Solutions have developed a suite of tactical field applications which can help capability improvement including:

- **WAVE product portfolio**: every device, every network, every team, connected like never before
- **The WAVE product portfolio is a communications interoperability and broadband push-to-talk (PTT) solution that delivers real-time voice and data securely over any network using any device.**
- **Intelligent Middleware**

From radios to smartphones, Intelligent Middleware is putting the power to effectively and efficiently share information across a range of users. Intelligent Middleware ensures seamless voice, data and intelligence communications between your teams, regardless of the network they are on or the device they are carrying.

**DragonForce - team collaboration application**: bring different agencies together as a team for effective, coordinated response.

Create enhanced situational awareness through real time personnel tracking, shared maps, floor plans and images for improved tactical and emergency response in the command centre and the field. This collaborative mapping and whiteboard application means all responders have a single operating picture with real time intelligence to accomplish their mission.

Hear how these Next Generation Mobile Intelligence tactical applications are transforming the way defence and public safety agencies respond.

2.6c Update: Extreme Profiling – Hunting for Bad Actors in Social Media Data

Presenter: Mr Clement Fredembach, Teradata

An incredible amount of information about a person can be inferred from the language he or she uses. A person’s mode of expression can be significantly more insightful than the vocabulary employed. Modern terrorist groups such as the Islamic State use social media in a very sophisticated manner for propaganda, recruitment and to disseminate messages of terror. The broad reach of social media is very difficult to combat, with every suspended account being rapidly replaced by another. Identifying and tracking terrorist group supporters is thus very challenging. In this talk I will describe how to combine machine learning, natural language processing, graph analytics and personality profiling to identify terrorist sympathisers in social media. This approach has proven more effective than simply finding relevant text content to identifying people of interest. While the specific proof of concept that will be presented focuses on counter terrorism applications using social media data, this approach can be applied to any text data across a wide range of use cases where the intent is to identify people of interest.

2.7a Update: Australian Land Vehicle C4I Specification Development

Presenter: Mr Peter Whalley, Senior Communications and Systems Engineer, Australian Department of Defence

The Australian Department of Defence is developing a standard for design of Command, Control, Communications, Computing and Electronic Warfare Systems (C4EWS) for installation in future land vehicle platforms. The standard is provisionally titled the Australian Common Vehicle Architecture (AusCVA). AusCVA is based on DEF STAN 23-09 Generic Vehicle Architecture (GVA) but with substantial additions to include radio communications systems being procured by LAND2072 Phase 3, the Battle Management System being procured by LAND75 Phase 4, voice intercommunications and video communications and management. AusCVA also includes additional system design description compared to GVA as well as modification of parts of GVA to suit standard Australian practice.
2.7b Update: The Next Generation Protected Mobility Vehicle—An Introduction to the Hawkei Land Platform Integral Computing System and Generic Vehicle Architecture (Land 121 Phase 4)

Presenters: COL John McLean, LTCOL Steven Welsh, *Australian Department of Defence* and Mr Cameron Botterill, Thales Australia

Many Australian Defence Force (ADF) and Industry members are aware that Land 121 Phase 4 and Thales Australia are providing the Hawkei Protected Mobility Vehicle – Light (PMV-L) to the ADF. Many would be familiar with the strengths of the Hawkei design in terms of ballistic and blast protection, which well exceed current ADF light mobility vehicles. Most readers however, are unaware of the advanced command and control requirements being addressed by the vehicle, which will support the digitisation efforts being undertaken across Army. Principally these advances address the concept of an Integral Computing System (ICS) capable of supporting multiple tactical applications, and the introduction of the Generic Vehicle Architecture (GVA).

Both the ICS and GVA advances are new to Army, where for the last decade projects have been independently adding simple and more complex electronic systems to platforms generating significant Size, Weight, and Power – Cost and Cooling (SWaP-C2) demands on vehicles. Independent systems typically introduce unique computers, cabling, antennas and other devices, generating significant engineering complexity and SWaP-C2 challenges, often creating bespoke mission fits, and poorly integrated outcomes.

The approach taken in developing the requirements for PMV-L was fundamentally different to those taken in the past. A key requirement for the PMV-L was the increased emphasis on integrated computing solutions and the use of an Open Architecture to reduce integration complexity.

