POLICY ANALYSIS ASPI

ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE

ADF capability review: C4ISR(EW)

by Douglas Abdiel and Andrew Davies

30

28 August 2008

This ASPI *Policy Analysis* is number four in a series intended to inform the Defence White Paper debate by providing a snapshot of ADF capability. The previous releases in this series considered Navy, Army and Air Force capabilities.

Introduction

Over the last few years, the concept of network centric warfare (NCW) has been at the forefront of planning for the way the Australian Defence Force will conduct warfare. The basic idea is that the ADF will use advances in communication and computer technology to take advantage of the sensors and systems of its various components, wherever they are located, and be able to draw the collective data together into common operating pictures. In the world of NCW, the 'fog of war' can be pierced by advanced sensors which immediately transmit their information to a network of men and machines that orient, decide, and act on that information in near real-time. Acknowledging the limits of similes, C4ISR is to the ADF what the nervous system, eyes and ears are to the human body.

NCW requires a number of underlying technologies, including a communications architecture, sensors and processing and data dissemination systems. And, of course, the users of those systems have to have a shared understanding on what data needs to be collected and shared, and how the actions of the various players on that network will be coordinated and controlled. The somewhat unwieldy term 'command, control, communications, computers, intelligence, surveillance and reconnaissance' (C4ISR) is used to describe the underlying systems and the means of collection and dissemination of the data (especially, but not limited to, positional information) that will form part of the traffic on the networks. This paper provides a snapshot and critique of current ADF C4ISR capabilities and details future plans.

Not surprisingly, the ADF's vision of the future is quite different from current capabilities. While it has made progress in networking, it has done so unevenly and still faces immense challenges before it can realise a fully-fledged NCW capability. While there is a joint vision for the implementation of NCW, the development of many of the enabling steps (such as a communications architecture) has not been coordinated well but is often environment (i.e. land, sea and air) specific. There are numerous

legacy systems that must be replaced or integrated into a future network. Australian forces may be called upon, either as a leader or member of a coalition, to operate alongside allied or other forces who will bring their own networks to the operation. And the modern battlefield is as large and complex as any of its historical counterparts, featuring urban terrain, and irregular combatants and non-combatants. As well, the technology is only part of the story. There will need to be significant investments made in doctrinal developments and training before the advantages of NCW can be fully exploited by the ADF.

NCW is not without its risks. Active, thinking enemies may be ready to exploit our newfound technological dependency, and seek to disrupt or deny the networks our forces will be relying upon. Technologies such as network attack and anti-satellite missiles could deny the flow of information at crucial times, and proven techniques of jamming and spoofing can disrupt sensors. The communication architectures that enable NCW must be hardened and resilient, and be able to resist attack and to repair themselves when disrupted.

Ideally, a networked force should know in relevant detail the physical environment, the location of neutral parties, and the movements, capabilities, and intents of all enemy, neutral and friendly force elements. It should be able to respond in a precisely coordinated way. For example, when US Army General William Hartzog conducted combined arms training with his division, he would persist until he could get one rifle bullet, one artillery shell, and one Hellfire missile to all hit the same moving target simultaneously. Rather than an intended war-fighting technique, the aim of the exercise was to perfect the seamless and real-time exchange of information required to achieve such coordination. If a joint force can pass the 'Hartzog test', it almost certainly has the connectivity and coordination to perform joint operations.

Electronic Warfare (EW) is often excluded from C4ISR but has many operational and technological overlaps. For example, surveillance of the electromagnetic spectrum for adversary transmissions and subsequent direction finding to locate transmitters is part of intelligence, surveillance and electronic warfare. (As well, EW involves applications such as radar warning and self-protection of ships and aircraft.) EW adds greatly to the effects produced on the battlefield, so this paper briefly discusses EW in addition to C4ISR. (Some of the ADF EW projects are also discussed in the project brief section of this year's ASPI Defence Budget Brief.)

The ADF has developed 'roadmaps' for its future ISR and NCW capabilities, which set out the steps and desired end state for the ADF's capability. With these developments in mind, this paper will elucidate the gap between where the ADF would like to go and where it is, by providing a snapshot of its current capabilities. It will also address where future plans are inadequate or where current plans have failed to deliver some of the building blocks that will be required. More than the other three papers in this series, there has been a spirited and frequently divergent set of responses to drafts from ADF reviewers. Some of our judgements are not universally shared. We see that as reflecting the relative immaturity of the subject—in many cases the potential of C4ISR technologies is yet to be fully exploited.

