POLICY ANALYSIS ASPI

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

The networked ADF—C⁴ISR capability summary 2010

by Andrew Davies

68

21 September 2010

This paper provides an overview of the capability of the ADF's Command, Control, Computing, Communications, Intelligence, Surveillance, Reconnaissance (collectively termed C⁴ISR) capabilities and how these systems come together to produce a networked force under the rubric of Network Centric Warfare (NCW).[1] This is an update of a 2008 ASPI paper. Previous papers in the 2010 update series reported on Navy, Army and Air Force capabilities.

This update at a glance—ADF C⁴ISR and networking since 2008

Capability

In 2008, ASPI reported that thinking within Defence on network centric force structures appeared to an external observer to be disjointed. That is no longer the case. The Australian Defence Force (ADF) now has a coherent vision and has made steady progress towards its goal of a networked force over the previous two years, due in no small part to more robust tri-service 'joint' structures. However, progress has been slower than anticipated, as can be seen by comparing public planning figures from 2007 and 2009 (see p. 6).

Table 1: Significant C⁴ISR and capability changes since 2008

Capability	Change	Comments
Satellite communications	↑	Increase in capacity as well as providing an increased range of data types (voice, images, video etc).
Long range communications (non-satellite)	↑	The long-delayed HF-Modernisation project has delivered an operational system.
Tactical ISR	↑	Provided via leased *Heron* unmanned aerial vehicles in support of ADF operations in Afghanistan.
Data transfer	↑	Defence is making progress towards standardising protocols and data formats across its systems and implementing common architectures. Examples include the successful implementation of an Internet Protocol (IP)-based network on naval vessels and the delivery of IP via satellite communications.

Nonetheless, the indicators are good. Some formerly troubled projects dating back over a decade are nearing completion. And the ADF's communications systems architectures more closely resemble the commercial world than hitherto—an absolutely vital evolution if the ADF is to avail itself of the rapidly changing world of information and communication technologies (ICT). But many proprietary legacy systems remain in service. These can be tricky to integrate with new systems as they come along. Making these systems work with newer ones is challenging, especially when block replacement is not possible.

The Defence White Paper

Table 2 lists the significant C⁴ISR capabilities announced in the 2009 Defence White Paper. Note that this table repeats some platform initiatives that have appeared in service-centric papers in this series but have significant C⁴ISR capabilities—such as the F-35 Joint Strike Fighter (JSF) and high-altitude unmanned aerial vehicles (UAVs), both of which appear in the RAAF paper. This repetition accurately reflects the 'embedded' nature of many C⁴ISR capabilities. Networking is not merely 'bolted on' to the ADF—it needs to be developed as an intrinsic part of the force structure and careful coordination across a large number of acquisition projects is required to get the best result. (The *Wedgetail* airborne early warning and control aircraft is another good example.)

Table 2: Selected major C⁴ISR initiatives in the 2009 Defence White Paper

Initiative	Nature	Comment
F-35 *Lightning II* (JSF)	Air combat/ C⁴ISR	While nominally an air combat platform, the F-35's very powerful suite of onboard sensors, and the ability to extensively share data with other network users makes it a potent ISR platform and its radar provides a significant EW capability.
(Manned) maritime patrol aircraft	Surveillance/ reconnaissance	To replace the AP-3C *Orion* fleet, for delivery around 2018.
Long endurance unmanned aerial vehicles	Surveillance/ reconnaissance	'Beyond 2020'.
Enhanced situational awareness	ISR	Rationalisation of networks into a Defence-wide architecture; standardisation of data formats and communication protocols; improved ability to exchange data with the United States.
Upgrade to Jindalee Over the Horizon Radar network (JORN)	Surveillance	Improved signals processing capability will presumably allow for detection and tracking of smaller/slower targets of interest.
Enhanced intelligence capability	Intelligence	'A number of mostly classified projects'.
Surveillance satellite	Surveillance	Probably using synthetic aperture radar technology. Collected data will be made available to the United States (and likely other friendly nations).
Cyber operations centre	Computers	Whole-of-government initiative, headquartered in Defence.
C3 and battlespace management	Command support system	High-speed communications and networking.

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 (ADF) 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 that can be used by local commanders. 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, one way to think about C4ISR is that it is to the ADF what the nervous system, eyes and ears are to the human body.

