MULTI-DOMAIN OPERATIONS
WEAVING THE TACTICAL FABRIC
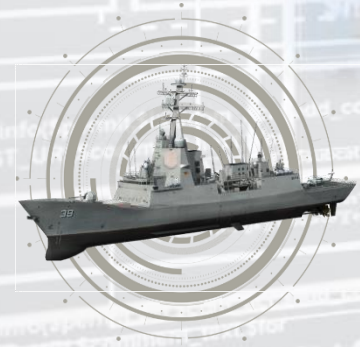
**TDL Summit
Canberra Convention Centre
11 Novemeber 2019**
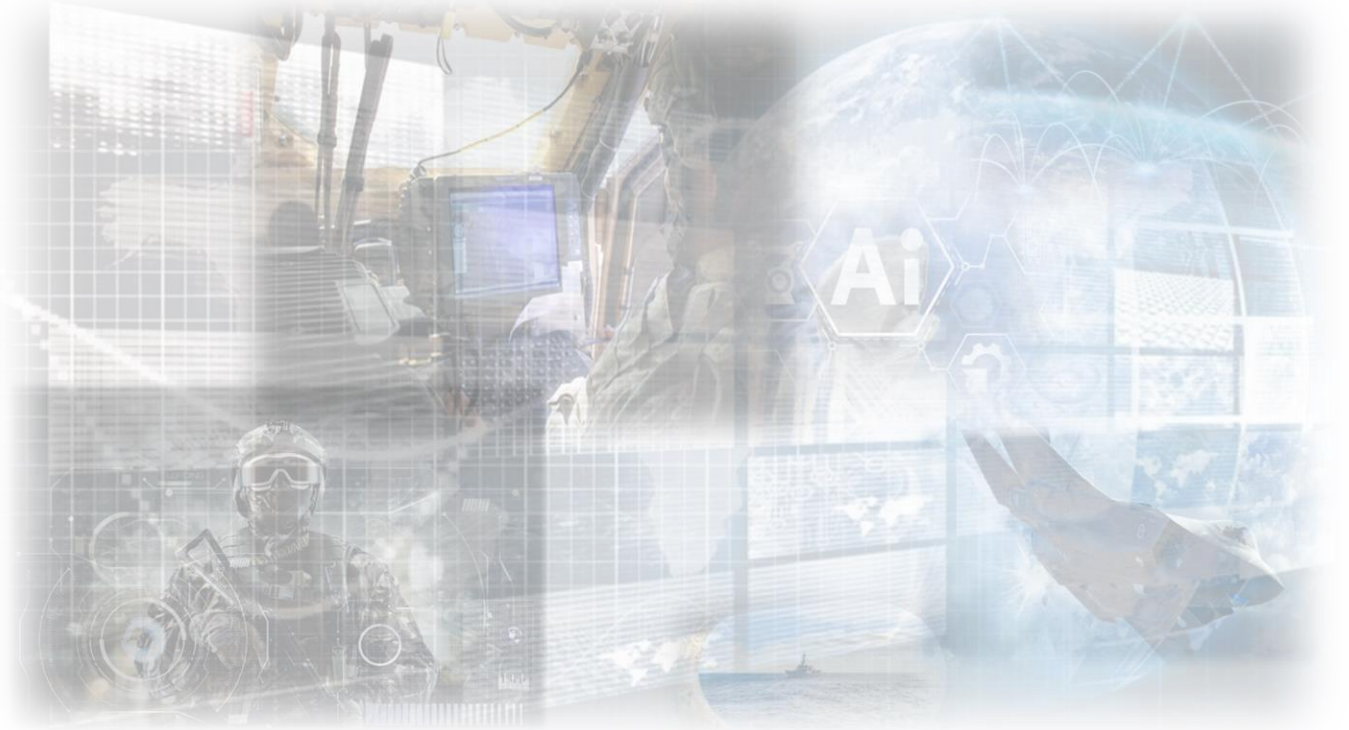
Creating a World That Works