The main disagreement is with respect to what is termed 'horizontal' and 'vertical' connectivity. The former involves the networking of ADF elements at the same level (e.g. small groups or individual soldiers, ships, aircraft etc) and the latter to the links between various levels of command. The authors are of the view that extensive networking is highly desirable in both domains. Application will depend on circumstances, but it is preferable to have flexibility

rather than to be limited by systems and doctrine. Recent conflicts in urban areas amid civilian populations provide good examples of the desirability of excellent situational awareness at all levels. A concurrent trend has been the use of networks and real-time data to push command decisions further up the hierarchical command structure. While sometimes valuable, this is not always positive. The key is to use these capabilities to make decisions at the *appropriate* level for the circumstance. The answer will lie in training and development of appropriate doctrine—which will sometimes be quite different from the past. Rather than 'shoe-horning' C4ISR technology into existing models, practices and structures will have to evolve to embrace new possibilities.

To the non-specialist reader, this is a somewhat arcane topic. The lay reader may prefer to read the overview that follows and omit the detailed discussion that follows. Every effort has been made to make it digestible, but a certain amount of jargon is unavoidable. Definitions of relevant terms and some other related concepts are included as an annex to this paper.

Overview

Command and control

Australia has shortfalls in its current C4ISR capability, particularly at the tactical level, and command and control systems are especially problematic.

The future development (and current support) of C4ISR capabilities is managed centrally by 'joint' (tri-service) authorities. In time this should result in improved levels of integration but currently each environment is serviced by parallel systems with varying degrees of interoperability and a plethora of 'legacy' formats and interfaces. A number of projects are in train to address current limitations (see the Annex: C4ISR Projects). However, we judge that the goal of obtaining a 'Networked Coalition Joint Task Force' seems very optimistic in relation to the projects that are currently in train.

Under current plans a joint commander would be able to know the disposition of his enemy with a reasonable degree of certainty (especially in areas close to Australia). There will never be a perfect enemy picture when fighting a determined intelligent enemy and adversary intent will often be unknown. (The picture of neutral forces remains problematic, though it is very important in current conflicts.) Coordinating multi-service assets to maximise combat effectiveness and to minimise the risk of 'friendly-fire' incidents would be difficult. And, since this level of control is difficult at the operational level, it becomes even harder at the tactical level, where communication and decision-making timeframes are further limited.

Communications

The communication architecture of the ADF is not currently suited to genuine joint NCW. While cross-service voice communications are generally available (albeit at varying degrees of reliability and connectivity), the ability to share tactical data between the services and to establish common operating pictures of the land, sea and air environments is highly problematic. Voice communications are often adequate for conveying executive orders and critical information, but not for providing full situational awareness information.

Given the fast 'generation' time in communications and computing technologies, it is difficult for multi-year projects to deliver 'state of the art' solutions. As a general observation, communications architecture projects work best when they are 'off the shelf' purchases of proven systems.

Where bespoke Australian-unique solutions have been sought, the result is frequently a protracted and troubled program—a good example being the modernisation of the ADF's high frequency radio communications.

Today a shortage of bandwidth limits the application of modern communications to the military, and requirements will only grow with time. A number of projects now underway will provide greater bandwidth for many applications, which will provide opportunities for more extensive exchange and exploitation of data between ADF elements. For example, Australia recently signed an agreement with the United States to participate in the Wideband Global SATCOM system. This 'off-the-shelf' purchase should provide a good capability for the ADF and greatly facilitate connectivity with US forces.

Intelligence

Australia's intelligence of state threats is robust in Southeast Asia and, under a division of effort agreement, we receive information from allies on developments outside of our region.

Post the 9/11 attacks, intelligence sharing and cooperation between agencies of the Australian Intelligence Community has improved markedly. The Iraq WMD saga highlighted some cultural differences between the Office of National Assessment (ONA) and Defence Intelligence. The 2004 Flood inquiry made recommendations that address these issues and, while progress has certainly been made, it seems a safe bet that ongoing reforms will be required.

Australia's ability to obtain information about non-state threats such as terrorists and smugglers is limited, although it has improved in recent years as extra resources have been allocated to the task.

Surveillance

Surveillance is ongoing, systematic observation, often over broad areas. Australia's surveillance capability is good in the immediate approaches to Australia and adequate in Southeast Asia. Further afield, it is primarily limited to allied assets, priority and availability of which is negotiated on a case-by-case basis.

The Jindalee Over the Horizon Radar Network (JORN) is a very capable system that provides coverage against moving targets over very wide areas. Its capability is degraded, sometimes significantly, at dawn, dusk and during periods of increased solar activity. In those circumstances surveillance relies on other assets.

Airborne surveillance will improve markedly over the next decade as the Wedgetail Airborne Early Warning and Control (AEW&C) and new manned and unmanned maritime patrol aircraft join the RAAF's fleet. The unmanned aircraft will provide a significant boost in terms of persistence and will greatly increase the areas able to be surveilled. The capability boost will be in aerial and maritime surveillance. The ongoing operations in Iraq and Afghanistan have provided an opportunity for Australia's unique AP-3C maritime patrol aircraft to perform land surveillance. With its Infra-Red Detector System and Electronic Support Measures systems complimenting its radar, the AP-3C has proven to be a useful land surveillance and coordination platform.

By virtue of their nature, small, slow moving boats (especially wooden ones) in the air–sea gap will remain difficult to find and track.