Seen this way, C4ISR is a 'force multiplier'—something that acts to make the collective effectiveness of the ADF greater than the sum of its parts. The trick is to achieve that without incurring the downside of a self-inflicted vulnerability in the form of platforms and units that lose effectiveness when networks go down (or are taken down by an adversary) or through information overload. 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. And, in the worst case, military force elements must be able to function autonomously if required.

NCW requires a number of underlying technologies, including the communications architecture, sensors and processing and data dissemination systems. And, of course, the users of those systems require 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.

To the non-specialist reader, NCW/C4ISR is a somewhat arcane topic. Because of that, this paper is different to the other three in the series. It begins with an essay that summarises for lay readers the challenges faced by Defence forces in making the best use of developments in ICT. It is followed by an overview of where the ADF is today and concludes with a review of related projects.

Every effort has been made to make the subject digestible, but a certain amount of jargon is unavoidable. Definitions of relevant terms and some other related concepts are included in a glossary at the end of this paper.

Harder than it looks—the challenges of military C4ISR

As will be seen in the sections to follow, the ADF is making progress towards its NCW vision. But progress is uneven. While there is an increasingly clear joint vision for the implementation of NCW, the development of many of the enabling steps (such as a communications architecture) is complicated by a number of factors that are difficult to manage. (And it is not a matter that can be managed entirely internally to the ADF—Australian forces may be called upon, either as a leader or member of a coalition, to operate alongside allied or other forces, all of whom will bring their own networks to the operation.)

At the hardware end, Australian platforms and equipment are sourced from different suppliers and frequently come with proprietary 'military off-the-shelf' (MOTS) C4ISR

systems. While there is increased standardisation of interfaces and data formats, making networking easier, it means that Australia's ability to tailor solutions to the ADF's architectures—which necessarily include the numerous legacy systems that remain in service—is constrained. As well, there are some subtle problems that can be imported, an example being the radio frequencies at which the systems operate. Australia's frequency spectrum allocation is not the same as supplier countries, and systems that comply with spectrum management requirements overseas may not do so here.

One solution might be for the military to make more extensive use of commercial off-the-shelf technologies. But that is sometimes easier said than done—at least where the wholesale use of civilian hardware and software is concerned. For example, the commercial world can rely on network infrastructure being in place for civilian use, an assumption the military cannot make in operational areas. (Indeed, in some deployments the existing civilian infrastructure could either be assumed to be compromised or may actually have been destroyed or degraded by earlier military action.) An iPhone is not useful in the absence of a carrier for it to connect to. So militaries must have systems in place that are independent of civilian infrastructure and are 'hardened' against attack.

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. (The ADF is making good progress here—see next section.)

The technological 'savvy' of incoming recruits is simultaneously an opportunity and a challenge. Young recruits are increasingly accustomed to using commercial networking technologies exemplified by multimedia-enabled handsets (such as the iPhone) and the internet. Military technologies seem, by comparison, to be lagging well behind the curve. To many of the recruits, who by enlistment age are likely to have operated in a world where new 'apps' are delivered daily and new hardware every other year, military C4ISR may look decidedly unexciting. But the newer generation of recruits will also bring positives with them—coming from a networked world, they are bound to bring new ideas and perspectives, and to be more willing to discover new ways of sharing and exploiting data.

The military acquisition system also needs to gain some agility to be able to exploit the possibilities provided by developments in ICT. The two-pass Kinnaird system is rigorous but slow—suited for the relatively slow pace of development of major defence platforms, but much less appropriate for systems where generation times are a year or two. For example, the *Collins* submarines were two decades in development—which means that they were conceived in the world of 1 MHz Commodore 64 processors and finally delivered (with working combat systems) as 3.5 GHz Pentium D based PCs entered the commercial market.[2]

One problem is the reliance on specifications when letting contracts. If it takes years between contract signature and delivery for a C4ISR system, there will almost certainly be developments in the intervening period that would be desirable in the final product—but in many cases neither the contractor nor the procurement agency have any great incentive to insist on its inclusion. To give one example, the author recently received a brief from a major defence supplier that highlighted some interesting and valuable work being done to exploit new approaches to data sharing between military users. However, one 'no brainer' change which would clearly result in better outcomes would not be delivered to the user in the first instance—because it was not specified in the contract.

And it must be noted that the models that work for suppliers in the 'few suppliers many customers' commercial world do not translate well into the 'few suppliers few (or one) customer' military world. Many major defence firms make a substantial part of their profits from systems integration and it is hard to see what incentive they

have to participate in a 'plug and play' approach. If a supplier can only sell a product once, it is in their interest to maximise the return on that sale. Conversely, suppliers to the commercial market can receive a small return per sale that is multiplied many times over—a low-cost 'app' that can be sold to ten million users can still be profitable.

