STRATEGIC INSIGHTS
ASPI

ADF capability snapshot 2016
C4ISR—winning in the networked battlespace

107

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

Andrew Davies and Malcolm Davis

This paper provides an assessment and overview of the ADF's command, control, computing, communications, intelligence, surveillance and reconnaissance (known commonly as 'C4ISR') capabilities in the context of the ADF's goal of pursuing a network-centric warfare capability. The paper is the final part of a series of ADF 'capability snapshots'. The previous three (Navy, Army and Air Force) were released by ASPI in late 2015.

Introduction

The *2016 Defence White Paper* (DWP-16) and accompanying Integrated Investment Plan (IIP) signalled a major boost in Australian defence spending, with a commensurately ambitious force structure plan. An important part of the plan is a greater investment in intelligence, surveillance, reconnaissance (ISR), electronic warfare (EW), space and cyber capabilities.[1] The development of ADF 'C4ISR[2]'—'command, control, communications, computers, intelligence, surveillance and reconnaissance'—and an emphasis on building network-centric warfare (NCW) capability lie at the heart of ADF capability development.

Jindalee Operational Radar Network © 2016 BAE Systems.

Although C4ISR and NCW have a much lower public profile than the ships, aircraft and fighting vehicles that make up the 'sharp end' of defence capability, the ability to collect, process, analyse and disseminate information is a critical warfighting capability. Having surveyed the individual capabilities of the three services in previous papers in this series, it's fitting to consider the capabilities that are intended to tie the ADF together into a coherent fighting force and allow Australian forces to operate with allies and partners when required.

To the non-specialist reader, the NCW/C4ISR area is somewhat arcane. Because of that, this paper is different from the other three in the series. Reviews of the performance and status of the ADF's many and varied C4ISR systems would make for formidably dull reading and would almost certainly obscure the wood for the trees. Instead, this paper takes a higher level approach based on what the ADF can do with its systems in practice, dropping down to details only when required.

The first section of this paper, designed for the reader interested in a high-level description, describes the changes in the ADF's C4ISR capabilities since ASPI last reviewed this topic in 2010, including an assessment of the state of intra- and inter-service connectivity. The second section reviews the role of C4ISR and the closely related concept of NCW in modern warfighting, with a focus on what it means for the ADF's ability to fight alone or in coalition with other Western forces. The final section, really only for C4ISR tragics, reviews progress on some of the major projects that will contribute to the ADF's future capability. The DWP-16 and the IIP provide a convenient vantage point to review progress in C4ISR modernisation and consider risks and opportunities ahead.

1. Capability changes since 2010

The previous two papers in this series make for interesting reading in retrospect. ASPI's 2008 report was critical of the ADF's lack of cohesion in planning for its networks. By 2010, there was a plan for more robust tri-service 'joint' C4ISR capabilities and some early progress had been made—albeit less than had been planned for. Now, another six years on, we can make a more measured judgement of progress to date.

As was the case with other ADF capability domains reported on earlier in this series, some impressive C4ISR capabilities have come on line in recent years. The E-7A Wedgetail airborne early warning and control aircraft has now achieved the full operational capability benchmark. The establishment of the Vigilare system—albeit after a protracted development process—has delivered an enhanced recognised air picture across Australia. The Tactical Information Exchange Domain is establishing common data links between air, naval and land forces for the sharing of battlespace information, and the Maritime Communication and Information Management Architecture Modernisation project has evolved from new radios for RAN surface vessels to the provision of fleet-wide data networks.