Reconnaissance

Reconnaissance operations are often cued by observations made during surveillance activities, so responsiveness is an important attribute of reconnaissance capabilities.

Australia's reconnaissance assets are limited in their capability, even in the near region. Australia's aging F-111s are its only Imagery Intelligence (IMINT) platforms. In the future, unmanned surveillance aircraft will provide IMINT capabilities. Given the vast areas around Australia, the effectiveness of the AP-3C Orions is limited by the size of the fleet, their speed and base locations. Replacement maritime patrol aircraft will be faster and have more modern sensors, but will operate in smaller numbers than the current AP-3C fleet. Army are operating a range of unmanned aerial vehicles for battlefield reconnaissance and more will enter service in the years to come.

Other reconnaissance assets include Army's Special Forces and Regional Force Surveillance Units, and Navy's submarines and patrol boats.

Electronic warfare

The ADF has experienced difficulty in establishing robust defensive EW capabilities on its major platforms, with integration issues frequently resulting in delayed delivery, underperformance, or both. Electronic attack capabilities are almost nonexistent in Army and Navy and current plans and acquisitions to fill this gap are piecemeal and do not provide any capabilities beyond the tactical/unit or platform level.

Capability summary

Command and control

Any time that different types of weapons systems are used, those weapons systems must be coordinated for effect on the enemy and for own-force safety. Otherwise, potentially catastrophic friendly-fire situations could occur. For example, the trajectory of artillery rounds must be coordinated with aircraft that may be flying through the same airspace. This requires coordination of command systems and unity of command.

The coordination of different weapons systems on the battlefield is important beyond the need to avoid own-force casualties. Coordination of weapons is often the key to tactical success. Just as when Australia's Sir John Monash pioneered the tightly orchestrated employment of infantry, armour and artillery to break through the German lines in 1918, the effect of coordinated arms continues to be greater than the sum of the parts. Modern technology allows increased flexibility for the employment of multiple weapon systems.

To help in this process computer programs called 'command support systems' have been designed to provide the commander with a common operating picture (the real-time location of friendly, adversary and neutral forces), briefing tools, mission planning tools and logistics information systems. With these systems, the commander is able to make decisions on the assets best suited to achieving the desired outcomes, providing resources to units, and disseminating information for review and analysis.

The five command systems used by the ADF are:

- Army: Battlefield Command Support System (BCSS), which has been successfully deployed since 1999 down to the infantry company and cavalry troop levels
- SOC: Special Operations Command Support System (SOCSS)
- RAAF: Theatre Battle Management System (TBMS), a component of a broader Air Command Support System (ACSS)
- RAN: American-developed Global Command and Control System-Maritime (GCCS-M)
- Joint: The Joint Command Support System (JCSS) which coordinates other command and control systems—in use on the HMAS *Manoora* and *Kanimbla* and at the Operational and Strategic levels

The future evolution of these systems (under Joint Project 2030) and their current support are jointly managed. Currently there is good interoperability between some of these systems, but not all of them. The following systems have good interoperability with each other (although this depends on the message formats being used):

- BCSS—JCSS—SOCSS (Army, Joint, SOC)
- GCSS(M)—TBMS (RAN, RAAF)
- JCSS—GCCS(M) (Joint, RAN)

All five have good interoperability with their American counterparts, in some cases better than they do with each other. (Again, this depends on the message formats being used.)

While there are good reasons to have different end-user screens that are tailored for the environment a commander is operating in, efficiencies would be possible if hardware and software could be standardised as far as possible. Systems should be able to accommodate various message forms, but particularly the different types of Variable Message Format (VMF), as this is what our allies and NATO are using. While it seems easy enough to enunciate those high-level specifications, the longevity of disparate legacy systems makes the practice difficult.

Ultimately, the ADF would like to achieve higher levels of interoperability than is currently the case, but that will be achieved in gradual steps that allow improvements with each generation of equipment and leads to a future truly joint system. This will not easily be achieved, and some of the work currently underway illustrates potential pitfalls.

For example, the ‘Vigilaire’ Project, is intended to integrate air command, control and communications and to provide a Common Air Picture (i.e. the location and tracks of aircraft) built up from data not just from Air Force radars, but also from the Jindalee Over the Horizon Radar (JORN) and, in the future, Navy’s Air-Warfare Destroyers. The project has experienced several major setbacks (see the project brief in ASPI’s Defence Budget Brief 2007-08 for more details) and is now three years behind schedule and not due to be released until 2010. From the point of view of a future joint system, Vigilaire will be a ‘legacy system’ that will require further development to allow commanders in the different environments to extract relevant information and integrate it with their own. And not long after its completion, Vigilaire will need to be integrated with the deliverables from phase eight of Joint Project 2030, which is intended to produce an ADF Joint Command Support Environment and is planned to enter service in the 2014–2016 timeframe.