The ICS requires the capacity to host a number of tactical applications employed within Army vehicles, to remove bespoke hardware, and allow users to switch between applications on the one computing screen, or indeed display applications in any configuration within a vehicle layout. This approach requires the Project Office and Thales to resolve a number of commercial and technical challenges, across the current applications identified. The ICS will integrate Land 2072 radio systems, the Battle Management System (BMS), Advanced Field Artillery Tactical Data System (AFATDS), Digital Terminal Control System (DTCS), a Remote Weapon System and Force Protection ECM equipment.

The Generic Vehicle Architecture offered by Thales is based on the UK GVA. The GVA includes a vehicle centralised computer and Distributed Data System (DDS) data bus, allowing command and control and vehicle services to be managed on the data bus. The implementation of the DDS bus will have an impact on industry, as a potential standard interface to reduce integration complexity. Army has stated its intent to watch the progress of Hawkei informing Land 400.

2.7c Update: Defence Spectrum Update

Presenter: Mr David Murray, *Defence Spectrum Office*

The Defence Spectrum Office will provide an update on developments in Defence spectrum management and the Australian spectrum regulatory framework. Spectrum is an important defence and national resource that is facing ever increasing demand from Defence and other government users and in particular from the commercial sector. Spectrum is a fundamental requirement for Defence communications, command and control, intelligence, surveillance and reconnaissance, and electronic warfare systems. As Defence capability undergoes significant modernisation and new capabilities such as the E/A-18 Growler come into service, effective management of the radiofrequency spectrum is critical - both in the domestic peacetime context and on operations. As the ADF modernises its spectrum capabilities there is a need for the development of concepts to manage the convergence between spectrum management, electronic warfare and cyberspace operations.

2.8a Product Brief: Transforming Defence Deployed Networks with the Cisco Digital Network Architecture

Presenter: Mr Will Blake, *Consulting Systems Engineer, Australia and New Zealand*

Cisco’s Digital Network Architecture, brings together the best of software defined networking capabilities, network automation, state of the art security visibility and enforcement, and Cisco’s rich networking capabilities to provide next generation networks. This session will demonstrate how these concepts will reduce the complexity faced in current Defence networks, whilst allowing the agility required to rapidly meet operational demands and increase security visibility.
2.8b Product Brief: High Performance Situational Awareness with LuciadLightspeed and LuciadRIA

Presenter: Dr Bart Adams, Product and Innovation Manager, Luciad

LuciadLightspeed is a set of software components that can be used to rapidly develop situational awareness applications. It enables the user to connect to any kind of data, organising that data if needed, visualising it to perform all kinds of geospatial analysis. It offers unparalleled performance, high accuracy and full customisability.

LuciadRIA offers Geospatial Situational Awareness in the browser with the fluency and speed of a desktop application. The software components of LuciadRIA enable the development of advanced and easy-to-use browser applications for any browser, using today’s most advanced web-based technologies.

2.8c Product Brief: Defeating Insider Threats with Identity-Based Security

Presenter: Mr Jon Green, Senior Director, Security Architecture, Aruba

Security threats come at you from all sides, including the inside of your network. After several high-profile data leaks from malicious or careless users inside government and military networks around the world, it has now become an imperative to put additional protections in place for internal systems. But it’s not just the human threat - at the same time, the risk from IoT, BYOD, and mobile devices is increasing. To deal with these threats, we must drive out anonymity from networks – every connection must be identified and secured. In this session, hear about Aruba’s Adaptive Trust architecture for wired and wireless networks that seamlessly integrates authentication, encryption, access control, and threat response in a way that is flexible and adaptive based on the identity of the user and device, the access method, time and location, and external conditions such as national defence posture.

2.9a Product Brief: Secure Replication Across Domains

Presenter: Mr Perry Smith, Myriad Technologies

The capability to replicate data across two domains is a key requirement to enable the collaboration of users who are separated by location. This is made even more challenging when the two domains are operating at different levels of security, for example classified vs secret vs top secret. In these instances the replication must maintain the strict security of each domain and ensure there is no chance of this security being breached.

Myriad Technologies in co-operation with our partners have developed solutions which allow for cross domain replication of SharePoint environments. More specifically, the ability to replicate data over a reliable one-way network which maintains a clear division between domains, providing protection for sensitive or classified environments.

Cross domain replication works by combining advanced replication software with a unique network appliance which restricts the flow of traffic in a single direction. These proven technologies are used by government and defence agencies around the world. The absolute certainty and integrity of data required by these organisations suggests the quality and capability of the replication technologies.

This session will outline and demonstrate a working cross domain replication solution and is suitable for organisations which require 2 domains with different security levels to collaborate with each other.

