Speech to the Williams Foundation

24 October 2019

Network Requirements for 5th Generation Manoeuvre

AIRCDRE Leon Phillips, OAM

Opening Comments

Firstly I'd like to thank Air Marshal Geoff Brown AO, the Chair of the Sir Richard Williams Foundation, for this opportunity to talk to you today about network considerations for 5th generation manoeuvre. Forums such as these are valuable opportunities to consider and debate different perspectives on contemporary air power topics. I was fortunate enough to brief this forum two years ago on the challenges of Integrated Air and Missile Defence and on a personal note was enriched by the perspectives offered by the other speakers. Much of the challenges of IAMD two years ago overlap with the challenges of information sharing in a 5th generation Defence Force and I will draw out these over the course of my speech.

I will start with a story. A city is planning the build of its new prison. It has a set budget, has allocated a parcel of land and is looking to extract maximum value for its investment. City planners are sitting down with key stakeholders to agree the design but are struggling to reach agreement. Those from the justice system see prison as a punishment so are for austere, minimal living conditions that house as many as possible. Law enforcement officials see the prison as a way of protecting the community from offenders so see security as a key factor, favouring layers of access control such as multiple high fences, bright lights, open spaces, and multiple building access controls which all take up valuable space. Civil libertarians are advocating education and rehabilitation. They want to see the prison with a library, a training kitchen, meeting rooms and educational facilities so prisoners can be returned to society and contribute. The local residents association want the whole thing surrounded by trees and hidden – they primarily care for their property values. The challenge here is not a construction challenge but one of purpose and choice with different ideologies pulling in different directions, ultimately leading to stalemate. I can see parallels between this prison problem and the challenges that face us moving towards an integrated and effective 5th generation Defence Force.

Before discussing network considerations for 5th generation manoeuvre its worth a few minutes discussing the geo-political climate that Defence Forces may operate in as that should shape our force structure and operating procedures. The events of this year alone highlight the complexity of modern conflict as it moves between tension and aggression. This year has seen Iran down a US BAMS-D surveillance drone and Iranian backed Houthi rebels attack Saudi oil fields using drones of their own. These events suggest that modern conflict occurs in the grey zone, one where war may be undeclared, where non-state actors are the provocateurs and where armed force may be employed in intermediate areas and where the real conflict may be economic, social, political and legal. Is this the landscape for 5th generation manoeuvre or less technically complex and distracting examples that shouldn't alter our views that force structure should be set around high-end warfighting? The prison conundrum.

In preparing this paper I came across an excellent article in last year's Australian Defence Magasine from Ian McDonald and AVM John Blackburn on the information management environment for a 5th Generation Force and a 2017 article by Dr Peter Layton on 5th Generation warfare. I'd commend them to you. Both outline aspects of 5th generation warfare and the challenges therein. There were a few key themes that came out of these papers that relate to this topic of networks, or more holistically information management, and I'll discuss those themes in the Australian context and offer my views on where we might focus our efforts and extract best value.

Technological improvements will compress our decision making time and potentially paralyse us with choice. The threat from ballistic, hypersonic and cruise missiles will challenge any single weapon system to respond as will the proliferation of unmanned technologies. Shorter response times and the need to prioritise response options is driving the need for greater information sharing and greater system co-ordination. This has led to concepts such as 'network centric warfare', 'the kill web' and 'any sensor best shooter'. Dr Layton has suggested these networks comprise four elements – an information grid, a sensing grid, an effects grid and a command grid that binds this together. We have started to see that in practice through tactical data links such as Link11, Link16 and VMF and in the future will consider the applicability of Co-operative Engagement Capability and Tactical Targeting Network Technology. What is clear is that we need to be more network centric that platform centric.

Information gathering capabilities are growing exponentially. The ADF is equipping itself with a greater volume and breadth of sensors through the likes of P-8A and Triton and radar technology has evolved to offer greater utility in the sensor space. This means we are capturing much greater volumes of information at the tactical level. It is likely that this 'big data' may be too large to move in real time with the potential to clog our communication channels. Furthermore, our current tactical systems are becoming more heavily reliant on rich data to pre-populate them prior to mission execution. The days of punching in a few frequencies and way points before launch are long gone. The data requirements for weapon systems such as the JSF are enormous and require connectivity back to home-based support and intelligence systems to ensure effective, enduring operations.

So what do we do with all of this data? How do we extract value from it? There is much hype over data processing being the saviour. Concepts such as Artificial Intelligence, robotic process automation, machine learning, quantum computing and the like are all touted to solve this problem. To that end we are already seeing value being extracted through machine learning and data mining in the military through examples such as Project Maven, where hours of surveillance video is being more quickly processed and categorised than was humanly possible. While we will exploit these technologies into the future, there is still much more thought to be done on exactly how they will be used and what value they tangibly offer.