Communications and computers

As most communications systems are still environment-specific, they will be disaggregated and then cross links will be discussed.

Army

Communications remain a problem for the Army at the tactical level, presenting challenges for the decentralisation of control. The ability of commanders to communicate their intent from the joint headquarters is quite good to operational command levels, but attenuates in the last few kilometres to forward deployed forces. Equally importantly, it is difficult to transmit back the data from a soldier in the field to incorporate it into the common battlefield picture. Projects LAND 75 and LAND 125 will provide these capabilities in future. (See Annex)

A Company-level field headquarters is the lowest level where the Army can claim to have some semblance of a common operating picture (discussed below in the Joint Capabilities section). In the field headquarters itself, presuming it is not aboard ship, the Army has several deployable Local Area Network systems that allow it to communicate over existing or new infrastructure.

After the field headquarters the bandwidth drops rapidly; and any semblance of a common operating picture and back reach to the Defence Wide Area Communications Network (DWACN) is lost. Only a few soldiers have the ability to communicate back to the field headquarters using the RAVEN and WAGTAIL radio systems, even these have low data rates and can only transmit or receive (not both at the same time—a.k.a. 'half-duplex'). These systems also require that a frequency management computer program be used to coordinate frequency-hopping and encryption data. The redeeming feature of the RAVEN and WAGTAIL is that they can be interoperable with Australia's allies, the UK and US. Very few soldiers may carry a secure data terminal which gives them basic computing and text capabilities. This limited data is nothing like what will be needed to obtain near real-time ammunition, casualty, photo, and video reports from units in the field.

It is not always necessary for all tactical elements (including individual soldiers) to be networked. A balance must be struck between networking and maintaining hierarchical command structures. But having the capability to network down to the smallest tactical unit is sometimes important—for example in complex urban environments, where the locations of individuals in complex terrain and amongst a civilian population is critical knowledge. Individual Australian soldiers may or may not have a secure personal radio which is capable of communicating with their section or their platoon and in many circumstances will have no reach-back capability to the field headquarters.

Navy

The RAN is the most networked sub-organisation of the ADF. This is largely because it has a very limited number of communications nodes, and because internal shipboard communication is fixed. All RAN major units are fitted with mobile versions of the same command and control networks and applications that exist within the fixed, strategic network of the DWACN. When each ship goes through major refit, the IT equipment is replaced with the latest fit. While some units may still have low-end equipment, all will be upgraded on a regular cycle.

Between platforms the RAN has good interconnectivity. Even the smallest ship can communicate on various bandwidths and through various communication platforms. Small boats have LF/MF/HF/VHF/UHF and satellite communications (SATCOM), all run through the Integrated Ship Communications System, while larger ships have higher capacity systems. Ships have satellite reach back provided by INMARSAT, or the WGS and HF reach back thanks again to the HFMOD.

Submarines have similar capabilities via their communications mast, but that is only usable when they are at periscope depth. Because radio-waves are strongly attenuated by sea water, communications to submerged boats are limited to very low frequencies or extremely low frequencies, with low-rate data transfer.

Air Force

Many of the RAAF combat air platforms were 'born' connected as they were acquired from the US Navy and thus are fitted with established systems. They have frequency-hopping VHF and UHF SATCOM communications. Tactical data (such as the tracks of other aircraft) is passed from aircraft to aircraft by Tactical Digital Integrated Links (TADILs). The TADILs on 'classic' Hornets and the soon-to-be-delivered Super Hornets are Link-11 and Link-16.

Link-11 is based on 1960s technology, where information is either transmitted or received sequentially, and because of its limited ability it is only occasionally used for more than radar tracking information. It has, however, successfully been used by the RAN and RAAF to provide inter-service data communications, as well as being used in international activities. Link-16 was designed to take advantage of developments in computer and communications technology, and is used to disseminate mission planning, electronic warfare, weapons assignments and surveillance information. However, Link-16 is available in a range of configurations, and Defence is being appropriately cautious in adopting the system in order to avoid being left with 'orphan' systems.

The Wedgetail will add a great deal of communications capability to the Air Force as well as to joint forces. It will be able to operate HF, VHF, UHF, Link-11, Link-16, UHF SATCOM and ICS.

Joint capabilities

In garrison or in the joint facility in Bungendore, the ADF maintains the Defence Wide Area Communications Network (DWACN) which has secure data, telephone, fax (these are much higher resolution than civilian facsimile) and telegraph. The DWACN is common to all of the services and by all accounts is functioning well, and supports the command and control systems detailed earlier, as well as allowing such functions as email and database sharing between widely dispersed units and across the services.

The DWACN has been linked to the Parakeet Satellite communication system as well as the High Frequency Modernisation program so that field headquarters will have access to many of the same services as they did in garrison. The current weakness in this system is for mobile units that cannot be fibre-optically connected to the Parakeet, resulting in a 2Mb/s capacity from a line-of-sight radio which constrains bandwidth for the communications to be carried.