2.9b Tutorial: Putting SharePoint at Sea

Presenters: Mr Perry Smith, Myriad Technologies

Having a secure, easy to use collaboration Information Management (IM) service available for use in the Maritime environment is an established requirement for Navy (and its contribution to Joint Operations).

The ability to provide such a service has proven difficult to describe and even more difficult to deliver. Fortunately, SharePoint is now able to deliver on the promise of a secure, easy to use collaboration service for various Force Elements (regardless of whether they are MFUs or Embarked Forces) even across very limited bandwidth bearers.

Combining the technology with good design can directly improve the IT service at the same time as delivering better information management outcomes. Full compliance with the relevant legal instruments that control IM within a Defence environment is quite possible whilst delivering a highly usable SharePoint environment.

Myriad Technologies will discuss the technologies in use within ADF and demonstrate capabilities that illustrate the types of Use Cases described. Myriad will also discuss some of the specific challenges from both a technology and information management point of view and highlight the solutions that have proven successful in overcoming those challenges.

This session is particularly relevant to Navy Information Managers, as well as technologists and records managers seeking an understanding of how such a solution aligns back to the first principles review for Defence.
Digitising and streamlining your business processes is one of the most significant ways that you can improve your organisations efficiency and lower costs. This session will explain how Microsoft SharePoint and Nintex can be used to workflow and automate your business process both within your organisation and in the field with Nintex Mobile.

Nintex has been widely recognised as an industry leading application for the creation of digital forms and workflows. As a premier partner Myriad Technologies has developed significant capabilities in how to best integrate the Nintex solutions within document, knowledge and organisation management systems.

Using Nintex and SharePoint can dramatically change the way your organisation streamlines your business processes. Come along to this session to see how Nintex can change the way you work today.
Session Abstracts: Day 3—10 November 2016

3.1 Breakfast Session Product Brief: The Role of Industry in Collaborative Cyber Security Threat Intelligence
Presenter: Mr Gary Hale, Director, Cyber Security & Innovation, Security & Trust Organisation, Cisco, Australia and New Zealand

Join us for this thought provoking session to discuss the vital role that industry is providing to governments and researchers in helping them to enhance their understanding of the threat intelligence landscape. We’ll delve into some specific use case examples of where these collaborative threat intelligence partnerships are making an impact against the advancement of cyber security.

3.2 Plenary Session: Defence Cyber

Keynote Address: Mr Michael Scotton, Assistant Secretary Cyber Security, Australian Cyber Security Centre
Keynote Address: Mr Chris Brookes, Assistant Secretary ICT Security, CIOG
Keynote Address: CDRE David Scott, RAN, DG Joint Information Environment Warfare, VCDF Group

3.3a SecureCanberra Plenary Session

Welcome Address: (ISC)²

Presentation: Prisoners Immunity and Bees – How Collaboration Works in Information Security
Presenter: Mr Craig Searle, CISSP, Chief Apiarist, Hivint, Australia

Ever wondered why collaboration in the hacker community isn't reflected in the real world? Why companies spend vast amount of money solving the same problems as everyone else, or worse, making the same mistakes as everyone else? There are plenty of examples in nature as to how and why collaboration is beneficial for all involved, and how those that don't play by the unstated rules are quickly punished by the community. Why is it so hard for well-funded and well-resourced organisations to achieve the same results as a loose collective of people spread all over the globe? Many Western governments are getting in on the collaboration revolution going as far as to introduce legislation to encourage it.

3.3b SecureCanberra

Presentation: Cybersecurity – What Have We Missed?
Presenter: Mr Chuan-Wei Hoo, CISSP, CISA, CFE, BCCE, Executive Security Advisor, APAC Security Tiger Team, IBM, Technical Advisor, Asia-Pacific, (ISC)², Singapore

3.3c Lunch Session Product Brief: Omni-channel Operator Engagement
Presenter: Mr David Lincourt, Vice President, Field Services – Global Defense Industry Business Unit, SAP

Digital technologies have changed the game. For example Hyperconnectivity enables higher operator and organisational agility, engaging in real time across the digital defence network to deliver against desired outcomes. Large-scale in-memory computing collapses transactional and analytical processing into a single platform, dramatically reducing cost and enabling massive simplification and value creation. New technology adoption and business innovation in what is termed the fourth industrial revolution is exponential. Technology infrastructure lives on new cloud-based collaboration platforms, which can enable Defence organisations to adopt new procedures in a matter of days. Sensors, robotics, 3D printing, and artificial intelligence are becoming the new normal.