Sometimes these improvements provide a quantum leap in capability, such as the recognised air picture system (previously reported in ASPI's 2015 RAAF capability review). But there's also a lot of work that steadily improves on existing capabilities, as is the case with the migration, over many years and project phases, of the Jindalee Operational Radar Network to an all-digital sensor. In some cases, progress hasn't been as hoped. The decision by Australia to sign on to the US-developed Wideband Global Satellite System under project JP-2008 in 2007 would've seen the ADF gain access to a key US satellite communications system in return for funding the sixth satellite, thus providing global access at a much lower cost compared to building and launching such a satellite system, and reducing dependence on commercial satellites for defence communications.[3] Australia's construction of ground station facilities is running five years late, but Defence advises that it's '*mitigating this delay by upgrading and extending its Interim Anchoring infrastructure in the East and West of Australia, refreshing its offshore anchoring capabilities and leveraging the USA's Remote Monitoring and Control Equipment in the East and West of Australia with an increased number of modems*'. While this is far from ideal, we understand that the bandwidth available through these workarounds is adequate.

Overall, the ADF is better networked and more digital today than it was five years ago. All three services have improved their C4ISR capabilities, and there's greater ability to share information within and between services. That's especially true of intra-service ability to share data, although the RAAF and Navy also have good levels of inter-service capability—inherited to an extent from the US Navy origin of equipment in both services. The RAAF's experience over Iraq and Syria shows that it's well able to work within

American and allied command and control structures. Similarly, the Navy is able to work in US Navy task groups, and some simple future steps would further improve interoperability.

Organisationally, one of the impediments to the coordination of C4ISR projects in the past was the lack of a champion at the Defence Committee table. The First Principles Review noted this deficiency and recommended that the Vice Chief of the Defence Force (VCDF) become the capability manager for joint capabilities. While the VCDF's responsibilities extend beyond C4ISR, this is a worthwhile step that should improve planning for ADF C4ISR.

As observed in 2010, there has been an increase in the adoption of communications and data architectures that more closely resemble those in the commercial world. That's a necessary step, because commercial ICT generation times are far shorter than traditional military acquisition systems can cope with. However there's a limit to how commercial-like military systems can be. For a start, they need to be harder to disrupt or hack. And, given that military platforms have lifetimes measured in decades, there are always 'legacy' systems that have to be integrated into new systems. (See the essay 'Harder than it looks—the challenges of military C4ISR' in the 2010 C4ISR capability report for further explanation.)

Table 1 shows our assessment of the current state of connectivity within and between the three services, and with the joint ADF command and control structure. The reasons for the ratings are explained in the capability report that follows. While there is some degree of subjectivity to the ratings, the overall assessment is that the RAAF is the most 'joined up' of the forces and is able to collect and fuse data and disseminate it to the various nodes of its network. However, there's more to be done—not least to work out how to operate fourth- and fifth-generation aircraft, with their very different data generation and processing capabilities, side by side in the 2020s. The RAAF's Project Jericho is a roadmap for further evolution and for the exploitation of the data collection and fusion capabilities that will arrive with such platforms as the F-35, G-550 Gulfstream, EA-18G Growler, P-8 Poseidon and Triton maritime patrol aircraft.

Table 1: An assessment of ADF C4ISR connectivity

	Navy	Army	Air Force	Joint
Navy	4			
Army	2	3		
Air Force	4	2	5	
Joint	4	3	4	4

(Note: shaded cells are omitted for clarity but are the same as those across the diagonal. E.g. Army-Navy = Navy-Army)

Key: 5—excellent connectivity, with minor if any shortcomings; 4—very good connectivity, with some shortcomings; 3—generally good connectivity, but with some significant shortcomings; 2—significant connectivity shortcomings; 1—poor levels of connectivity

The RAN also has a robust set of networks and advanced methods of sharing data. However, there are some important capabilities that aren't yet in place. One is the *Hawklink* functionality that allows embarked Seahawk helicopters to transmit data to surface ships in real time. While the RAN's new Romeo model Seahawks have the functionality (though it was a near thing—the Defence Materiel Organisation almost insisted on its removal), the Anzac frigates, the remaining Perry-class frigates and the air warfare destroyers (AWDs) currently under construction don't. Presumably, the requirements for the future frigates will include the *Hawklink* system, but until then the RAN's Romeos will have better tactical data communication with US Navy vessels than with their own. Another system that would greatly improve the Navy's capability to conduct air defence would be the incorporation into the AWDs of a cooperative engagement capability that would let them fire missiles at targets beyond their own radar horizon based on third-party targeting data from other vessels or from aircraft that can see over the ship's horizon.