In terms of tactical systems, the RAAF is largely cut off from the Army in all but voice communication, though it has good connectivity with the RAN because many of the communications platforms for both the RAN and RAAF were acquired from the US Navy. Connectivity with the Army is being improved under the Joint Terminal Attack Controller (JTAC) initiative, which is being used in theatre in Afghanistan to coordinate allied air support to land forces.

The RAN is well connected with the Army at the Operational level. The RAN has even fitted the HMAS *Manoora* and HMAS *Kanimbla* to be mobile joint headquarters ships which provide advantages over a field headquarters in terms of risk and connectivity. In the future the amphibious ships (LHDs) will fulfil a similar role.

At the tactical level, joint connectivity is limited, though functional for some roles. On land there is a limited ability to track larger assets such as tanks, but it is problematic to track individual infantrymen, so coordinating naval and air-to-ground fire is more dangerous. The capability to track friendly forces will be improved under project LAND 146 (see Annex), but until that time it will be difficult for the joint commander to know the location of his own units.

One application where increased connectivity may require a rethink of doctrine is fire support. Currently few soldiers have the ability to call for naval gunfire support, air support or artillery. These tasks are reserved for the few soldiers who have the correct type of radios to communicate with these platforms. But a more integrated approach is possible. For example, the US Marine Corps has just stood up several Air Naval Gunfire Liaison companies which coordinate joint fire across all US services. And even that is seen as an interim step towards a model where all marines are able to call for fire support when appropriate.

The last few kilometres remain a difficult area for communications. Control of all of the ADFs military assets are not pushed down to the platoon and section leaders let alone individual soldiers at the edge of the battlefield. This lack of control limits the speed at which the individual soldier can respond to enemy threats.

Intelligence

Military commanders have requirements for intelligence on a number of timescales. Real-time (or, in practice, near real-time) intelligence is highly perishable information on the immediate movements and actions of battlefield players. Assessed intelligence is the result of deliberation over information sourced from a variety of inputs, such as human agents, radio interception, imagery etc.

Defence maintains its own Canberra-based intelligence agency, the Defence Intelligence Organisation (DIO), which has the role of providing ADF commanders with assessed intelligence. DIO is staffed by a mixture of civilian and military personnel. Most military headquarters also have an intelligence cell consisting of uniformed officers.

At the national level, Defence has two intelligence collection agencies. The Defence Signals Directorate (DSD) is the signals intelligence (SIGINT) branch of the defence intelligence establishment and is responsible for the collection of communications and electronic intelligence. The Defence

Imagery and Geospatial Organisation (DIGO) is responsible for providing (mostly satellite-sourced) imagery. Allied and commercial satellite imagery is acquired and disseminated as required. DSD and DIGO are both well connected to allied agencies, and are able to effectively expand Australia's reach beyond the range of our own collection resources (which remain largely focused on Southeast Asia and have limited capability thereafter). However, while Australia is able to submit collection tasking requests to the US, these requests must compete for priority with requests from other US allies as well as from the US military itself.

Each service also has intelligence collection assets and specialised personnel who operate them. Their activities include SIGINT and Human Intelligence (where language and cultural factors allow it).

The single largest intelligence capability gap in the ADF is limited connectivity between the various intelligence collectors, assessment agencies, headquarters and end users of information. The preponderance of 'stovepiped' single-environment approaches, each pursuing different technical solutions, was responsible for Project DEF224 being born, the end state of which is intended to be a seamless connectivity of ADF SIGINT efforts.

The situation is somewhat better for near real-time intelligence. Satellite broadcast systems are able to provide all ships, aircraft and land forces in their footprint with the latest tactical picture of nearby movements. In practice the feed, while useful, is limited by its incompleteness—not all sources of data are provided—and by the lack of a coherent approach to broadcast systems by allies. Again, single service systems with less than perfect interoperability have been the order of the day. From Australia's point of view, it is a matter of waiting until the US decides on a single unified system and standardising on that.

Surveillance

Surveillance capabilities provide the tripwire for the rest of the ADF (or other authorities) by identifying activity that requires a response—which can range from investigation to engagement with weapon systems. They constantly observe Australia's neighbourhood, particularly the air–sea gap and Southeast Asia for threats to Australia's interest.

The JORN is an active over-the-horizon Doppler radar system that operates from three stations around Australia by bouncing radar waves off of the ionosphere and looking for return signals from moving objects. It is a tripwire surveillance system that allows operational and tactical surveillance assets to be cued. Because it relies on atmospheric physics, the JORN system suffers degraded performance at dawn and dusk as these times are periods of great dynamism in the ionosphere around the earth. Similarly, periods of unusual solar activity can affect the performance of JORN.

Several systems have tried and failed to provide a surveillance capability for small boats. A similar system to the JORN using short-range (hundreds of kilometres) surface waves rather than atmospheric propagation was trialled by the Defence Science and Technology Organisation but was found to be unsuitable. Experiments with ocean bed acoustic arrays have been conducted at various times, but no operational system is in place—and the acoustic properties of northern waters often make efficient sonar detection problematic.