The discussion above doesn't preclude a greater use of commercial or military off-the-shelf (COTS or MOTS) purchasing in military C4ISR, but serves to highlight some of the challenges to be managed. In fact, while there is still some way to go, military applications are increasingly being hosted on commercial standard computer and communications platforms. And while software was often written in mil-spec computer languages in the past, today it is more likely to be in languages that conform with wider industry standards. An excellent example is the shift from the software in the 1990s vintage Lockheed Martin F-22 *Raptor*, written in the once military standard Ada language, to that in today's F-35 *Lightning II* (JSF), which is written in the software industry standard C++ language, with all of the advantages that accrue from a much wider skills base and ease of development.

Similarly, many commercial software programs are finding their way into military systems—not so much as end products, but by being used as components. And the speed of uptake in this case can begin to mirror the 'outside' commercial world. For example, many C4ISR applications concern the sharing and representation of positional data. Today it is not unusual to see military data displayed on a background of *Google Earth/Maps*. Before that, the geospatial tool of choice was the commercial application *ArcView* or its relatives, which in turn replaced *Oilstock*, a US Government-developed application that was introduced in the late 1990s. Support for *Oilstock* ceased in 2002, so it had a very short life and was quickly replaced by commercial programs as they became available.

These examples suggest what the future of C4ISR will look like—it will increasingly be military applications of the hardware, software and engineering techniques that are driving the wider revolution in data transfer and communications. However, military platforms have long lives, and the cost and difficulty of integrating these products into existing military communications, sensors, combat and weapon systems means that the ADF, like other militaries, is likely to have to have a foot in the old mil-spec world for some time to come, despite adopting new systems as they become available. This observation forms the background for the discussion of ADF capability that follows.

Progress in the ADF's C4ISR and networking capability

The ADF has developed 'roadmaps' for its future ISR and NCW capabilities which set out the desired end state for the ADF's capability and the steps to be taken to get there.[3] Public versions of both roadmaps were released in 2007 and the NCW paper was updated last year.

In the 2008 paper, ASPI wrote that 'we judge that the [NCW] goal … seems very optimistic in relation to the projects that are currently in train'. This is now borne out by the ADF's own figures. Comparison of the two versions of the NCW plan reveals slippage of the planned 'in-service' dates for various steps of the networked capability. Table 3 shows the milestones in the 2007 and 2009 plans.

Between the two documents a complete review of the NCW Roadmap was conducted in conjunction with the development of the 2009 Defence White Paper in 2009. The opportunity was taken to align the revised plan with the Defence Capability Plan and to incorporate insights derived from operations. As a result of the review, some NCW milestones were amended and, in some cases, adopted a more joint approach, rather than single service capabilities and systems.

Table 3: Milestones in 2007 and 2009 NCW Roadmap documents

2007 milestones	2009 milestones*
SEA	
	• Milestone 1 – Networked Maritime Units (2009–10)
• Milestone 1 – Networked Maritime Task Group 2011	• Milestone 2 – Networked Maritime Task Group (2014–17)
• Milestone 2 – Networked Fleet 2014	• Milestone 3 – Networked Fleet (2016–19)
LAND	
• Milestone 1 – Networked Special Operations Task Unit 2008	• Milestone 1 – Networked Special Operations Task Unit (2009–10)
• Milestone 2 – Networked Battle Group 2009	• Milestone 2 – Networked Battle Group (2011–13)
• Milestone 3 – First Networked Brigade 2012	• Milestone 3 – First Networked Brigade (2013–15)
• Milestone 4 - Networked Special Operations Task Group 2012	• Incorporated into Milestone 4
• Milestone 5 – Second Networked Brigade 2014	• Milestone 4 – Networked Land Force (2015–19)
AIR	
• Milestone 1 – Networked Air Combat Force 2008	• Milestone 1 – Initial Networked Air Combat Force (2008–10)
• Milestone 2 – Networked Rapid Mobility Force 2009	• Deleted – not seen as an ongoing NCW milestone
• Milestone 3 – Networked Combat Support Force 2011	• Milestone 2 – Networked Combat Support Force (2016–18)
• Milestone 4 – Networked Aerospace C4ISR Force 2014	• Deleted – incorporated into the Networked Air Combat Force
	• Milestone 3 - Networked Air Combat Force (2017–19)
ISR DOMAIN	
• Milestone 1 – Networked Tactical ISR 2011	• Milestone 1 – Establish ISR (2009–11)
• Milestone 2 – Networked Operational ISR 2014	• Milestone 2 – Ensure ISR (2013–16)
	• Milestone 3 – Extend ISR (2016–19)
JOINT FORCE	
• Milestone 1 – Networked Deployable Joint Task Force Headquarters 2012	• Milestone 1 – Networked Deployable Joint Task Force Headquarters (2014–16)
• Milestone 2 – Networked Joint Task Force 2014	• Milestone 2 – Networked Deployable Joint Task Force (2016–18)
• Milestone 3 – Networked Australian Defence Force 2016	• Milestone 3 – Networked Deployable Joint Task Forces (3 AOs concurrently) (2016–19)
NETWORKED COALITION DOMAIN	
• Milestone 1 – Networked Coalition Combat Force 2014	• Milestone 1 – Networked Coalition Combat Force (Contributor) (2016–19)
	• Milestone 2 – Networked Regional Coalition Combat Force (ADF Lead) (2016–19)