The Australian Army has made good progress in linking up its various force elements but is probably the least advanced of the three services in being able to work seamlessly with the rest of the ADF. As noted in the earlier Army report, it has two digital battlefield networks when one would be preferable, and it has some platforms that have bespoke C4ISR systems that will be hard to keep in synch with the rest of the force. In considering the Army's digitisation process, ASPI analysis suggests that:

> … the ad hoc approach to date has resulted in multiple projects operating in parallel with little consideration of systemic standardisation or C4ISR … integration. The result has been an amalgam of systems and capabilities that were never designed to operate in concert or as part of a single fighting system. The need to de-conflict these programs after the fact has impeded the modernisation effort.[4]

The result is that Army lags the other two services and in some ways is ploughing a furrow of its own, which will make it hard to achieve genuine joint connectivity and interoperability with partners and allies, and even to upgrade its own systems in the future. To be fair, the Army is aware of this shortcoming, and Project Land 200 is intended to standardise its digital architecture (see the last section of this paper for more details). And a recent demonstration of an 'airborne gateway' system mounted on a Gulfstream aircraft successfully provided Army's Tiger helicopters with access to data feeds from other ADF platforms, such as Wedgetails and Super Hornets.[5]

All of the services have good-to-excellent connectivity with the joint level, which reflects a maturation of the jointness model the ADF set out on a decade ago and the resourcing of initiatives such as the Joint Headquarters at Bungendore, New South Wales.

2. Essay: Modern warfighting, C4ISR and network-centric warfare

The modern Western approach to warfare is to use communication and computer technology to draw together data collected by disparate sensors into a consolidated common operating picture that can be used by local commanders to make rapid decisions based on a greater appreciation of the battlespace around them. If it all works properly, the 'fog of war' can be pierced—though never completely removed—by advanced sensors that immediately transmit gathered information to a network of machines and people who can then make decisions based on that information in near real-time. 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 most vivid demonstrations of C4ISR as a force multiplier were in the 1991 Persian Gulf War and the main combat phase of the 2003 Iraq War. In both conflicts, American-led military coalitions arrayed against Iraq demonstrated the value of superior sensors and communications systems and the ability through command and control systems to understand the battlespace better than their opponent did. The devastating effectiveness of air and missile operations in Desert Storm, and the subsequent rapid offensive of air and ground forces in Desert Sabre that liberated Kuwait in 1991, showed that knowledge superiority, together with superior training and command and more advanced military capabilities, could be the basis for victory, overcoming numerical advantage or the brute application of firepower.

Operation Iraqi Freedom in 2003 took the exploitation of C4ISR and smart weapons to a new level, with the debut on a large scale of 'network-centric warfare' (NCW). This concept seeks to exploit superior knowledge through a reorganisation of military forces to better use superior sensors, secure global communication systems and data links. The ability to push information forward allows for flat rather than hierarchical command and control structures. And having common operating pictures based on shared and fused data allows joint and coalition forces—be they on land, in the air, on or under the sea—to better coordinate and synchronise military operations.

So decisive were the victories against Iraqi forces in 1991 and 2003 that it seemed that NCW as practised by the US and its partners was unchallenged as a war-fighting strategy. A lot has changed since then. At the less technical end of the spectrum, Iraqi insurgents after the 2003 surrender adopted a low-profile asymmetric strategy that minimised their exposure to advanced C4ISR systems and allowed them to engage at times and places of their choosing—a strategy that echoed the tactics of the Taliban in Afghanistan against both Soviet and later coalition forces. At the same time, technically sophisticated competitors such as Russia and China have taken steps to close the gap in technical capability and are working on systems and capabilities designed to degrade Western C4ISR systems. China is also well advanced in the development of anti-access/area-denial (A2/AD) systems designed to keep American platforms well away from areas where China wants to be able to deploy military force.[6] The combination of counter-network and A2/AD is shattering two key foundations of military power—relative invulnerability from attack, particularly at long range, and assured information superiority.