Omni-channel user experience is now a key driver for technology adoption. Operators’ desire and organisations’ demand simple, seamless, personalised experiences across any channel, anytime, anywhere, and on any device. The outcome-focused defence organisation requires a deep change in operating concepts and new organisational and business process capabilities to take advantage of these technologies and to improve the user experience. Additionally, Big Data allows defence organisations to sense and respond to operators’ needs in real time and predict the next, best step for meeting these needs.

By focusing on the outcome and not on the “how”, with the rapid introduction of disruptive technologies, we will see improved operational effectiveness by means of:
• orchestrating business processes across operator-facing functions;
• delivering personalised experiences in context with each interaction;
• creating a single, harmonised experience for each operator, while reducing the burden on personnel;
• being prepared to engage the operator on the channels they choose at any moment while on operations; and
• full integration with your core business processes.
3.3d SecureCanberra

Presentation: Containment vs Prevention—Realistic Strategies for Dealing with Cybersecurity Threats

Presenter: Mr John Kendall, Border Security Program Director, Unisys Global Public Sector

Much of the current thinking and approach to cyber threat countermeasures assume that tools and procedures will prevent cyber threats from accessing sensitive data and resources. However, experience shows that if a human is involved, a cyber breach is inevitable. Given that reality, cybersecurity strategies must include strong breach containment measures. This presentation explores emerging cryptographic micro-segmentation technologies as a means to provide breach containment and examines the practicality of such approaches.

3.3e SecureCanberra

Presentation: Securing the IoT: Convergence of Anomaly Detection & Device Security

Presenter: Mr Nick Savvides, CISSP, Manager – Cyber Security Strategy, Symantec

The era of the ubiquitous, connected device network is here. From city planners instrumenting their streets to consumers connecting their homes; the explosion of new devices, new protocols & new ecosystems present new security problems. This talk will examine the some of the failures of existing approaches & the new evolving mitigations including the role of streaming and big data analytics.

3.3f SecureCanberra

Presentation: Considerations for Establishing the Australian Army’s Cyber Work Force

Presenter: LTCOL Lisa Davidson, UNSW Canberra

3.4a Update: ABCA Armies CIS Update

Presenters:
LTCOL Nathan Schurmann, LNIC
LtCol Adrian Woodley, British Army
LCol Dany Boivin, Canadian Army
Mr Joseph L. Wiley
Mr Jeffrey L. Hendren, US Army
LT Thomas Raxworthy, New Zealand Army

The America, British, Canadian, Australian and New Zealand (ABCA) Armies' Program mitigates interoperability gaps, leverages opportunities and informs modernization to optimize ABCA interoperability for full-spectrum land operations up to and including the two-star level in a Joint, Interagency, Interagency, Multinational (JIM) environment. Within ABCA the CIS Line of Effort (LOE) is responsible for developing standards for CIS interoperability between the five armies. This plenary session will provide an overview of the current challenges facing each Army in providing CIS to support warfighting, as well as issues for coalition interoperability.

3.4b Update: Evolving Core Communications Considerations for Planners in contemporary operations – Interoperability, Network Security and Information Management

Presenter: LTCOL Michael King, SO1 CIS Plans, Headquarters Joint Operations Command

Commanders are becoming increasingly dependent on computer networks to conduct contemporary operations throughout the scale of conflicts due to the increasing requirement to rapidly collect, disseminate, and process available information. This reality is forcing communications planners to review and reconsider some core considerations when developing a network architecture to be used on operations. Three key examples have become increasingly more complex over recent years and only deliberate and considered efforts to address these issues will ensure future operational success. Interoperability with coalition and interagency organisations, our ability to protect these networks, and our capacity to manage the exponential increase in information are significant challenges that are increasing in complexity. The success of any operation today and into the future could hinge on our efforts to address these core requirements. Importantly these efforts not only require careful consideration by communications planners, but equally as important, they need to be understood by the whole operational planning group and the deploying force.
3.4d Update: Army's Land Network Battle Lab (LNBL)

Presenter: Mr Tom Schar, *Land Network Integration Centre (LNIC)*

This session will give an overview of the Land Network Integration Centre’s LNBL 100 EPLRS radio trial conducted in the lead up to Ex Hamel 16. The session will outline the challenges faced by Army when transporting C2 and Fires information around the battlefield and highlight the limitations of the underlying bearer and C2/Fires systems when operating in challenged environments. We will discuss our LNBL EPLRS lab trials; the results of which enabled Army to make significant improvements to the Tactical Communications Network (TCN) deployed on Hamel 16.