- **Multi-Domain Operations (MDO)**
  - Characteristics + Challenges
  - DNA
  - OODA
- **MDO Layers**
  - Cyber Security + Algorithmic Warfare
  - MDO – 'AI' Insights
  - Combat Cloud
  - Quantum Communications
  - Capability Access: Technology & Capability Convergence
- **MDO Force Multipliers**
  - F-35
  - Aegis
  - NASAM
  - Sensor Netting - CEC
  - Missile Defence
  - Space
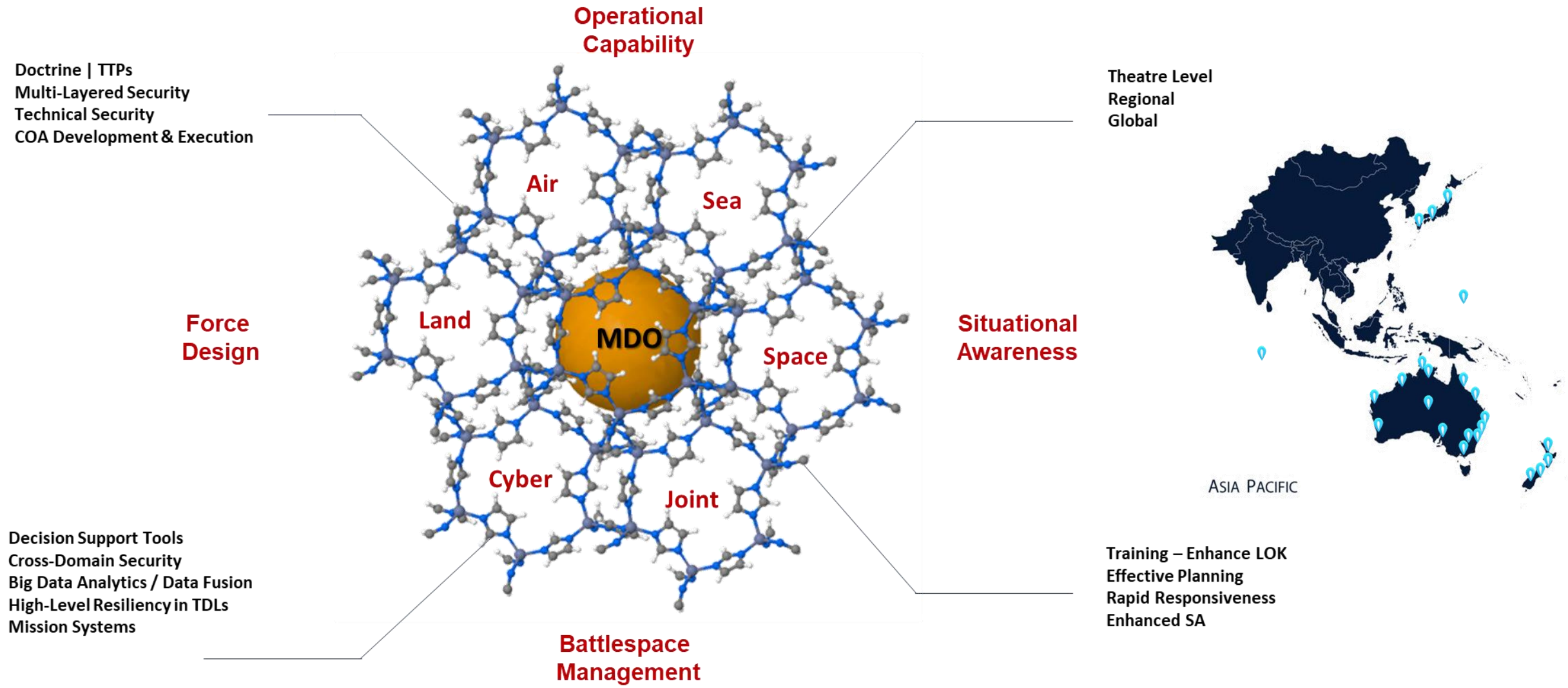- **MDO Challenges**
- **So What?**
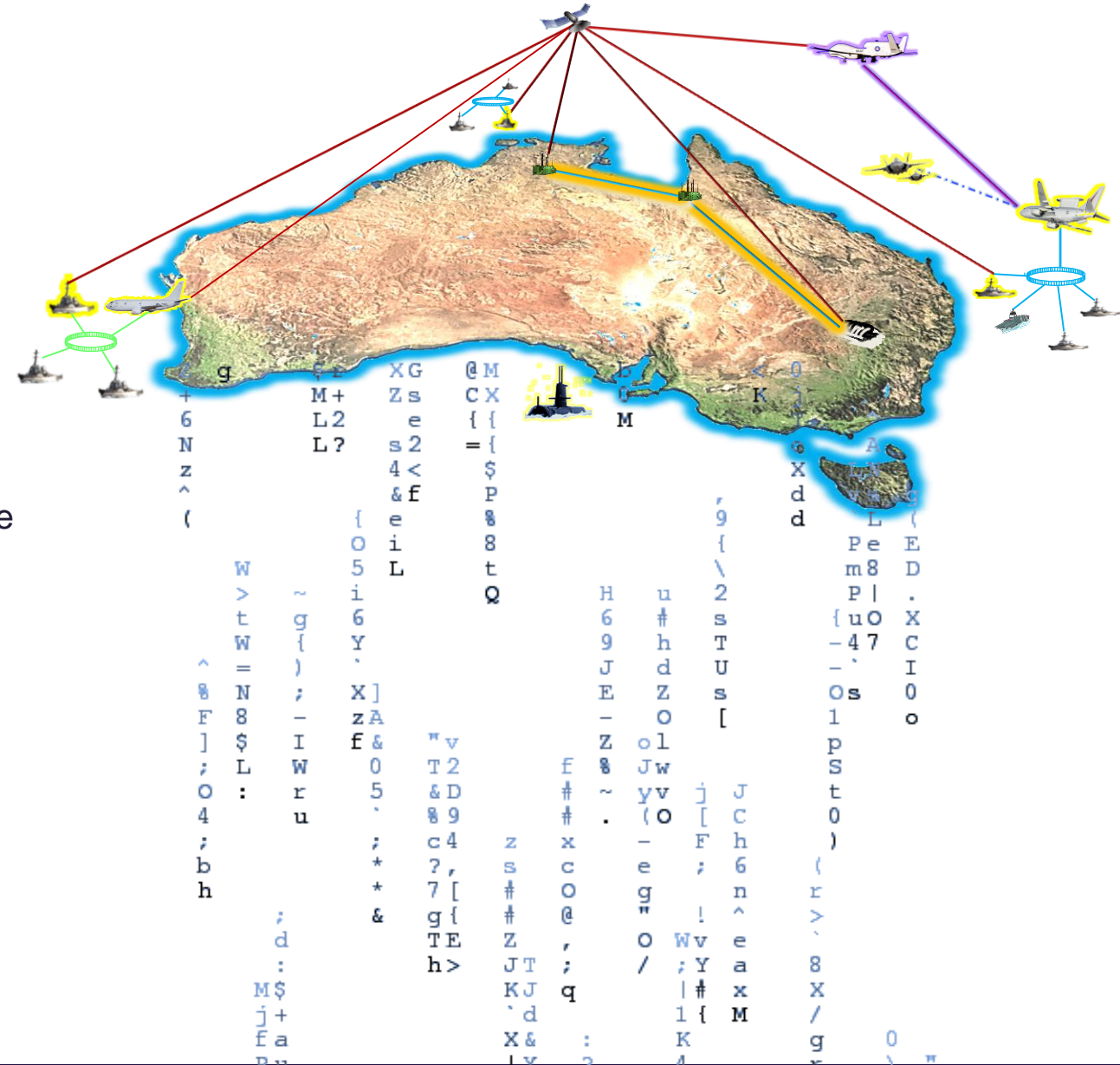
Multi-Doman Operations (MDO):