The net result of those developments is that decisive victories such as those in Iraq are increasingly unlikely against near peer competitors. In the worst case, a strategy based on networked warfare and a knowledge edge via networked C4ISR systems could be a potential Achilles heel if an adversary can attack those networks and pull apart the connectivity across operational domains, or operate in a manner that renders specific technological advantages of their opponents largely irrelevant. Future adversaries will try to disrupt the collection and transmission of this information to increase 'fogginess', behind which they'll try to achieve their own objectives while at the same time increasing their knowledge edge relative to our own. Technologies such as electronic warfare (EW), computer network attack and anti-satellite weapons could deny the flow of information at crucial times. Just as long-established EW techniques of jamming and spoofing can disrupt or deceive sensors, new approaches to 'electronic attack' against networks and ISR platforms may erode our ability to undertake NCW in the future.

The period of an assured knowledge edge for the US and its allies was grand but ephemeral. In response to new developments, the US is now embarking on a 'third offset strategy' as a means of countering A2/AD technologies and strategies to ensure that US military forces can operate in an era in which its opponents have long-range precision strike capabilities that neutralise traditional military–technological advantages that the US has held since the end of the Cold War.[7] In this framework, C4ISR architectures have to be hardened and resilient and, in the worst case, military force elements have to be able to function autonomously if C4ISR networks are degraded.

In the future, the US and its key allies, such as Australia, will have to fight to gain a knowledge edge, and then struggle to keep it in the face of much more capable opponents with a greater ability to exploit the vulnerabilities of our dependence on networked C4ISR systems. C4ISR and NCW are therefore both strengths and potential Achilles' heels for the US and its key allies, including Australia, because dependence brings vulnerability. As well, the West has become accustomed in recent decades to waging war in a high-tech manner with high precision, low levels of collateral damage, and an emphasis on information superiority and manoeuvre that leads to rapid and relatively low-cost outcomes, rather than an extended effort involving mass and attrition. We won't be able to do that without the C4ISR systems that we're now wedded to as essential foundations for our ability to use force.

An adversary's ability to remove or erode such capabilities would be devastating. It would force us back to a more brutal and bloody form of war that, short of a war of survival, would be difficult for modern societies to fight. In considering where C4ISR and NCW is going in coming years, a key emphasis should be on building resilience and the ability to rapidly reconstitute existing capabilities in the event of an attack on our critical networks and systems. Recent capability development has focused on introducing new network-centric structures and bringing non-networked forces into a digitised present. The future must be focused on preserving these capabilities in the face of determined adversary counter-responses.

3. Australia's approach to network-centric warfare and current projects

Since 2003, and especially with the release of the 2009 Defence White Paper, the concept of NCW has been at the forefront of planning for the way the ADF will fight. The key planning document is the *NCW Roadmap* (the most recent iteration of which was released in 2009).[8] Also important are a series of key policy papers, including *Force 2020* and *Future Warfighting Concept* (2002). The conceptual foundation in those documents was expanded in 2007 with the release of the Future Joint Operational Concept—*Joint Operations for the 21st Century* as well as the *NCW Roadmap*. The 2009 Defence White Paper and the 2009 revision of the *NCW Roadmap* firmly placed NCW as the essential basis for Australia's approach to the use of military force.

A new Networked Joint Force Roadmap, which has been developed and is awaiting endorsement at the time of writing, will be the overarching document to the *ISR Roadmap*. The replacement term for 'NCW' is 'Networked Joint Force'.