3.4e Update: Analysis of HAMEL 16 Data

Presenter: FLTLT Sibi Ravindran, *Land Network Integration Centre (LNIC)*

This session will provide an analysis of the network and application traffic flows captured during Exercise HAMEL 16. This is the first attempt Army has made to capture such large amounts of data for a Divisional level field exercise. There are a number of insights Army has gained by using the Land Network Integration Centre (LNIC) Land Decision Support Environment (LDSE) advanced data analytics. The intent is that the information and knowledge gained from this analysis can be used by Land C3I projects, such as EDLAN, JP2072 and LAND200 to better understand the characteristics of a modern deployed IP network.

3.4f Update: Land Platform Radio Performance Study

Presenter: Mr Peter Whalley, *Australian Department of Defence*

The CoA has conducted a Land Platform Radio Performance Study to characterise the performance of the radio systems installed in vehicle platforms under the LAND75 project. The Study involved desktop studies, measurements and simulations of a wide range of factors which together contribute to the usable range of tactical communications systems operating in the HF, VHF and UHF bands. The results of this work have produced draft radio system performance requirements for Australian military vehicles which are achievable, cost effective and verifiable. Testing methodologies have been developed based on various US, British and International standards and these form part of the project deliverables. A number of the tests have not previously been undertaken by the Australian DoD and have resulted in significant insights into the challenges involved in producing meaningful and useful results within reasonable time periods and using scarce resources such as large shielded enclosures. Comparisons have been made between measured antenna radiation patterns on vehicles and calculated patterns using FECO. The work was jointly undertaken by the Directorate of Systems Engineering and Integration and Accredited Test Services within the Land Engineering Agency, and Codarra Advanced Systems Pty Ltd.

3.5a Product Brief: Streamline User, Data, and Network Defence in a Multi-Level Environment

Presenter: Mr Steve Stratton, *Director Federal Product Management, Forcepoint*

How can you make it harder for adversaries to find and breach your most sensitive data when faced with the distributed realities of a multi-level environment consisting of 2, 3, 4 or more networks? Reduce the attack surface with multi-level access technology.

Trusted Thin Client®, an authorised multi-level access solution, provides you the capability to consolidate one of the more vulnerable aspects of your environment: many endpoint devices per user, all with local storage.

Trusted Thin Client reduces the attack surface by replacing separate endpoints for each network with a single read-only device. Leveraging virtual desktop infrastructure (VDI) technologies, all desktop images and data are stored and managed in a central datacentre. This approach separates the data from the device and delivers seamless access to all allowed networks from approved devices and locations.

Join Steve Stratton, Senior Director of Product Management for Forcepoint, to learn how Trusted Thin Client:
- Enables secure, simultaneous access to multiple networks / multiple clouds (public, private, hybrid) from a single device
- Provides centralised enterprise management for the system, networks and users
- Supports a wide variety of backend virtualization servers: Citrix, Microsoft, VMware
- Supports Size, Weight, Power, and Cooling (SWAP-C) requirements
- Strikes the right balance of cost, performance and security required for high-assurance

Forcepoint (formerly Raytheon|Websense, Raytheon Cyber Products) provides a flexible platform unifying your enterprise protection tools. Forcepoint protects against insider and outsider threats, rapidly detects breaches, minimizes dwell time, stops data theft and enables secure access and transfer of sensitive data between multiple networks.
3.5b Product Brief: Exploiting the Data Deluge with a Unified Data Architecture

Presenter: Mr Ross Farrelly, Teradata

Defence organisations are inundated daily by a large volume of multi-structured data from diverse sources. To make sense of this data and achieve their aims in a challenging and adversarial setting they need infrastructure capable of ingesting these data, analysing it at scale and deploying advanced analytics upon it to infer and predict future events.

This product briefing will introduce Teradata’s Unified Data Architecture (UDA) as a solution to this challenge. The UDA comprises Teradata’s Enterprise Data Warehouse, its scalable discovery platform (Teradata Aster) and the Hadoop open source distributed file system, along with Teradata Listener for ingesting and distributing extremely fast moving data streams throughout the analytical ecosystem.

Real world use cases will be presented to demonstrate how the UDA has been deployed in diverse global adversarial settings.

3.5d Panel Discussion: Defence IT Education and Training

Presenter: AVM Andrew Dowse, CIOG & Professor Michael Frater, UNSW Canberra

3.5e Update: Recent Advances in Low SWAP for Position, Navigation, Timing and Frequency Sources for Military Communication Systems

Presenter: Ms Lisa Perdue, Applications Engineer, GNSS Systems, Spectracom

Driven by the need for low Size, Weight, Power (SWAP) and cost in drones, the components providing Position, Navigation, and Timing (PNT) to airborne communication systems are becoming more integrated and efficient. This presentation will cover several recent advances in oscillator technology, resiliency in GPS-denied environments, and higher component integration.