- Characteristics
  - Is Joint – not single service
  - MDO has a dynamic multi-axis!
  - It's complex!

- Challenges:
  - Cognitive Overload
  - Multiple Disparate Systems
  - Multiple Protocols
  - Culture
  - Multiple Security Levels

*"**Accelerated Warfare** provides the start-state for how we **think, equip, train, educate, organise and prepare for war.** This is a critical step in becoming future ready".* **Lieutenant General Rick Burr**

Operational Capability

Doctrine | TTPs
Multi-Layered Security
Technical Security
COA Development & Execution

Theatre Level
Regional
Global

Air

Sea

Force Design

Land

MDO

Space

Situational Awareness

Cyber

Joint

Decision Support Tools
Cross-Domain Security
Big Data Analytics / Data Fusion
High-Level Resiliency in TDLs
Mission Systems

Training – Enhance LOK
Effective Planning
Rapid Responsiveness
Enhanced SA

Battlespace Management

ASIA PACIFIC

SYPAQ

> **Information deception provides a behavioural defence, creating uncertainty and doubt in the adversary's mind and reducing the degree of trust they have in the information available.**

Cyber Security

- **Objective(s)** – ensure that Joint forces can achieve its mission in a contested cyberspace environment

- **Considerations:**
  - Manage Threat and Anomalies
  - Conduct Predictive analysis
  - Responsiveness toward Cyber-Attacks
  - Employment and Management of Electronic countermeasures
  - Employment and Management of Offensive Cyber Operations
  - Employment and Management of Defensive Cyber Operations

Algorithmic Warfare

- **Algorithm** – this is a sequence of instructions and rules that machines use to solve problems.