For now, the *NCW Roadmap* is an overarching document to the *ISR Roadmap.* The latter concerns itself with the integration of existing C4ISR capabilities and the introduction of new sensor capabilities and platforms capable of producing and handling massive amounts of ISR data.[9] Integrated ISR is therefore an essential requirement for NCW and a foundation for establishing a common operating picture shared across the joint and coalition battlespace by all units. This is the minimum essential requirement for a military force to fully exploit NCW.

The 2009 *NCW Roadmap* had a five-year outlook, so the development of the new *Networked Joint Force Roadmap* is timely. Similarly, the Defence *ISR Roadmap* reaches its endpoint next year. With the release of the DWP-16 and IIP, now is a good time to review where we've got to, and whether Defence is achieving goals and milestones in C4ISR modernisation that generate an effective NCW capability for the ADF.

Key projects: the state of play

It's useful to consider the status of a number of key C4ISR projects and how they contribute to the ADF's overall progress towards achieving its C4ISR/NCW goals, particularly in the light of the release of DWP-16 and IIP. The IIP notes that Defence will invest around 9% of funding into C4ISR, space, EW and cyber capabilities. The funding will continue existing projects from the now-defunct Defence Capability Plan (DCP) and instigate new capabilities within the IIP through to 2025–26.[10] The unclassified IIP (like the DWP-16) is disappointingly short of specific information on projects compared to the old DCP, which was also unclassified. That makes it difficult to determine which projects are enduring from the DCP era and which are new.

AIR 5077: the E-7A Wedgetail AEW&C aircraft capability and upgrades

The RAAF's E-7A Wedgetail airborne early warning and control (AEW&C) aircraft procured under AIR 5077 were declared to have achieved final operational capability in May 2015, and one is currently deployed in Operation Okra against ISIS forces in Iraq and Syria. The six Wedgetails acquired by the RAAF are an entirely new capability for the ADF and provide Australia with one of the world's most advanced air battlespace management capabilities. More than just an AEW&C aircraft for controlling air operations, the Wedgetail is a key node in the ADF's network, as it's able to gather, analyse and redistribute information originating from a wide variety of sensor platforms in the air, at sea and on land.

The 2012 DCP and the accompanying 2012 Defence Capability Guide highlighted some key projects related to AIR 5077. The 2016 IIP, though lacking in detailed information on the exact nature of improvements, explains that Wedgetail will continue to be upgraded 'in order to maintain its capability edge ahead of a major refresh or replacement in the mid-2030s. Software, hardware and communications elements will also be upgraded to enhance interoperability with other ADF and coalition assets.'[11] A key component of that upgrade is likely to be the Cooperative Engagement Capability (CEC). First flagged in the 2009 White Paper, CEC would allow the Wedgetail to provide targeting data to a broad range of ADF and other forces, among them the RAN's new Hobart-class AWDs and the future frigates. Such a capability would allow the AWD's 375-km range SM-6 naval air defence capability to be targeted well beyond the ship's own radar horizon using the Wedgetail's sensors. That's likely to be an important capability, given the proliferation into the region of advanced anti-ship cruise missiles, such as the supersonic 290-nm (537-km) range Chinese YJ-18.[12]

Vigilare and JORN upgrades

As the previous C4ISR snapshots discussed, the Vigilare air surveillance network was a long time in the making, but eventually delivered a high level of capability. Similarly, the long-in-development Jindalee Operational Radar Network (JORN) has become an important part of the nation's surveillance capability. But the IT-driven field of C4ISR doesn't stand still for long, so it's not surprising to find that the new Defence White Paper says that:

> … Government will make a substantial new investment to strengthen Defence's intelligence, surveillance and reconnaissance capabilities. This includes upgrading our current air defence network (including the Vigilare air surveillance system and the Jindalee Operational Radar Network) and introducing new, modernised all-source intelligence systems supported by enhanced information processing capabilities. (Para. 4.12)