For oscillator technology, the Chip Scale Atomic Clock (CSAC) is now a reality, providing atomic stability in a fraction of the size and power footprint. GPS-disciplining provides further high accuracy at lower cost. New isolation and compensating techniques provide low phase noise frequency even under high vibration conditions.

New resiliency methods are providing PNT even under GPS-denied situations by integrating GNSS receivers with Inertial Navigation Systems (INS) and other sensors such as Lidar. MEMs technology is reducing the size and cost of INS systems while improving accuracy to reach tactical performance levels. Smart Antennas are using electronically steered beams to maximize the gain toward the navigation satellites while pointing the nulls toward interfering sources. All of these components are being deeply integrated with networking components such as rugged switches and interfaces to new emerging standards such as the US Army’s VICTORY standard and VITA 75.

The presentation will cite some example applications where low SWAP PNT technology is being used, such as airborne communications relays; signal intelligence drones; airborne Synthetic Aperture Radar (SAR) systems; and Satcom on the Move. These exciting advances will be of interest to communication system integrators for both airborne and surface applications.

3.5f Product Brief: Taking Text from Files to Actionable Information

Presenter: Mr Clement Fredembach, Teradata

Most operational and administrative systems generate substantial information in the form of text documents and files. Once stored, extracting, understanding, and analyzing the content of such files in an effective and user-friendly manner can be challenging. This tutorial guides attendees through a step-by-step process of acquiring and using information from a collection of text and documents.

Starting with a collection of documents in various formats in a fileserver, attendees will learn how to automatically load, parse, and extract the files’ text content, to structure it and to insert it into a database. With the information now available in a structured form, we demonstrate how to perform natural language processing tasks with state of the art interactive text analytics algorithms, to select, filter, and categorise documents as well as extracting entities (e.g., people or places) contained within. Finally, methods that enable the visualization of document content as well as linking documents together through network graphs are explained.
3.6a Product Brief: How Skynet 5 Can Complement WGS with Military Grade X-Band, Enhancing Australia’s Operational Effectiveness

Presenter: Mr Simon Barker, Airbus Defence and Space and Ashley Neale, Speedcast

X-band satellite capacity is reserved exclusively for military and government organisations and is used for mission critical, sensitive command and control communications systems, where loss of communications is not an option.

Whether the need is for government, military, humanitarian, emergency response or other diplomatic communications, it can provide uncontended capacity and availability wherever and whenever required on its own constellation of military secure X-band satellites.

3.6b Update: Geospatial Services and Network Enabled Operations – Utilising JP2064 Phase 3

Presenter: Mr Scott Ralph, Project Manager PM JP2064 Evo1, Australian Geospatial-Intelligence Organisation

JP2064 delivers enterprise Geospatial Infrastructure, Information and Services to Defence on DRN and DSN. JP2064Ph3 Evo1 will provide an online geo-capability for users to access geospatial information (GI), applications, services and map viewers. GI encompasses maps, charts, imagery, weather, and other geo-enabled data about the earth, environment and man-made infrastructure providing global coverage.

Users can access JP2064 services through a web browser to discover, visualize and exploit a wide range of geospatial services. The system enables sharing of data or products and integration of these products into Defence operational and business workflows.

Services provided by JP2064 include simple visualization of imagery and maps through to complex terrain enabled 3D visualizations complete with on-line collaboration tools. Features such as generation of fly-throughs, and the ability to record and play back in presentations is provided. More broadly, users have access to simple tools to analyse data and to generate custom views of available information for sharing, or simply to load into power-point presentations. Significant search capabilities are provided to allow users to rapidly explore Defence data holdings and explore content.

Where combat systems require GI as specific data sets or formats, operators can identify, package and download these to meet their needs. Alternatively on-line services are available that provide machine to machine connections from geospatial services to systems such as C2, flight planning and simulation systems. Selected users can even publish their own services and web “mash-ups” for use within their own business areas.

This presentation will cover the extent of capability being delivered on Defence networks, and raise ideas on how the data and services can be used in Defence daily operational business. It will also inform ICT and acquisition professionals on project delivery ‘lessons learnt’ and the philosophy behind delivering a more agile project within the Defence environment. This will reflect on the challenges of team organization, system design, integration, implementation, transition to service, and how the agile project approach will ensure the capability continues to evolve; remaining contemporary and relevant.