- **Considerations:**
  - This includes – Advanced Computing, 'Big Data' Analytics, Artificial Intelligence (AI), Autonomy and Robots
  - Algorithms may become the conceptual and technical foundation of future warfighting
  - Algorithmic Warfare is dependent on the following computing technology advancements:
    - Decades of advancement in computing-processing
    - Ability to grow and utilize large dataset suitable to train learning-cable machines
    - Steady evolution of Cloud technology

- **Considerations:**
  - Must have a clear vision
  - Must have a clear understanding
- **AI – Intelligent Automation is essential**
  - Reaction Time
  - Management of various Autonomous Systems
- **Establishing the right level of AI**
  - Trust but verify!
- **Multi-Domain Integration**
  - AI can enhance data throughput
  - AI can assist in enhanced decision making
  - AI can collect volumes of data (tera-bytes)
  - AI can enhance LVC Training
- **Challenges**
  - Still in the immature and development phases
  - Cognitive decision making ability
  - Human-in-the-Loop is required
  - Cyber Security vulnerabilities
  - Cross-Domain requirements
  - Barriers – Culture Shift vs. Risks
  - LOK - Training

Investment into AI and future Intelligent Automation is a must!

Multi-Domain – Combat Cloud

- ❏ Combat Cloud has significant technical challenges to produce a fused comprehensive picture of the battlespace in real time.

- ❏ The concept of fusion warfare provides the ability to Observe, Orient, Decide, Act in a near-real time application which depends on 3 major axis:
  - **Speed**
  - **Agility**
  - **Synergy**

Vulnerabilities

Architecture Requirements

Open Arch(s) SoS

Dependencies
- **SATCOMs**
- **Cyber**

Cross-Domain Solutions

Implied Doctrines

HW / SW Impacts BCU Cycles

Translation / DF
- **MIL-STD**
- **STANAG**
- **IEEE**

- **Joint Readiness**
- **Operational Effectiveness**
- **Impact**
  - **Tactical**
  - **Operational**
  - **Strategic**
- **Chain of Command / OPCON**
- **Rules of Engagement (ROE)**
- **Tactical Edge Authority**

- **Multi-Domain Missions**
- **Information Exchange Requirements**
- **Monitoring & Management**
- **HITL requirements vs. Autonomous reliance**
- **Knowledge Management**

- **Time Critical**
- **Throughput**
- **QoS / Latency**
- **Standards Conformance**
- **Filtering / Crypto Isolation**
- **HW + SW Layers / Requirements**
- **Cyber intrusion / Spoofing**
- **Contested / Congested**