Vigilare is designed to fuse input data from a wide range of disparate sources into a single recognised air picture that can then be shared with ADF and coalition forces. The disparate inputs include tactical data links (TDLs) such as Link 16, JORN, Wedgetail and other platforms, including Navy and Army sensor systems, and information processed from sensors such as radar, EW

and 'identification friend and foe' (IFF) systems. Future upgrades of Vigilare under project JP2089 Phase 4 will see the more sophisticated Link 22 data link architecture introduced, as well as CEC, with initial operational capability to be delivered in the middle of next decade. Link 22 is a NATO standard datalink (often referred as 'NATO Improved Link 11, or 'NILES') that connects air, surface, underwater and ground-based systems and is the key to achieving NCW. Link 22 will replace the older Link 11 standard as well as complementing and interoperating with Link 16 as currently used by Vigilare.[13] More than 120 operational units can use a 'Link 22 Super Network' for seamless communication across a wide geographical space, significantly boosting network centricity. Link 22, together with Link 16, will help update Australia's military airspace command and control and provide more effective C4 for the Army as well as maritime communications for the Navy.

Another key development will be the spiral upgrade of JORN:

> … in order to realise its full potential as a wide area surveillance capability. Enhanced command, control, communications, computers and intelligence integration will allow Jindalee to cue and be cued by other systems across the sensor network.[14]

A 2013 'health check' of the JORN capability found that peaks and troughs in the workflow threatened the ability to maintain the required industrial base for this important and nearly unique capability.[15] The DMO subsequently announced a rephrasing of the project to mitigate that potential problem:

> JP 2025 Phase 6 and Phase 7 are currently planned for JORN. Phase 6 will be a smaller-scale upgrade to keep all three radars up-to-date and is planned to reach Initial Operational Capability (IOC) between FY 2018–19 and FY 2020–21. Phase 7 is an interim investment to retain 'Priority Industry Capability' skills in the niche OTHR industry until the start of Phase 6. Work on Phase 7 will include a mixture of outcomes, including risk reduction and preparation for future upgrade phases.

Phase 6 of the JORN upgrade will improve performance by moving from analogue to digital radar receivers and transmitters, and enhanced frequency management, in a process that will see radars and operations centres updated under a rolling approach to avoid any disruption in services.[16] Moving to digital systems and ensuring that JORN is fully networked into the broader ADF C4ISR capability is a vital step, given the introduction of advanced C4ISR platforms such as the E-7 Wedgetail AEW&C aircraft and new capabilities such as the MQ-4C Triton high-altitude long-endurance unmanned aerial vehicle, the E/A-18G Growler, and up to five Gulfstream G-550 EW aircraft to be acquired as part of the updated Force 2030 plan of DWP-16.[17] Furthermore, recent improvements under JP2025 Phase 5 have allowed for greater performance and operational agility by allowing JORN to observe a specific area (or 'tile') over a larger geographical region and enabled more rapid shifting from one tile to another. The radar system can also operate for longer because it can operate at reduced power mode, although with somewhat reduced performance.

Other C4ISR projects

Under DCP 2012, there was a strong emphasis on upgrading communications for the Air Force (AIR 5397 Phase 2), the Army (Land 75) and the Navy (SEA 1442), as well as several joint projects (JP 2030 Phase 9, JP 2072, JP-2089 and JP 2065). However, with the release of the lamentably short-on-detail IIP, and as noted above, it's no longer clear what the status of these projects is; the IIP merely states that 'Defence will acquire new and enhanced command, control, communications and intelligence, surveillance and reconnaissance systems.'[18] That somewhat bland statement is expanded on later:

> … a new, more sophisticated command, control, communications, computer and intelligence system will also be required to be able to fuse information from multiple sources. This will enable coordination of forces and more timely operational response, including an ability to support the more comprehensive situation awareness required for capabilities such as integrated air and missile defence.[19]

