AIR SPACE
ASPC's crowd-sourced blog
https://airpower.airforce.gov.au
Crawford, S (2026) *Air/Space* **5**, bp56668348
Date Published: 27/05/2026

Sustaining communications across a degraded network

Steven Crawford
Australian Defence Force

The increase in interconnected systems within the Royal Australian Air Force (RAAF) requires the creation of a Degraded Communication Exchange Framework (DCEF), to allow for sustained operational outcomes across degraded communication networks. Planning for continued operations through a highly contested network is a difficult problem to solve due to the amount of interconnected systems and functions that exist within the RAAF. To do so from a central point within the RAAF would be an insurmountable task given the likely timeline to conflict. With the assistance of a guiding framework, the process to make changes at the squadron (SQN) level will be more manageable and allows bespoke solutions to each enacting SQN. This will allow the solutions to better serve each SQNs operational objectives and their customers.

Operational outcomes are tied to current technology. Advancements in technology over the past decade has allowed for the increased interconnectivity of RAAF (and wider Defence) systems with improved information fidelity and speed of delivery to support superior operational objectives. With the advancements in network and computational capabilities, the RAAF have adapted to this advancement by migration towards technologically augmented tactics, techniques and procedures (TTPs). While retiring TTPs that have become slow and antiquated in comparison. To put it simply, we have given up the graph paper and pencil in favour of the calculator, and now find ourselves unable to operate without one. This advancement has been mirrored in civilian life with technology augmenting the way we communicate and interact with the world around us.

Current operational technology passes through targetable civilian networks. In order for RAAF networks to attain the speed and connectivity required while deployed, we leverage civilian network infrastructure as our primary connection, while Defence controlled networks are utilised as the alternate due to them being less efficient (~10 to 80 times less efficient by comparison). Due to this reliance on civilian infrastructure, any computing device attached to the global internet has been given the ability to inflict negative effects on RAAF operations through targeted civilian infrastructure attacks. Where previously an enemy force needed to be within proximity of deployed or domestic operations, now the enemy has access to the same network infrastructure that Defence data flows through from any location across the globe. This attack vector to Defence network connectivity is an obvious and known threat, but the degradation and/or destruction of the Defence networks and systems could render new TTPs useless and could require quick spinning up of older retired TTPs or communication technologies not supported, forgotten, or not prepared for.

How can a DCEF prepare SQNs for a contested network environment? The main objective of a DCEF is to help plan and build resilient communication pathways for a SQNs Fundamental Inputs (FI) and Fundamental Outputs (FO). These FI/FO pairs are the keys to maintaining operations and planning your link speed management. Once identified, the DCEF asks what is needed to allow a FI/FO to remain operationally valuable when the LSR (Link Speed Requirement) is not met or a connection is destroyed.

The application of a DCEF requires 5 phases:

1. **Identify.** The first phase would allow a SQN to identify how information is first received, processed, and then forwarded on to the customers. The identify phase would entail identifying the following:
    - **Bearer(s)**. The communication pathways that send and receive data for the SQN, these should be listed in the communication PACE plan (Primary, Alternate, Contingency, and Emergency). This could be Local/Wide Area Network (Ethernet/Fibre Optics), Radio, Microwave, or Mobile / Satellite Communications.
    - **Fundamental Inputs (FI).** Refers to data received by the SQN through the identified bearers.
    - **Fundamental Output (FO)**. Refers to the data sent out from your SQN. As example intelligence reporting, ISR (Intelligence Surveillance Reconnaissance) data, command and control, logistics plans, etc.
    - **Information Originator (IO)**. This refers to the source of the information received, which could be platforms or other SQNs/Units/Organisations that output data to your SQN as their own FO.
    - **Link Speed Requirement (LSR).** The link speed (e.g. 1Gbps, 500Mbps, 256Kbps, 64Kbps, etc) that is required for these FI/FO data streams to operate in a timely manner.
    - **Information Format and Standards (IFS)**. Information relayed can be in a form of text, image, audio, video, or other types of structured data.
    - **Information Pathway (IP)**. The path that data takes through your SQN to transform from a FI to a FO. What software is used, what team utilises the data, how is it passed between teams or systems within the SQN.
    - **Classification Requirements (Encryption)**. The control requirements listed in the Australian Signals Directorate's ISM (Information Security Manual) for classified data at rest and in transit. This ensures the secure transmission and handling requirements for the classified data.
2. **Access Impact**. Once familiar with the data requirements, it then enables the SQN to create an impact matrix to assess what varying levels of network degradation would have on their FI/FO. This also allows for the creation of possible solutions; bearer changes, software changes, changes in IFS. These solutions can then be brought forward to the next phase. Changes in IFS is the likely choice when trying to reduce the LSR, as an example changing from video to image, image to text, or text to predefined codes can decrease LSR while still allowing timely information travel.
3. **Negotiate Standards**. Negotiate with your Information Originator and Customer on what IFSs can meet the differing network speeds while still enabling operational outcomes. The suggestions used in phase two would highlight the possible changes that can be made and planned for. In order for a Unit to react to changes in network connectivity in a timely manner (while still ensuring ingress and egress of usable operational data) requires IFS to be planned, organised and agreed upon prior to network degradation.
4. **Implement Actions**. Once IFS have been agreed on, actions should be taken to prepare for continued operational outcomes during sudden changes to bearers and IFS. This can be done through software changes, user training, bearer configuration, and updated communication PACE plans. Developing methods to monitor network health and possibly automate systems to enact changes to the IFS automatically would allow for seamless transitions during operation.

5. **Monitor & Refine**. Once implemented there should be frequent tests during exercises to ensure that switching between the Primary, Alternate, Contingency, and Emergency bearers and the switching of IFS is a smooth transition with minimal cost to the SQNs contribution to the exercise. Monitoring and adjusting your LSR as new technologies arise will also be a part of this monitoring and refining process.

Conclusion

With the complex networks RAAF depends on for its network operations, it is imperative that we start preparing information resilience for a degraded network. SQNs creating their own flexible data requirements and standards allows for a faster and more decentralised approach to securing future communication. A structured approach provided by a DCEF allows a method for the identification and allocation of resources to solving this problem prior to conflict. Minimising the data footprint of FI and FO will prepare RAAF SQNs to be more agile within the Cyber Domain.