- *Quantum Entanglement + Quantum Internet + Quantum Teleportation what does this mean?*
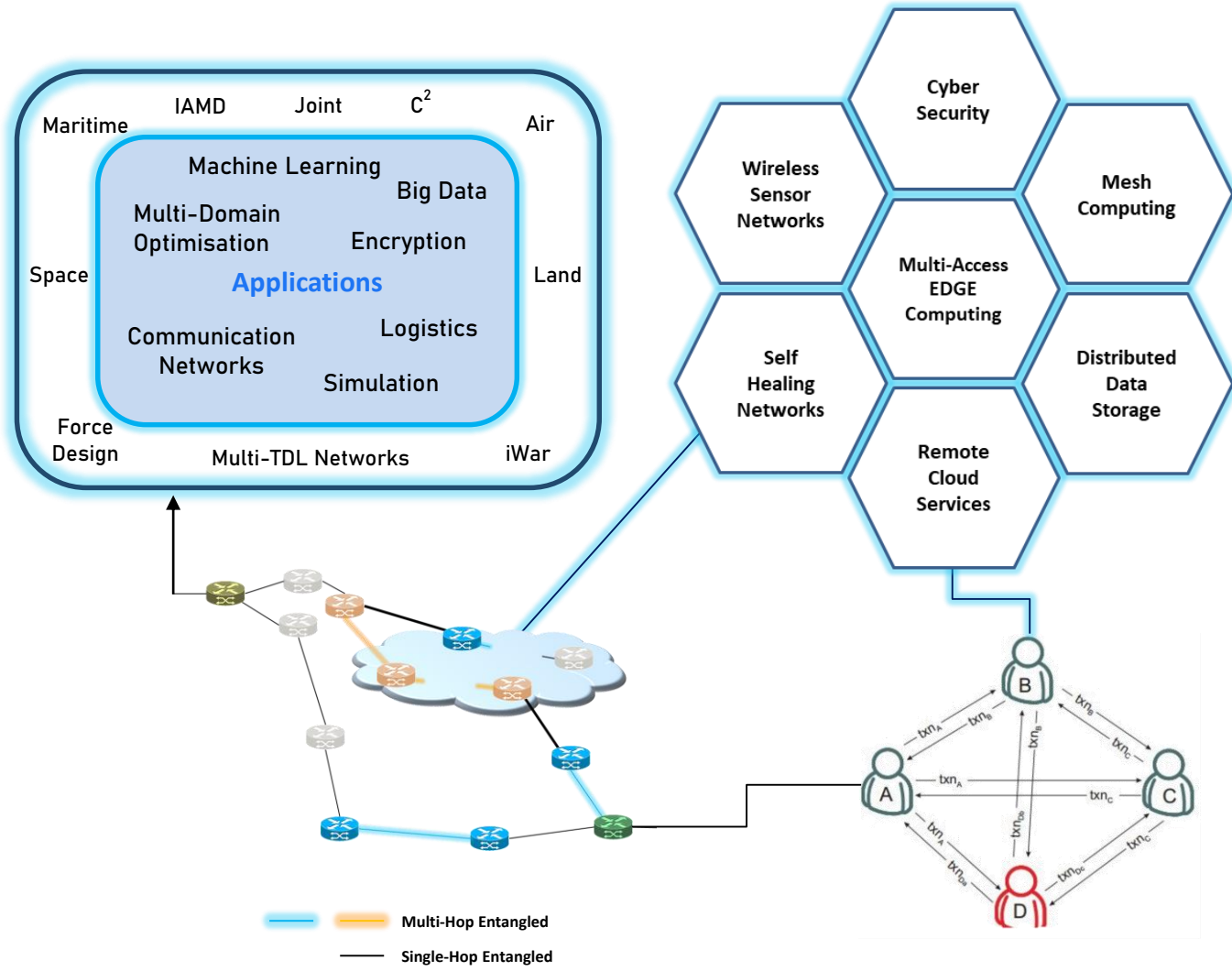
- **Qubits**
  - Building blocks of matter – electrons, proton, neutrons and photons. These are the fundamental 0's and 1's the DNA of Quantum Communications.
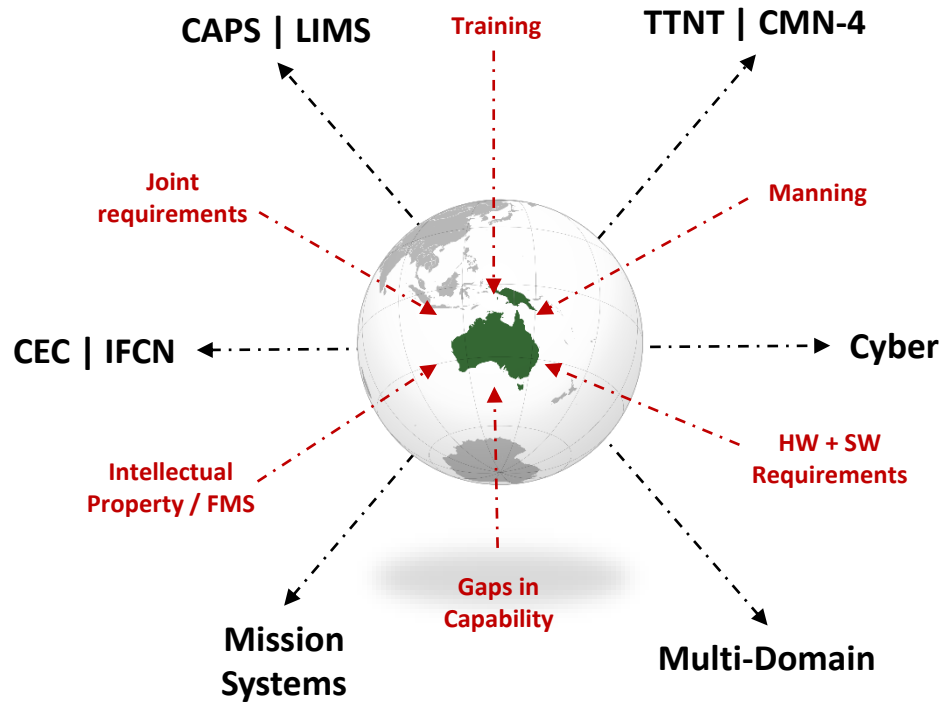
- **Benefits**
  - **Security (P) via Quantum Key Distribution (QKD)**
  - Secured COMMS
  - Secured PNT
  - Quantum Based-Sensors