* The first date in the 2009 figures is the date for initial operating capability while the second is full operating capability.

The slippages shown in this table are due to a number of factors: the late delivery of some key platforms (especially the *Wedgetail* in the air domain), the delayed delivery of some systems (such as the modernised high frequency communications network), operational demands and revised priorities and, last but certainly not least, the usual overly optimistic approach to the estimation of the schedule for projects.

Nonetheless, the ADF has made real progress, in no small part due to the maturing of the Joint Headquarters under the auspices of the Vice Chief of the Defence Force (VCDF). Given its tri-service nature, the natural home of networked C4ISR is within a joint setting. The bringing together of operational command and control arrangements under the Chief of Joint Operations (CJOPS) at the joint headquarters at Bungendore NSW has also forced a greater focus on joint systems.

Similarly, the management and coordination of the capabilities required belongs in a joint setting. Data is collected by and shared between the three services. So, in much the same way that the Chief of Navy is the obvious manager of the submarine capability (for example), the VCDF is best placed to manage the ADF's networked force initiatives.

Other organisational changes within Defence have helped as well. Changes in the Capability Development Group, the Chief Information Officer Group and the Defence Materiel Organisation mean that there are more robust mechanisms in place to coordinate standards and interfaces all the way from the conceptual development of networking models through to the acquisition of equipment and implementation of networks and other systems.

Some key acquisitions have delivered powerful networking capabilities 'off-the-shelf'. Chief among these—at least in the air domain—is the F/A-18F *Super Hornet*. Defence also reports that some milestones (Networked Maritime Units, Initial Networked Air Combat Force and Establish ISR) plan to achieve initial operating capability (IOC) in 2010. These milestones will achieve final operating capability (FOC) in 2011.

Collectively, these changes (and experience gained in NCW) should see more progress made in years to come—but it shouldn't be too surprising if there is further slippage in the dates in Table 3.

Capability shortfalls and issues

Command and Control

Australia (like most nations) has shortfalls in its current C4ISR capability. These are most significant at the tactical level, where data delivery is sometimes limited and timeframes for decisions are often short. However, the situation is improving and the ADF's command and control systems—identified as especially problematic in the 2008 version of this paper—are in the process of being upgraded.

The networking of Navy and Air Force is in some ways more straightforward than Army. Navy has a limited number of communications nodes, and intra-ship communications are robust. Many of the RAAF combat air platforms were 'born' connected as they were acquired from the United States Navy or Air Force and thus are fitted with established systems. 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 to operational command levels is quite good, 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. However, a significant program of modernisation is underway which will

deliver a new battle management system and new radios and will see voice and data services delivered via encrypted services through a range of communication modes.[4] (See Projects section later.)

Communications

The communication architecture of the ADF is being overhauled to make it more suitable for joint NCW. Inter-service voice communications are generally available but the ability to share tactical data between the services and to establish common operating pictures of the land, sea and air environments remains patchy (but is improving). Voice communications are often adequate for conveying executive orders and critical information, but not for providing full situational awareness information or for exploiting the potential of multimedia data.