If information sharing and networked systems underpin a 5th generation defence force it can also be a single point of vulnerability. Near peer conflict is likely to involve some form of competition in this network space which at times may have us operating with limited or degraded communication nodes. Effort will be needed to ensure these modern warfighting networks have redundant paths, have an element of self-healing, are monitored and well defended against cyber-attacks.

So herein lies our next conflicted choice. In a constrained defence budget, how much do we spend on platform improvements vice network improvements? How much resilience and redundancy do we need in our networks? How much operational planning and training do we put into high-end warfighting, assuming assured, large data paths and how much time do we put into retrograde operations?

Rounding out this environmental scan, information dominance in a 5th generation Defence Force is characterised by a multitude of dispersed data rich sensors sharing information over multi-path networked systems being processed and fused through intelligent processors creating a rich, shared picture. Course of actions are taken using a synergistic mix of sensors and shooters at the earliest opportunity and the continuing military campaign will require a rich coupling between the tactical and strategic levels as both need to evolve to respond to an adversary's intent.

Network Challenges for Australia

Now I want to make a few observations on the specific challenges Australia may face in establishing information dominance in a 5th generation defence force. They relate to the closer coupling of tactical and strategic networks, designing our connected 5th gen information environment and data analytics.

Tactical and Strategic Networks as a Continuum

As technology and information needs have evolved, tactical and strategic networks are merging. In the past there has been a tenet that CASG delivers deployable networks while CIOG delivers fixed, strategic networks. This enticingly simple notion was struck at a time when ruggedness and reliability for deployable systems were the driving concerns and when support and sparing were the core life-cycle strategies. It was a time when these systems were predominantly isolated ecosystems, optimised around tactical outcomes. In the Australian context this has led to the disparate development of Deployable and Enhanced Deployable LANs for Army, fleet environments for

Naval vessels, customised networks in Air Force capabilities such as Wedgetail and a strategic network from which to run joint operations.

Today’s reality however requires a much tighter coupling of these tactical networks with strategic networks. This is being driven by a range of factors. Firstly there is now a greater volume of information needing to be exchanged between the tactical and strategic level for mutual benefit. At the tactical level, intelligence from strategic sources needs to be available to deployed commanders to best prepare their weapon systems and people for operations, often in a complex, somewhat murky political landscape leading to similarly complex set of rules of engagement and command direction. Similarly, the ability for ‘big data’ to be collected at the tactical edge to add to the strategic picture or identify adversary vulnerabilities needs to be drawn back to the strategic centre for exploitation and dissemination. A second consideration is the cyber threat faced by modern information systems and the need for prompt counter measures. Any lack of co-ordination between network owners risks tactical systems being isolated from strategic systems or strategic systems being vulnerable should the need for continued connectivity prevail. Finally, the ever increasing iteration of commercial ICT hardware and software that is the core of many of our networks further underpins the need for tactical and strategic networks to evolve together. Concepts such as ‘evergreen’ introduce iterative updates to operating systems, replacing the larger, but less regular, step changes associated with new software. A single, major jump from Windows XP to Windows 7 within a decade will now be replaced with six-monthly evolutions of Windows 10. While this offers more frequent and gradual modernisation, Defence may have less latitude in the timing of its software updates and will need closer coupling of the various network test environments to assure continued functionality through upgrades.

There is now a recognised understanding within Defence that these bespoke, separately developed environments cannot thrive moving forward. CIOG, in partnership with the services and the strategic centre, are pursuing a deployable network convergence strategy which will lead to a closer coupling of land and maritime deployable networks with the strategic network – both the technology and the support model. This will require closer co-operation with a wider coalition of system sponsors, testing our culture of collaboration and compromise.

Modern 5th generation information and decision needs have moved our focus from Products to Protocols.

Designing our Networks

Turning now to our connected 'network' of war fighting systems. Our defence force is made up of some very leading capabilities which have been optimised around someone else's ecosystem. JSF from the USAF; P8 and Triton from the USN; land based control systems from Israel; naval systems with the Aegis combat system from the USN. And in the future we will see UK designed Type 26 Frigates and French submarines, albeit with our choice of combat technologies. Of course these bring a level of connectivity and 5th generation robustness through improved data links and updated cryptographic security, but their development roadmaps aren't all aligned. There are perhaps competing options for us for future weapons and sensor/shooter couplings with CEC and TTNT as examples.

Further complicating this choice is the development of our own unique technologies such as JORN, Vigilare, shipborne (and now landborne) CEA radar systems and our leading edge Wedgetail AEWC capability.