A number of Global Hawk unmanned aerial vehicles will come online early next decade, which will provide extended surveillance capability (missions in excess of twenty-four hours) but they will be limited in the continuous broad area surveillance role by the size of the fleet.

Finally, Australia has a cooperative intelligence relationship with the United States through the Pine Gap Agreement. The Joint Facility at Alice Springs provides Australia with forewarning of large missile launches in Southeast Asia and Oceania and access to high-resolution US satellite imagery as part of an intelligence sharing arrangement.

Reconnaissance

Reconnaissance is often a follow-on activity to surveillance. Reconnaissance assets can be directed towards unknown or suspicious contacts, where they can investigate further.

The Defence Imagery and Geospatial Organisation (DIGO) provides satellite image data to Australian military and government customers. There can be delays of hours or days between requests being made and imagery being provided.

For fast-developing situations, responsive assets such as aircraft can sometimes provide a faster turnaround. Australia depends largely on four aging RF-111 aircraft for this role. These are slated for retirement in 2010 and there is nothing to replace them. Future development paths for the Infra-Red targeting pods of the Hornets and Super Hornets (and possibly JSF beyond that) may provide a fast response IMINT capability, but that will depend on the establishment of suitable datalinks. The Global Hawk fleet will provide some reconnaissance capability as well.

For maritime reconnaissance, Defence flies an aging fleet of nineteen AP-3C Orions. They are capable in the wide area surveillance role, but they are most effectively employed as cued assets. Their relatively slow speed and their distant bases (in Adelaide) also mean that they are often not available to quickly respond to threats in the air–sea gap. Their limited number and lack of in-flight refuelling capability means that only a handful could be maintained in Australia's northern approaches at any given time.

When the six Wedgetail AEW&C aircraft enter operational service they will greatly add to Australia's C4ISR capabilities. The electronically-steered radar will be able to simultaneously track ships and aircraft and Wedgetail will also provide a communication hub and control function. Only six are being acquired, so there will be capacity constraints on continuous operations in geographically separate areas, although air-to-air refuelling will extend individual mission times. Six aircraft should be able to provide continuous surveillance of two areas simultaneously over several days. Wedgetail will make a significant contribution to maritime and aerial surveillance, but will not provide a ground tactical picture like that of the US JSTARS aircraft and will not contribute to a common tactical ground picture (a map showing the location of units to all friendly forces).

The Army has used the rapid acquisition process to acquire Tactical UAVs such as ScanEagle and Skylark which have been used down to the company level to provide near real-time reconnaissance to field units.

Electronic warfare

Electronic warfare is often linked in with C4ISR, with the covering term sometimes extended to C4ISREW, but it seems to have been largely omitted from holistic C4ISR planning in Australia—the publicly-released ISR roadmap does not mention EW and the NCW roadmap only mentions it in passing as being covered by Project *Bunyip* (see below). The next White Paper could usefully pull these threads together.

Electronic warfare breaks down into three principal categories:

- Electronic Support (ES) is really part of the surveillance category above. It is the passive gathering of information about enemy electronic signals (ELINT). For instance, Australia maintains a basic Direction-Finding capability (that is triangulating the position of an enemy based on his radio transmission) on the *Armidale* patrol boats and in the CLEWS system for the Army. Some of these capabilities have already been listed above in the surveillance section.

- Electronic Protection (EP) systems are designed to deceive or render ineffective enemy attacks on important Australian ships and aircraft. Australia has a relatively large array of these capabilities including chaff (radar deception) flares and Directed Infrared Counter Measure (infra-red deception).

- Electronic Attack (EA) includes:
  - Disruption: destroying sensitive electronic equipment by overloading it with energy (such as missile seekers)
  - Jamming: flooding adversary systems with so much energy that they cannot function as designed, disrupting sensors or communication systems by swamping the intended signals
  - Spoofing: providing adversary sensors or systems with false data
  - Networks attack: ‘hacking in’ and overloading or disrupting them.

Australia does not have an extensive EA capability. Future plans such as Project DEF 224 *Bunyip* (ADF Sigint and electronic warfare) will provide some improved jamming capabilities for the Army, but little for the other services. While recent conflicts against insurgents in Iraq and Afghanistan have involved adversaries that make use of civilian communications networks, and hence are not attractive targets for attack, electronic and network attack still has an important role in force-on-force conflict.

The only current EA capabilities are with the Army, which has a basic jamming capability. The RAN has explored a basic EA capability with Project *Cuttlefish* which targets seaborne radar, but currently has no fielded capability.

With the delivery of the Super Hornet and Wedgetail aircraft in the years to come, the RAAF will be able to utilise the capabilities of their electronically steered radars to conduct electronic attack, including disruption, jamming and false target generation. There is a dedicated electronic warfare variant of the Super Hornet—the EA-18G Growler, which has electronic attack capabilities well above the strike/fighter variant and which has been mentioned as under consideration of the now-underway air combat review. However, it is not in the Defence Capability Plan and is not a straightforward addition to the force as it would bring with it many new systems that require specialised support.