Bandwidth was identified as an issue in the 2008 ASPI summary, but the situation has improved significantly. New capabilities will provide opportunities for more extensive exchange and exploitation of data between ADF elements. For example, Australian users now have access to the US-built Wideband Global Satellite system. This 'off-the-shelf' purchase provides a good capability for the ADF and greatly facilitates connectivity with US forces. This capability is increasing with further satellite launches planned, including an additional satellite (funded by Australia).

In terms of tactical systems, the Air Force has some restrictions on connectivity with Army. This has 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 situation will improve further as higher bandwidth data communications become available in the next few years. The Navy is well connected with the Army at the Operational level and has fitted the HMAS *Manoora* and HMAS *Kanimbla* amphibious ships as 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. The Air Force and Navy have good communication with each other because many of their platforms were acquired from the US Navy or have United States Navy (USN) systems.

Surveillance

Airborne surveillance will improve markedly over the next decade as the *Wedgetail* airborne early warning and control (AEW&C) joins the RAAF's fleet. Australia's AP-3C *Orion* maritime patrol aircraft will continue to be the mainstay of airborne maritime surveillance until replacement aircraft are acquired after 2016 but, as identified in the RAAF paper in this series, decisions on the timing of the maritime patrol fleet mean that surveillance capability will decline later this decade.

Reconnaissance

At the tactical level, Army are operating a range of unmanned aerial vehicles for battlefield reconnaissance and more will enter service in the years to come. (See the Army paper in this series.) At the strategic level, the ability of the ADF to perform reconnaissance is limited. The RF-111 aircraft—in the process of being retired—are the ADF's only airborne Imagery Intelligence (IMINT) platforms. In the future the F-35 (from 2016) and unmanned surveillance aircraft (beyond 2020) will provide a replacement capability.

Projects

The following is a summary of the current status of important projects for the development of NCW. Virtually every ADF project has network (or at least C4ISR)

aspects, but these ones are the primary means by which the ISR and NCW roadmaps will be advanced.

New Artillery (LAND 17)

LAND 17 is intended to enhance the Australian Army's artillery pieces when they reach the end of their service life. But the Army needs to coordinate the fire from its own mortars and artillery and also 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.

Army Battle Management System (LAND 75 and LAND 125); Battlespace Communications System-Land (JP 2072)

LAND 75 Ph 3.4 and LAND 125 Ph 3A, approved in November 2009, will provide the Australian Army with a Battle Management System (BMS). The systems to be delivered 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. Earlier phases of LAND 75 provided the Australian Army with a Battlefield Command Support System (BCSS). LAND 75 Ph 3.4 includes funding for interfacing the BMS with the BCSS.

LAND 75 will provide a vehicle-mounted capability, while LAND 125 will provide dismounted (foot) elements with BMS capabilities. Joint Project 2072 will provide the deployable communications backbone over which the BMS data will be transmitted. The combination of the BMS and the supporting communications system is referred to as the Battle Group and below, Command, Control and Communications system (BGC3). A contract was let for the BGC3 in March 2010.

The Army has trialled the BMS-C2 in command post exercises and will field the system in Operation *Talisman Sabre 2011*. Preliminary results suggest that the ability to pass data will have an appreciable effect (perhaps 80% reduction) in the demand for voice communications. A networked battle group is scheduled for delivery in 2012.

Combat Identification (LAND 146)

This is a multi-phased project that is intended to acquire and introduce a technically simple Combat Identification (CID) capability that enhances the operational effectiveness of the ADF Land Force elements and minimises the risk of fratricide ('friendly fire') incidents.

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 allow the precise and discriminative application of firepower in the battlespace and, therefore, minimise fratricide.

Satellite Communications (JP 2008)

This project is delivering strategic and tactical satellite communications capability. A major decision a couple of years ago saw Australia sign on to the US-developed

Wideband Global Satellite system. This has resulted in a significant and rapid improvement in the bandwidth and global reach available to the ADF. An Australian funded satellite will be added to the constellation in 2013. (Was 'early 2012'.) The ADF gains progressively greater bandwidth as each satellite in the constellation is launched. Three satellites are currently operational.

JP 2008 is also delivering narrowband UHF communications that will be used by ADF elements, including aircraft and ships as an 'over the horizon' communications capability.

ADF Joint Command Support Environment (JP 2030)

The Joint Command Support Environment is evolving through the development and integration of several new and existing command support systems in the joint, maritime, air and special operations land environments.

The first seven 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. Future work will include further rollout and enhancement of the Joint and Air Command Support Systems. The aim is for a single integrated environment linking all elements of the ADF.