The IIP emphasises the importance of building a common operating picture via the development of TDLs such as Link 16 and Link 22:

> Success in all operations is dependent on providing tailored and near real-time situational awareness to commanders. In the operational sphere this is provided by generating a trusted common operating picture. Defence will continue with functionality

enhancements to relevant systems in order to integrate the common operating picture at all levels and provide enhanced situational awareness across the joint force.[20]

This aspiration segues neatly into existing projects described in DCP 2012. For example, AIR 5397 Phase 2 was focused on building more effective communications links between air and ground forces, including the use of TDLs and Internet Protocol based systems, as well as radio-over-internet and voice-over-internet protocols.[21]

There's a lot of activity concerning Army C4ISR. The Land 75 project to develop battle management systems and battlefield command support systems is mostly complete and will equip two battle groups in 7 Brigade, plus 7 RAR and elements of special operations as well as RAAF Airfield Defence units, while Phase 4 will continue the acquisition and provision of enhancements to battle management systems to additional brigades, building common systems to enhance situational awareness and interoperability up to the joint and coalition levels. Phase 5 of Land 75 continues to develop the Army's ability to enhance its battle command systems. Land 75 is a crucial element of Army digitisation and ensuring that Army units can plug and play with the Air Force and Navy and with coalition partners.

For the Army, which has lagged behind the Air Force and Navy, the move towards digitisation and NCW is vital, especially as the amphibious capability is worked up. That capability will at the very least require robust command and control arrangements from ship to shore. Land 200 is at the core of Army digitisation, and tranche 1 of Land 200 achieved final operational capability in early 2015.[22] Land 200 comprises elements of Land 75 (Battlefield Communications), Land 125 (Soldier Enhancement) and Land 2072 (Battlefield Communications Systems) to create a battlefield management system that then plugs into the Joint Command Support Environment (JCSE) noted above, as well as the Tactical Information Exchange Domain under JP 2089, to ensure interoperability and compatibility with wider ADF forces and coalition allies.

Naval C4ISR modernisation is in part centred on SEA 1442 Phase 4, which seeks to upgrade communications for the RAN's Anzac-class frigates and which builds on the introduction of the Maritime Tactical Wide Area Network to major fleet units under Phase 3. This will significantly boost the communications capabilities of the vessels and allow high-speed networking of ships within a task group, as well as more effective communications between ship and shore. [23]

Finally, in the joint environment, JP-2030 Phase 8 has been approved. It builds upon previous phases to develop the JCSE and extends the ability of existing systems to conduct networked operations to Headquarters Joint Operations Command and other fixed headquarters locations.[24] Phase 9 will consolidate the existing command support systems into a single integrated environment, linking all elements of the ADF, including maritime, air, special operations and battlefield command support systems, with initial operational capability planned for around 2020–21. The JCSE is designed to allow better communications between operations staff and troops, particularly commanders and Special Forces. By integrating existing command support systems into a single, integrated environment, this will enable better support for amphibious forces, including the new Canberra-class landing helicopter docks.[25]

Notes

1 Annaliese FitzGerald, *DWP 2016: the future of C4ISR*, *The Strategist*, 4 March 2016.

2 Strictly speaking, the acronym should read C[4]ISR, but common usage is now C4ISR.

3 Andrew Davies, Australia's WGS communications—what went wrong?, *The Strategist*, 22 September 2015.

4 Michael Clifford, Michael Ryan, Zoe Hawkins, *Mission command and C3 modernisation in the Australian Army: digitisation a critical enabler*, ASPI Special Report, December 2015, p. 6.

5 See *Airborne gateway provides air–land integration for Jericho Dawn firepower demonstration*, *Australian Aviation*, 21 March 2016.