- **Challenges**
  - LOK – Understanding the CAPS & LIMS
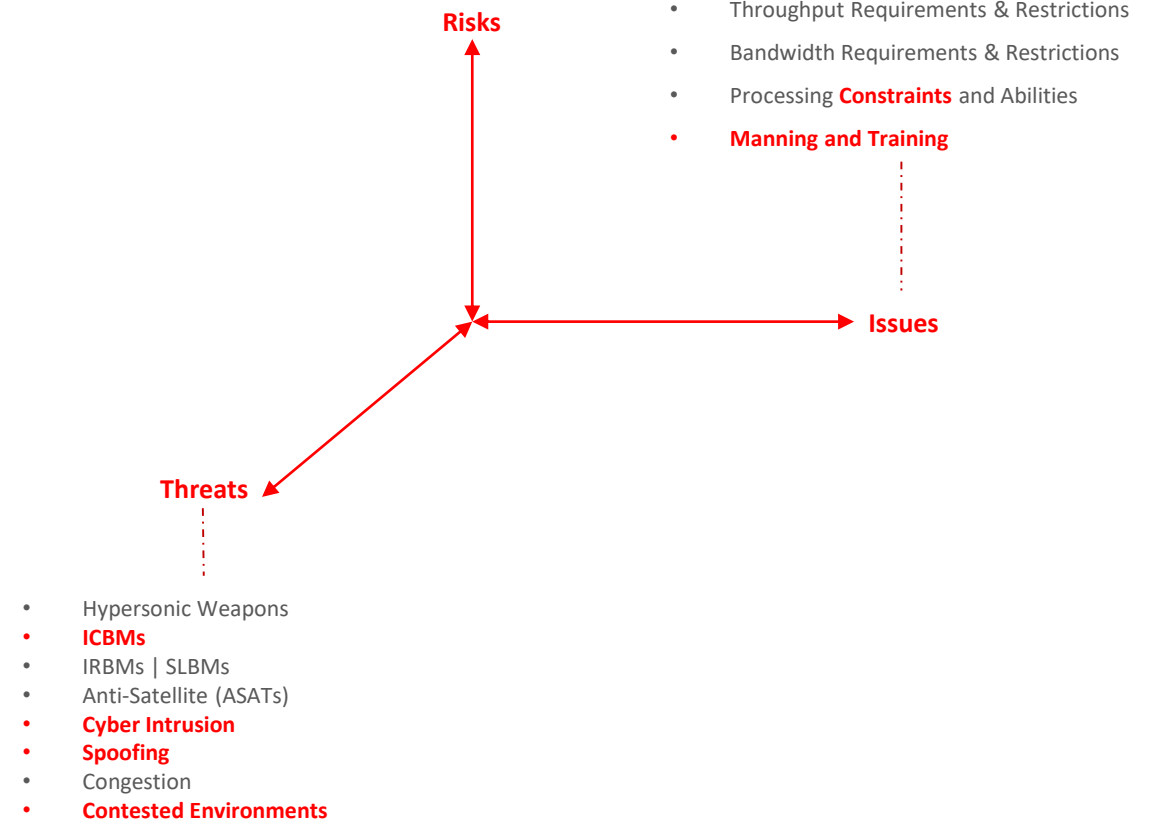 - HW requirements to ensure a True End-to-End
  - Funding!

CAPS | LIMS

Training

TTNT | CMN-4

Joint
requirements

Manning

CEC | IFCN

Cyber

Intellectual
Property / FMS

HW + SW
Requirements

Gaps in
Capability

**Mission
Systems**

Multi-Domain

G a p (s)   i n   C a p a b i l i t y

- **Requirements**
- Plug-n-Play
- Doctrine Alignments
- **IER priorities**
- Fusion

Risks

- MIL-STD / STANAG **Conformance**
- **Alignment** of these standards
- HW + SW Compatibility / Constraints
- PSI Boundaries / **Accountability**
- QoS / Latency
- Throughput Requirements & Restrictions
- Bandwidth Requirements & Restrictions
- Processing **Constraints** and Abilities
- **Manning and Training**

Issues

Threats

- Hypersonic Weapons
- **ICBMs**
- IRBMs | SLBMs
- Anti-Satellite (ASATs)
- **Cyber Intrusion**
- **Spoofing**
- Congestion
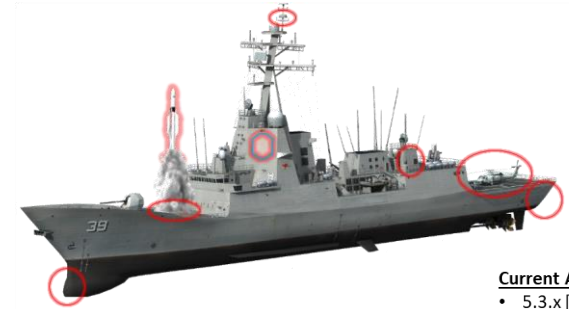- **Contested Environments**

SYPAQ

F-35

Advantages:

- C^2 Platform
- Distributed Lethality
- Adv Sensors - Enhanced Situational Awareness
- Effective and Accurate Combat ID (CID)
- Improved Cognitive Performance

Challenges

- Information Management
- Reliance on SATCOMs
- Software Vulnerabilities
- LOK

AEGIS

Advantages:

- Advanced Mission Systems
- 3D Phased Array Sensor
- Multi-Warfare capable
- Advanced Weaponry
- Advanced EW Suite

Challenges

- Multiple Baselines
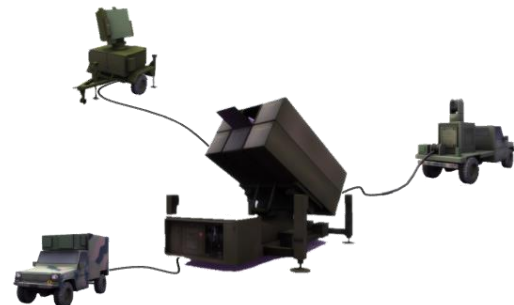- Sensor Management
- LOK

Current Aegis B/L

- 5.3.x [BMD]
- 6.1
- 6.3
- 7.1.2
- 7.1.3 ⎫ [CEC]
- 7.1R
- 8.1.0
- 8.1.1
- 9.A [Non-BMD]
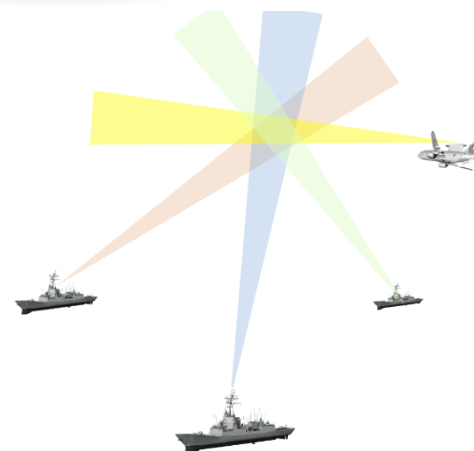- 9.C [BMD]

NASAM

Advantages:

- C^2 Platform
- Sentinel X-Band 3D Radar
- Electro-Optical / Infrared Sensors
- Fire Distribution Centre (FDC)
- Netted & Distributed

Challenges

- Sensor Management
- Information Management
- Volume vs. Threat
- LOK

Indo-Pacific Region

CEC

2000 – Aegis Class
- 30+ Platforms

2018 – Hobart Class
- HMAS Hobart
- HMAS Brisbane
- NUSHIP Sydney (2019)

2019/20 – JMSDF
- Maya Class (2019/20)

2019 – Kolkata Class
- INS Kochi
- INS Chennai

Advantages:

- High Quality Situational Awareness (SA)
- Integrated Fire Control Network (ICFN)
- Sensor Cooperation
- Composite Identification (COMP ID)

Challenges:

- Limitation - CEC Platforms
- COMP ID Configuration
- LOK

SYPAQ

- **Advantages:**

  - Addition to existing Layered Defence

  - Systems of Systems (SoS) Approach

  - Open Architecture Adaptability

- **Challenges:**

  - Integration vs. Interoperability
    - IER Management
    - Which pipe?

  - HW + SW commonality
    - Not all Mission Systems are alike
    - Filter Effectiveness
    - Sensor Migration

  - Information Management

  - Multi-Warfare Doctrine and TTP alignment

  - Threat [Hypersonics / ICBMs / IRBMs / SLBMs, etc.]

  - LOK

NASAM AEGIS - Limited F-35* Surveillance Allied IFCN

Reaction Time

Threat(s)

Future Consideration - High-Mobility Artillery Rocket System (HIMARS)
   - **Land**
   - **Sea**

- **Advantages:**
  - Pedigree + Competition
  - R&D Initiatives
  - Robotics and Automation
  - Access to Space

- **Challenges:**
  - Competition
  - Culture
  - Doctrine | TTPs
    - SSA
    - Early Warning
    - Space Sensor Management
  - LOK + Training

SPACE
SITUATIONAL AWARENESS

- Changing Character of War

- Technological Advancements (Modernisation)

- Incremental Improvements

- Cognitive Overload

- Extreme Global Competition

- Information Exchange Requirements (IERs)