There is no public visibility of network attack initiatives, although these may well be under way. As potential adversaries become more reliant on computers their vulnerabilities increase and the ADF should be prepared to exploit these.

C4ISR Glossary

Command The authority that a commander in the Armed Forces lawfully exercises over subordinates by virtue of rank or assignment. Command includes the authority and responsibility for effectively using available resources and for planning the employment of, organising, directing, coordinating, and controlling military forces for the accomplishment of assigned missions.

Command and control (C²) The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission.

Computing and communications Two enabling technologies that support C^2 and intelligence, surveillance, and reconnaissance. Computers and communications process and transport information. Computers also enable cyber warfare activities.

Control Authority that may be less than full command exercised by a commander over part of the activities of subordinate or other organisations.

Information superiority The relative advantage of one opponent over another in commanding and controlling his force. Information superiority or dominance is achieved both through the training of leaders to make rapid and appropriate decisions using superior technical information means provided to them, and through efforts to degrade and deny these same capabilities to an opponent while protecting one's own capability.

Intelligence (I) The product resulting from the collection, processing, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding.

Network Centric Warfare The aim of Network Centric Warfare is to improve the ability of the ADF to collaborate internally, with supporting agencies, and with coalition partners across organisational and geographic boundaries. Network Centric Warfare will allow Defence to harness recent developments in computing and communications technologies to enhance decision making and warfighting capability.

Reconnaissance A mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or potential enemy, or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area. Reconnaissance is often instigated as a result of observations made during surveillance.

Situational awareness The knowledge of where you are, where other friendly and neutral elements are located, and the status, state, and location of the enemy.

Surveillance The systematic observation of aerospace, surface or subsurface areas, places, persons, or things, by visual, aural, electronic, photographic, or other means.

SOURCES: Based on definitions contained within the US Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms:* http://www.dtic.mil/doctrine/jel/doddict/ and the Department of Defence (Australia) Annual report: http://www.defence.gov.au/budget/04-05/dar/07_96_glossary.htm

ANNEX – SELECTED CURRENT DEFENCE C4ISR PROJECTS

The following project summaries are taken from Defence public documents. While many projects have C4ISR facets, these ones are the primary means by which the ISR and NCW roadmaps will be advanced.

LAND 17

LAND 17 is intended to enhance the Australian Army's artillery pieces when they reach the end of their service life. But as explained in this paper, the Army's offensive support system needs the ability to apply precise lethal and non-lethal effects from mortars, howitzers, ships and aircraft over large areas on the battlefield.

LAND 17 therefore also includes an Advanced Field Artillery Tactical Data System (AFATDS) as a Command and Control component of the Battle Management System. It is intended that the modernised system will complement current and future ADF surveillance, target acquisition, digitisation and land logistic capabilities.

LAND 75 and LAND 125 Army Battle Management System

LAND 75 and LAND 125 will provide the Australian Army with a Battlefield Command Support System (BCSS) and Battle Management System (BMS). These systems will allow the transfer, processing and management of tactical level information necessary for the command and control of land operations. A BMS is a tactical command and control system that is used by commanders in the land tactical theatre of operations to increase battlespace awareness, automate combat messaging and assist in the execution of operations. It will be capable of exchanging messages with the Army's higher level planning, monitoring and control support system and the Battlefield Command Support System.

LAND 75 will provide a vehicle-mounted capability, while LAND 125 will provide dismounted (foot) elements with BMS capabilities including a low range, intra-section communications device and a data capable Combat Net Radio—a digital situational awareness and data management system to provide commanders with improved command and control functionality.

LAND 146

Land 146 is a multi-phased project that is intended to acquire and introduce a Combat Identification (CID) capability that enhances the operational effectiveness of ADF Land Force elements, while minimising the risk of fratricide.

CID is the process of determining an accurate understanding of objects and persons detected in the battlespace to allow the timely application of tactical options and weapons effects. The key role of the CID system is to positively identify the location and status of friendly forces to both other ADF and to coalition forces. This will allow the precise and discriminative application of firepower in the battlespace and therefore minimise fratricide. The situational awareness expected to be provided by this capability will form a significant building block of the Network Centric Warfare concept.

The project will proceed in phases, with Phase 1 delivering an interim capability for a Deployable Battle Group and later phases building on that to provide the rest of the land force with coalition-compatible systems. Current plans will not extend down to the single-soldier level.

JP 2072 Battlespace Communications System (Land)

The goal of Joint Project 2072 is to provide the Land Force with deployable and integrated Battlespace Communications, with connectivity across all component systems such as C2, intelligence, offensive fire, logistics, ground based air defence and sensor-linked weapon systems. The project involves the upgrade of existing equipment and the acquisition and integration of new communications equipment.