3.6d Product Brief: ISR Information Sharing: Data, Entities, and Objects in Context

Presenter: Mr William Sokol, MarkLogic and Mr David Eastman, Esri Australia

Analysts are being asked to synthesize actionable intelligence from an overwhelming tide of data. Ops Tempos are increasingly antagonistic to painful serial Tasking/Collection/Processing/Exploitation/Dissemination (TCPED) cycles. So the question is, how can you help stakeholders at all echelons get the freshest intelligence without sacrificing accuracy, information integrity, access, or security?

Adding to these challenges is the need to operate in an All-Source environment, as the data silos created from legacy systems stand in the way of providing commanders with the information needed to respond to evolving threats.

The analysts these leaders depend on need to be able to see beyond the data trapped in silos. Facts drawn from authoritative GeoINT, ImINT, HumINT, SigINT, MASINT, and the internet need to be aggregated, expressed as entities and objects, and then put into context: Geospatial, Temporal, and Semantic.

The centre of a response to these factors is in liberating data from the confines of legacy systems, focusing on metadata management, exposing data and related functionality via APIs and web services, and balancing the need to share with safeguarding sources and methods.

Two leading COTS software firms—MarkLogic Corporation, the Enterprise NoSQL database leader and Esri the world’s leader in geospatial information systems—are helping government and commercial customers to meet these
challenges head on. In this session, they will provide an overview of key advances in data management and analytics with relevance to:

- Human Geography & Socio Cultural
- Common Intelligence Picture
- Situational Awareness for C2
- Intelligence Operations including Detached Users
- Open Source & Social Media Analysis

3.6e Update: Air-Sea C2 Connectivity for 4th and 5th Generation Platforms

Presenter: Mr Anthony Karkainen, Director of Business Development, Northrop Grumman

As a follow-up to the successful Jericho Dawn 16-3 Air-Ground demonstration, Northrop Grumman will discuss how to expand the Airborne Gateway concept to include ideas on how to bring 5th generation forces and sensors into the Air-Sea domains, how to connect the seaborne forces to shore for amphibious support, provide connectivity for shore observers to call in Naval Gun Fire support and ensure positive aircraft command and control is maintained for ship launched aviation assets.

Today's 4th generation forces will greatly benefit from having 5th generation sensor and target data. By using Airborne Gateways, Northrop Grumman has demonstrated the ability to provide 5th generation data to Naval forces by means of various data and voice networks. This "5th to 4th" connectivity provides the advantages of having advanced sensor information provided directly to legacy platforms.

Line of sight with amphibious forces moving ashore can be obscured by obstacles, interference or simply curvature of the earth. An Airborne Gateway can be used to connect these amphibious and littoral forces to provide uninhibited communications through all phases of the amphibious landing. If communications is interrupted by obstacles, or distance, an Airborne Gateway can reposition to regain the connection. If the connection is lost due to interference, the Airborne Gateway can switch to different radios, frequencies or waveforms to regain communications.

Finally, the Airborne Gateway can be used to provide for aircraft command and control at any distance from the ship using a UHF to Airborne Gateway to SATELLITE bridge.

3.6f Update: Concept of Operations Changes with Hand Held Link 16 and Other Small Form Factor Terminals Deployed

Presenter: Mr Mark Yelsits, Software Product Manager, Viasat

A discussion of new technologic advances in Link 16 Products to include the deployment and implementation of Hand Held Radio applications. The presentation will discuss technology advances in hardware and software capabilities, platform implementation and integration issues and overall concept of operations changes based on these new participating units.

This technology improvement allows additional personnel and platforms to participate in net centric warfare with applications ranging from very small UAVs to forward observers and air controllers. The addition of these participants will change how information is shared on the battlefield and how networks must be designed in order to accommodate the new participants.

3.7a Update: Lean and Agile Practices for Product Development

Presenter: Dr Suzette Johnson, Agile Center of Excellence, Northrop Grumman Corporation

Being lean and agile in the development of products is imperative where budgets are tight, schedules are compressed, and the need for innovation high. Building off the lessons from lean manufacturing we execute a flexible and disciplined engineering approach that enables us to develop features in short cycles while providing regular visibility of progress. This approach provides a rapid feedback loop for improved product validation while enabling the organisation to identify constraints and bottlenecks in the system. Through a regular inspect and adapt process we can take action to streamline processes and improve the overall product development cycle.