6 Timothy L Thomas, 'Chinese and American network warfare', *Joint Force Quarterly,* issue 38, July 2005, pp. 76–81.

7 Shawn Brimley, Lorden Dejonge Schulman, *Sustaining the third offset strategy in the next administration*, *War on the rocks*, 15 March 2016.

8 Department of Defence, *NCW Roadmap 2009*.

9 Department of Defence, *ISR Roadmap 2007–2017*, July 2007.

10 Department of Defence, *Integrated Investment Plan*, 2016, 1.1.

11 Department of Defence, IIP, 2016, 5.21. Based on the former DCP and the intent expressed in the DWP-16 and IIP, the Wedgetail looks likely to follow an upgrade path including Mode 5/S identification friend or foe (IFF) interrogator; cryptographic modernisation; web-enabled internet protocol; GPS selective availability anti-spoofing module; integrated broadcast system; and resolution of obsolescence issues. Initial operational capability for this project is from 2017–18 to 2019–20. Estimates Statements note that Boeing Defence Australia will 'design, prototype, test and deliver upgraded mission computing and … IFF capabilities' before a more significant mid-life upgrade between 2025–26 and 2027–28.

12 Lyle J Goldstein, *China's YJ-18 supersonic antiship cruise missile: America's nightmare*, *The National Interest*, 1 June 2015.

13 Northrop Grumman, *Understanding voice and data link networking*, December 2014.

14 Department of Defence, IIP, 2016, 1.14

15 Defence Materiel Organisation, *Priority Industry Capability Health Check—2013: High frequency and Phased Array Radars (HFPAR)*, 2013.

16 Kathrine Ziesing, 'The next evolution of JORN', *Australian Defence Magazine*, March 2016, pp. 25–26.

17 Malcolm Davis, *The Gulfstream G550 and the ADF—plugging the ISR gap*, *The Strategist*, 14 January 2016; James Mugg, *The next Battle of the Beams*, *The Strategist*, 2 March 2016.

18 Department of Defence, IIP, 2016, 1.3.

19 Department of Defence, IIP, 2016, 1.8

20 Department of Defence, IIP, 2016, 1.9.

21 Tom Muir, *Air: IP's promise for air-ground-air communications*, *Australian Defence Magazine*, 26 March 2013.

22 Nigel Pittaway, *Rolling out a digital army*, *Australian Defence Magazine*, 1 July 2015.

23 ANZAC class frigate communications upgrade, *Australian Defence Magazine*, 3 December 2013.

24 Australian Department of Defence, *Defence Capability Guide 2012*, p. 25.

25 Gregor Ferguson, *Network centric warfare: JP3030 reaches its next stage*, *Australian Defence Magazine*, 1 November 2011.

Acronyms and abbreviations

AEW&C	airborne early warning and control
C4ISR	command, control, communications, computers, intelligence, surveillance and reconnaissance
CEC	Cooperative Engagement Capability
DCP	Defence Capability Plan
DWP-16	2016 Defence White Paper
EW	electronic warfare
IFF	identification friend and foe
IIP	Integrated Investment Plan
ISR	intelligence, surveillance and reconnaissance
JORN	Jindalee Operational Radar Network

JSCE	Joint Command Support Environment
NATO	North Atlantic Treaty Organization
NCW	network-centric warfare
RAAF	Royal Australian Air Force
RAN	Royal Australian Navy
TDL	tactical data link
VCDF	Vice Chief of the Defence Force

Important disclaimer

About the authors

Andrew Davies is Director—Defence & Strategy Program and ASPI's Director of Research.

Malcolm Davis is a Senior Analyst in Defence Strategy and Capability.

The authors would like to thank the Department of Defence for commenting on a previous draft of this paper. All opinions and any errors in this paper remain the responsibility of the authors.

About Strategic Insights

Strategic Insights are shorter studies intended to provide expert perspectives on topical policy issues. They reflect the personal views of the author(s), 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

Facebook.com/ASPI.org

@ASPI_org