So how do we move forward in a unified approach? How do we stay connected? How do we maximise the sum of the parts? The advent of our strong strategic centre is a step towards network vice platform centricity and its influence is growing as evidenced by the appointment of VCDF as the Joint Force and C4ISR Design Authority but detail is still lacking. McDonald and Blackburn, in the aforementioned article called for a 5th generation Information Management Environment CONOPS and I *strongly agree* this is not only necessary but one the warfighting community must own, more strongly supported by capability owners and CIOG. This is not an a task to be left to the ICT shop. I say this because ultimately I believe it will come down to trade-offs and choice and that is a business decision not a technology one. Our very own prison conundrum.

This CONOPS is not an easy task either. Having read industry proposals for AIR 6500 a few years ago it is clear that when it comes to unifying and connecting systems there is no 'plug and play' and each vendor took ideologically different approaches. I have seen this difficulty also play out in Wedgetail. Having spent the last few years driving some of the early thinking on our Ph6 capability upgrade, at least from an industry engagement perspective, it is clear we will need to be pragmatic to fit within the prescribed budget and timeline.

Despite these difficulties we should not shy away from developing this 5th gen CONOPS to agree our roadmap. I believe we need to invest more in modelling and simulation so we can compare technology choices and importantly their costs, with a range of '5th gen' scenarios. We need to model these in both free and contested network conditions and most importantly use it to broadly educate decision makers. We are better placed now than ever before to understand US technology roadmaps to feed these models. Our move from Foreign Military Sales arrangements to co-operative partnerships for the JSF, P-8A and Triton now means our people are embedded within the US's forward planning cycle, offering us better and earlier insight into their capability roadmaps and influence over what is important in *our* ecosystem. We need to make the more of this opportunity.

Where we have more direct control over design choices like we do for the Australian sponsored systems I mentioned earlier, we should invest more heavily there – both in people and budget – so we can seize opportunities to better share and process information. Only here can we potentially break down the ITAR, IP and compartmented security layers for our own integrated effect. US upgrade cycles may drive what individual capabilities we get but our own systems can be iterated to be the unifying and integrating 'glue' that binds them together.

Data Analytics

Finally a comment on 'big data' and data analytics. I stated before there is much hope, arguably hyperbole in this space. Here we must be more adventurous if we want to extract value. We must form better partnerships between sponsors, users, our delivery agencies such as CIOG and industry.

We must fund this development and we must own and control it. It is iterative and it is very much 'churn and learn'. We need to acknowledge this is R&D work and subject to risk. We will need the courage to allocate decent funding here without certainty of outcome. This is not Costco buying where we leverage US economies of scale by buying in packs of 6. Like all good investment portfolios, there should be some money slated for high risk, high return ventures. The real Jericho challenge is to convince the Investment Committee and Government of this.

Noting the volume of data we capture and the likelihood of constrained data paths, I suggest this data analytics needs to be at both the tactical and strategic level to ensure only data of value is kept and shared. For instance, you can collect a lot of imagery on a maritime patrol flight but how much is useful? Processing at the tactical edge to extract more immediate value and sharing only what is of value is paramount. Opportunities exist to use our developed and controlled technologies such as our converged deployable and embedded networks to be the hub of this effort. It's the applications that are hosted here that we need to invest in with a tighter coupling of strategist, warfighter, delivery agency and industry.

At the strategic level there will be an abundance of data. Data from allied sources and data collected over days, months and years. Combing through the data, perhaps more slowly than at the tactical edge, can offer us early queues on our adversary's intent. Earlier on I mentioned the geopolitical landscape and the murky nature of modern conflict. Data analytics at this level may need to expand beyond traditional military sources, depending on the circumstances. How much social media and public information would we also be interested in? Having an agility to respond and evolve our analytics given the strategic circumstance we find ourselves in is important. Again, investment in Australian owned and developed data systems allows us this flexibility.

Conclusion

In conclusion, modern, 5th generation defence forces, will need to be competent across the continuum of conflict, supporting times of political tension through to high-end peer to peer warfighting. This left and right of arc has the potential to leave us conflicted with choice over exactly what our data and network needs are. Notwithstanding, technology growth is leading to a greater array of more complex sensors and shooters, dispersed across the battlefield. We face the threat of faster, more agile hypersonic threats and the proliferation of disruptive technology offered by cheaper drones as well as attacks on our networks. For us to be effective we need to ensure our systems are well connected, through robust, multi-pathed networks and that we are capable of operations despite degraded networks. Data exchange between tactical and strategic networks offers us competitive advantage and we need to recognise the merging and synergistic nature of both. We are benefiting through our investment in high-end warfighting technology however need to think more deeply about the information exchange between these and our CONOPS so we make the best investments and tradeoffs in a fiscally constrained environment. Finally, we must invest more heavily, both intellectually and financially in the development of weapon systems and C2 systems that *we* develop as they give us control in how we bind and glue our tactical systems together, ensuring *our* ecosystem is optimised.