- Training

- Sustainment vs. Advancements

- Obsolescence
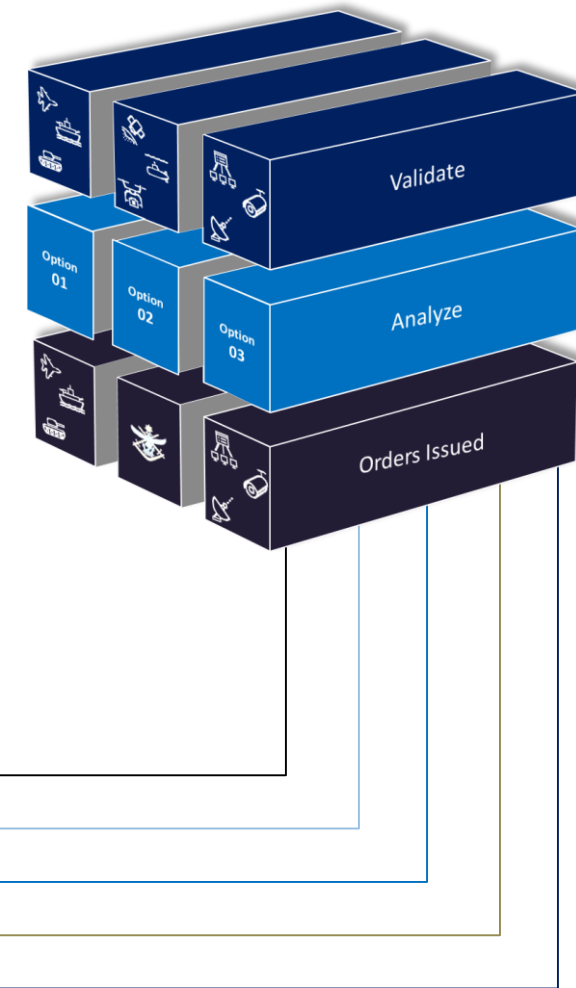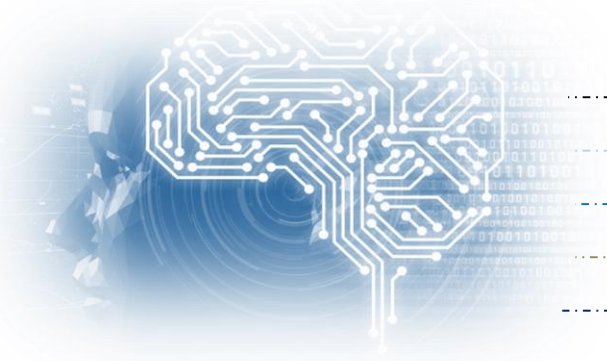
Space Domain

Cyber Domain

Air Domain

Land Domain

Maritime Domain

SYPAQ

- **How do we address the magnitude of challenges and establish an effective layer within Multi-Domain Operations (MDO)?**
  - Before we can answer this we must understand the CAPs & LIMS of our current, future and emerging technologies and that of our Coalition and Bi-Lateral Partners.

- **Importance of Collaboration** – we must address the cross-thread of capability, scalability, automation, user experience, and more to increase the LOK and most of all the ability to be effective at the Tactical Edge!
  - We must continue to collaborate at all levels of Defence, Industry and Academia

- **Cultural Barriers** – we must remove the 'Stove Pipes' and remove the check in the box mentality and expand the existing fundamental framework removing the barriers.
  - Must be aligned internally before we go externally!
  - Capability Impacts - Legacy vs. Current vs. Future
  - HW vs. SW
  - It's not 80% and Forget!

- **We must have the ability to "Train Like We Fight"!**
  - Design, Develop and Deliver within - AIC
  - If FMS - We must clearly understand what we are purchasing

- **Training! Training! Training!**
  - Must invest at all levels to be effective!

- Can we answer the following expression?

$$\frac{WFP \cdot LOK}{IERs} \bullet \left[\frac{Sensors}{Mission\ Systems} + \frac{Networks}{Platforms} \right]$$
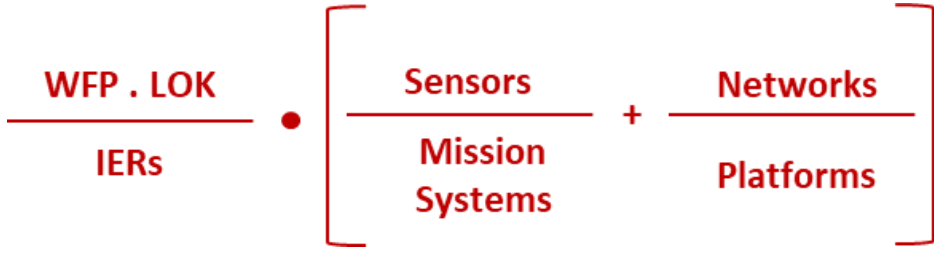
Creating a World That Works!

Russ Below
Principal JC4I and SPACE

rbelow@sypaq.com.au