JP 2072 Battlespace Communications System (Land)

JP 2072 is a multi-phased project designed to provide a deployable, digital, land-based tactical communications system, known as the Battlespace Communications System (Land), or BCS(L). The BCS(L) will connect deployed operational and tactical headquarters to allocated tactical units from the Australian Army, Navy and Air Force via a mobile, secure and survivable network. The network will extend to all users within and between areas of operations, to Joint or Allied/Coalition elements and provide an interface to the Australian Defence strategic network.

Tactical Information Exchange Domain (Data Links) JP 2089

Tactical Information Exchange (TIE) systems, including Tactical Data Links (TDL), are a key enabler to ensuring that tactical information is created, processed and shared among war fighters in real, near real, and non-real-time. Under JP 2089, the ADF is introducing a coherent and coordinated TIE environment and is systematically introducing TIE capability to selected legacy platforms.

Previous phases of JP 2089 include:

- Phase 1 (in closure) was a study to quantify TIE requirements to ensure all current and future ADF platforms will be able to seamlessly exchange tactical information across the battlespace.
- Phase 2A (in progress) will provide Variable Message Format (VMF) and Link-16 datalink integration with the combat management system on the *Anzac* Class frigates, and will provide the initial Common Support Infrastructure (CSI) to support tactical information exchange.
- Phase 2B (in progress) will implement a VMF digital communication system on F/A-18A/B Hornet aircraft to provide greater interoperability with land forces during Close Air Support (CAS) Missions.
- Phase 3A is intended to further develop the initial CSI procured and delivered under Phase 2A. It is anticipated to be an operational multiple tactical data link network management environment for the ADF.
- Phase 3B intends to develop a VMF Tactical Information Exchange (TIE) solution for the TIGER Armed Reconnaissance Helicopter (ARH).

Maritime Communication & Information Management Architecture Modernisation (SEA 1442)

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. (See Table 3.) Since the previous paper, some elements of this project have been subsumed into other projects. For example, project JP 2008 (see above) will provide satellite communications and other infrastructure.

Recognised Air Picture (AIR 5333 'Vigilare')

Project *Vigilare* 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 DDGs. The upgraded CRUs will fuse this sensor data with intelligence from other sources to help compile the ADF's Recognised Air Picture across Australia's area of interest from the mid-Indian Ocean to the western Pacific.

The *Vigilare* 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.

The future

The networked ADF still has some way to go, but the essential elements are being put into place and there are signs that the benefits of high-bandwidth communications and constantly improving processor capabilities will in turn deliver improved military capabilities.

As well as improvements in the enabling C4 systems, the delivery of some important new platforms will provide a big boost in networking capability—in terms of both data collection and dissemination and their ability to act as network hubs. This includes the *Wedgetail* and F-35 (JSF) in the air domain and the Navy's new DDGs ('air warfare destroyers').

But the most important change is probably further consolidation of the integrated joint command and control environment—a process that has already significantly shaped the way the ADF approaches its business. That is the level at which ISR data can best be brought together into a common operating picture and disseminated to the end user in a form that enhances operational capability.

Endnotes

1 The purist might object that we have mixed two different topics in NCW and C4ISR, but they are intrinsically related. Much of the data that is shared in NCW is positional data obtained as part of ISR operations. Electronic Warfare (EW) was included in the corresponding 2008 paper, but is excluded this time around because it is a complex subject that really requires a separate discussion to do justice to it.

2. Or, to put it another way, the *Collins* project was instigated when *Donkey Kong* played on an outsize arcade box was still in vogue and delivered when 3-D online gaming via the *X-Box* and *PlayStation 3* was available to homes.

3 The most recent NCW and ISR Roadmap publications are available at http://www.defence.gov.au/capability/_pubs/NCWRoadmap2009.pdf and http://www.defence.gov.au/publications/ISR_Roadmap_2007_2017.pdf respectively.

4 For a summary of Army's plans see *Networking Army*, Vanguard Issue 10, Australian Army, August 2010. (Not on web at time of writing.)

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 (C^2)—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

About the Author

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

Note: The 2008 ASPI paper updated by this paper was co-authored by Andrew Davies and Douglas Abdiel.

Acknowledgements

The author would like to acknowledge the assistance of the Department of Defence in providing input and helping shape the final version of the paper. However, the content and the views expressed in this paper and any errors or omissions are entirely the responsibility of the author.

About Policy Analysis

Generally written by ASPI experts, the **POLICY ANALYSIS** series 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