JP 2072 is an especially significant project in that it will be developing the foundation architecture for the ADF's overarching Network Centric Warfare (NCW) capability. BCS-L was the first major project on the NCW Roadmap, which set out Defence's goals for NCW through a series of targets. By 2010 the Roadmap envisages the ADF having established an information distribution architecture with which all capital projects (including selected legacy systems) would need to comply.

Procurement was originally scheduled to occur in 2007 for delivery and installation throughout 2008. But the project has run into significant delivery problems, and the original contract was terminated. The project will continue, but other projects may be required to provide urgent items to the ADF.

JP 2030 ADF Joint Command Support Environment

The Joint Command Support Environment is evolving through the development and integration of several new and existing command support systems, including the Joint Command Support System, Maritime Command Support System, Air Command Support System, Special Operations Command Support System, and the Battlefield Command Support System (part of Project LAND 75).

The first six phases are complete and have delivered a 'core' command support system to support the planning and conduct of joint operations. This system was delivered to strategic, operational and tactical level headquarters as well as selected ADF units. Current work will include further rollout and enhancement of the Joint and Air Command Support Systems.

Later phases are intended to build upon the capability delivered under previous phases of JP 2030, and in particular to extend functionality through the development of applications that support the planning and conduct of ADF networked operations. The aim is for a single integrated environment linking all elements of the ADF.

JP 2089 Tactical Information Exchange Domain (Data Links)

Tactical data links are key information exchange systems within networked defence forces. Under JP 2089, the ADF is introducing a coherent Tactical Digital Information Link (TADIL) architecture and is systematically introducing data links to selected platforms. Phase 1 is a Project Definition Study to evaluate the requirements of the ADF's current and future platforms out to 2015 and quantify the requirements to ensure all platforms can seamlessly exchange tactical information across the battlespace.

JP 2089 is intended to deliver tactical data links to existing platforms and capabilities of the ADF and the infrastructure required to support tactical data exchange at the force level. The initial focus will be on providing tactical digital information links comprising Link 16 and Variable Message Format (VMF).

The project will implement Tactical Information Exchange (TIE) solutions on the following platforms: Link 16 and VMF in the ANZAC-class guided missile frigates, and VMF on the F/A-18 Hornet aircraft. Phase 2 will also include further definition studies related to other ADF platforms, such as ground-based elements, the Tiger Armed Reconnaissance Helicopter and tactical air transport.

SEA 1442 Maritime Communication & Information Management Architecture Modernisation

This project started life as a simple radio replacement project, but has evolved to provide local and wide area networks at sea, and to include the entire Maritime Tactical Communications System. SEA 1442 will form the basis of the Networked Fleet, which is a major milestone in the ADF's Network Centric Warfare Roadmap.

Currently unapproved Phase 4 is intended to provide for the enhancement of the Maritime Tactical Wide Area Network (MTWAN) including expansion of MTWAN into Fleet units not covered under earlier phases, integration of capabilities being delivered to maritime platforms by other approved communications projects, and consider the replacement of radios, antennas and other systems to enhance maritime communications.

AIR 5333 (Vigilaire)

Project Vigilaire will replace obsolete processors, displays and communications equipment and will also fuse the RAAF's Command and Reporting Units (CRUs) into an extended command and control network. It will receive, process and share sensor data in real, or near-real, time from JORN, Wedgetail, civil and military air traffic control radars and the Navy's future Hobart-class Air Warfare Destroyers. The upgraded CRUs will fuse this sensor data with intelligence from other sources to help compile the ADF's Recognised Air Picture (RAP) across Australia's area of interest from the mid-Indian Ocean to the western Pacific.

The Vigilaire system will also interface with new sensors, TADILs and other defence and government agencies as they come on line including agencies using legacy data and communications formats and protocols.

About the Authors

Douglas Abdiel is a communications specialist with the United States Marine Corps and is currently studying at the Australian National University. The views expressed are those of the authors and do not represent the official policy or position of the USMC, the Department of Defense or the Government of the United States.

Andrew Davies is the Program Director for the Operations and Capability Program at ASPI.

Acknowledgements

The authors would like to thank their ASPI colleague Justin Tim and defence writer Tom Muir for their help in critically reviewing this document and for providing much useful information. They would also like to acknowledge the assistance of ADF personnel who reviewed various drafts and helped shape the final version of the paper. The authors remain solely responsible for the content and for the views expressed.

About Policy Analysis

Generally written by ASPI experts, **POLICY ANALYSIS** is provided online to give readers timely, insightful opinion pieces on current strategic issues, with clear policy recommendations when appropriate. They reflect the personal views of the author and do not in any way express or reflect the views of the Australian Government or represent the formal position of ASPI on any particular issue.

ASPI
Tel + 61 2 6270 5100
Fax + 61 2 6273 9566
Email enquiries@aspi.org.au
Web www.aspi.org.au