This presentation begins with an introduction of lean principles that support our goal of building and delivering value. The benefits of each principle and how they are implemented in product development environments are discussed. Once we understand the principles at the implementation level then we explore the practices of management and leaders in this environment. Traditional management and development practices focused on repeatability, efficiency, and scale of producing goods. While these may be important some of the focus today has shifted to increasing development flow, taking a systems view, frequent demonstrations of value through self-organising, self-managing teams, and collaborative problem solving for increased synergy and knowledge sharing. Participants will be able to identify the
principles and practices that have been successful in industry and build the foundation for accelerating flow and adaptability where people are energised and engaged to contribute their best every day. For some of us these practices are already part of our environment and you will resonate with the potential these practices offer; for others, these practices may be a paradigm shift in how we collaborate to achieve product development flow and deliver value.

3.7b Update: Technologies Advancements in Both RF Interference Mitigation and Digital IF Applications

Presenter: Mr Bob Potter, VP of Signals and Ground Systems Technology, Kratos

In the last year, there has been significant technical advancement in the areas of RF interference mitigation and digital IF technology for both military and commercial satellite applications. The former addresses the need to mitigate RF Interference; while the latter enables the transport of RF signals to virtually anywhere over public and/or private IP networks.

Satellite RF communications is a critical component of modern military infrastructures and operations, making RF interference a serious issue. For satellite based communication, as much as 1-2% of all satellite capacity is impaired by some type of RF interference. Technology to rapidly detect, characterize, Geolocate and even mitigate interference has steadily improved, and there have been significant advances within just the last year. These new advances, particularly around TDMA networks, Geolocation, and signal cancellation technology will be reviewed.

Digital IF is a new and exciting technology, in that it breaks the need for the processing equipment to be physically located near the antenna/RF systems. This leads to the possibility of exciting and innovative new architectures. This technology is already operational in military and commercial satcom systems for a variety of applications. One example application that will be discussed is how Digital IF can allow an existing satcom network hub/gateway to be extended into a new region, with only the addition of a few line cards. Digital IF offers few of the more exciting applications that will be covered in the presentation.

3.7d Product Brief: Situational Awareness in the Field and Advanced Biometrics Securing your Critical Data and Locations

Presenter: Mr Ian Hamer, Principal Architect, Fujitsu

Fujitsu has been the ADF’s strategic partner for the sustainment and support of the Defence Information Environment across all security domains for several years. We committed to the continuing development of Australia’s Defence and Security capability and to nurturing industry capabilities to support Defence. Our technology developments include the provision of Body Worn Video for the NSW Police Force and PalmSecure biometric authentication that has been adopted by a range of global customers and has a range of capabilities applicable to Defence. BWV utilised in security situations allowing commanders to gain real-time situational awareness enhancing decision making in critical events via like video feeds from each deployed officers location, coupled with the ability to review all actions in the field after the event for assessment and more realistic training for future events.

The ability to integrate PalmVein in to both Windows for logon and application security but also in to devices allows for not only data security but complete control to access of secure rooms, storage facilities and even vehicles. Matching in less than a second and impossible to duplicate has made the PalmVein the biometric security device of choice for customer ranging from door access in DataCentres and Prisons, to banking to remove the need for PIN’s and even carts for ATM access.

3.7e Product Brief: Fighting Security Challenges with AI

Presenter: Mr Vlado Vajdic, Cylance

Fighting security challenges with AI: Modern enterprises need to protect their organization's expanding network canvas against vast numbers of both known and unknown threats, and this requires a technologically sophisticated security solution. The need for endpoint protection is really nothing new, although most organizations don't spend a lot of time thinking about it. Traditional security suites can only protect against threats that have been previously identified. These legacy solutions sort through signatures stored in their database to determine whether an application meets their profile of a threat; once detected, the malicious program is neutralized. But this all depends on the program already existing within the database. Not only are there millions of new threats released each month, but there are new threats that are able to hide their presence and mimic other types of file. Through artificial intelligence, enterprises can secure a system against previously unknown threats, in addition to threats that may hide their malicious behaviour while under scrutiny.
With an overwhelming amount of data and the dynamic changes that happen in attack methods, organisations are faced with expanding risk of malicious attacks. Whether internal or external the many tools, applications and dependence on manual analysis often falls short in providing comprehensive timely intelligence. The power of advanced data machine learning models holds great promise to drastically change the way we approach cyber threat intelligence. Real time prediction using machine learning can help organisations reduce “time to action” as advanced data science methodologies gain better insight from their existing arsenal of threat intelligence tools.