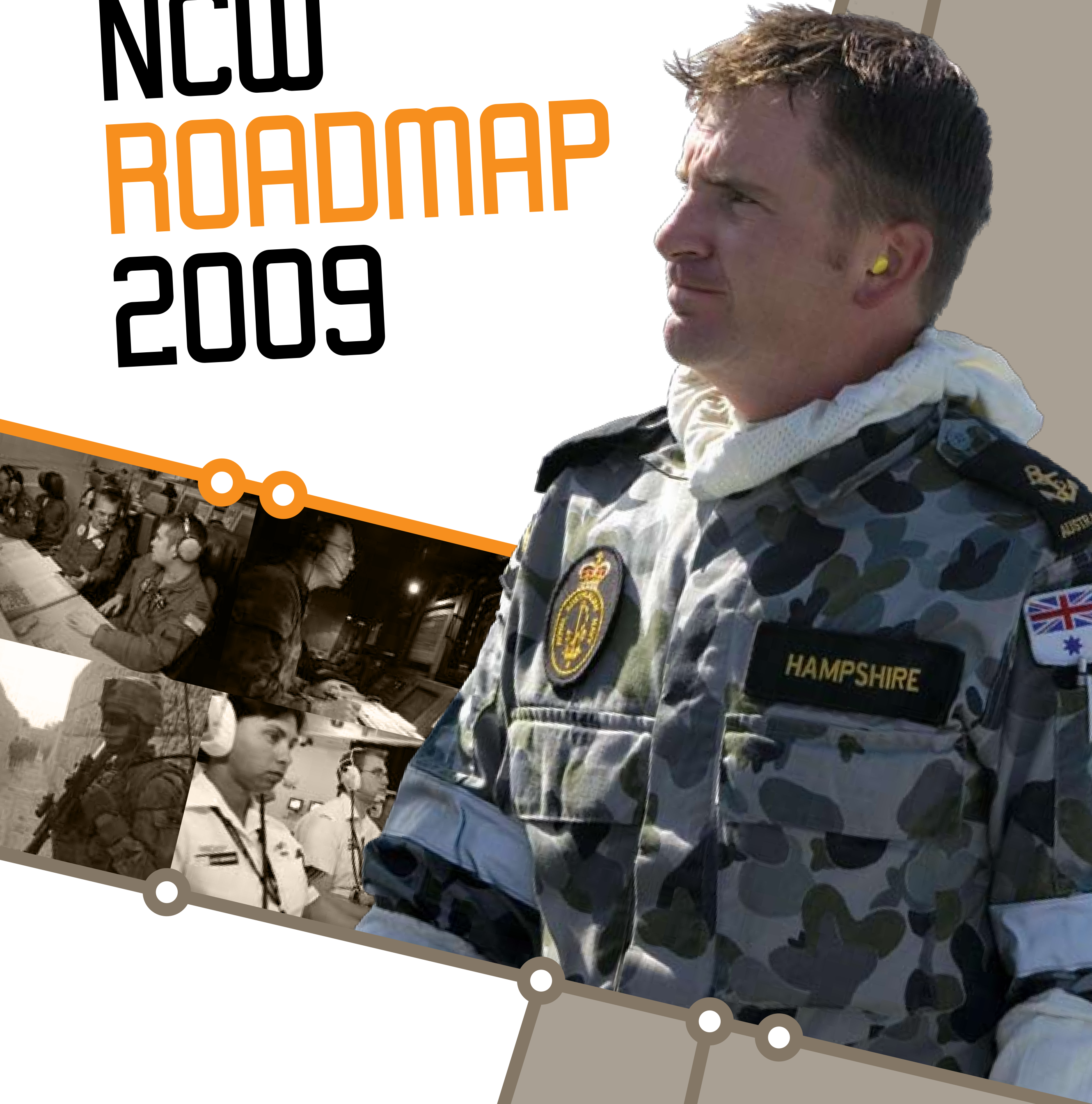
Australian Government

Department of Defence

NCW ROADMAP 2009



Announcement statement - may be announced to the public.

Secondary release - may be released to the public.

All information, whether classified or not, is protected from unauthorised disclosure under the **Crimes Act 1914**. Defence information may only be released in accordance with the **Defence Security Manual** and / or Defence Instruction (General) OPS 13-4-**Release of Classified Defence Information to Other Countries**, as appropriate.

Sponsor

Chief Capability Development Group

Developer

Director General Capability and Plans

Publisher

Corporate Graphics - Defence Publishing Service
Campbell Park Offices
CANBERRA ACT 2600

DPS:FEB005/09

Australian Government

Department of Defence

NCWROADMAP2009

Foreword

In response to both the warfighting complexities of the information age and the requirement to harness the warfighting advantages offered by modern technology, the Australian Government in its recently released 2009 Defence White Paper, *Defending Australia in the Asia Pacific Century: Force 2030*, has stated that Defence is to continue its efforts in building a networked Australian Defence Force (ADF).

As a key enabler to the networked ADF, and as first cited by the Chief of the Defence Force in the *Joint Operations for the 21st Century*, Network Centric Warfare (NCW) is to be implemented through the use of modern technology to link sensors, command and control and engagement systems; and through the development of our people, doctrine and organisations within a networked ADF.

As the Chief Capability Development Group, I am responsible to the Chief of the Defence Force for the development and coordinated implementation of NCW-enabled capabilities within a networked ADF. These responsibilities present significant challenges, given the extent to which NCW manifests itself across nearly all aspects of Defence. In particular, the implementation of NCW-enabled capabilities across the Services and Groups will require extensive collaboration and coordination across the whole-of-Defence to ensure that the technical, cultural and organisational impediments to progress are identified and removed.

It is therefore my intent to centrally coordinate Defence's efforts and to have in place the mechanisms required to build this collaborative effort across Defence. This also means engaging expertise from outside of Defence, through collaborative partnerships with industry, other government agencies and our allies, if Defence is to gain the maximum leverage possible in developing a networked ADF.

Pivotal to achieving such collaboration and coordination is the requirement to clearly articulate Defence's intentions for the development of the networked ADF. I therefore commend to you the 2009 NCW Roadmap, endorsed by the Defence Committee 28 Sep 09 which builds on the 2007 NCW Roadmap but with a renewed emphasis on the actions required to continue the ADF on its transition to a networked force.

M.J. TRIPOVICH, AM, CSC
Vice Admiral, RAN
Chief Capability Development Group

1 October 2009

Executive Summary

The 2009 Defence White Paper, *Defending Australia in the Asia Pacific Century: Force 2030*, explains how the Australian Government plans to strengthen the foundations of the nation's defence. In particular, the White Paper lays out the Government's plans for the development of 'Force 2030'.

As part of that development, Defence is to build a networked Australian Defence Force (ADF) by progressively delivering networked maritime, land, air, and intelligence, surveillance and reconnaissance (ISR) domains.

The implementation of the Network Centric Warfare (NCW) concept across the ADF is a key enabler for the development of a networked force. The NCW concept uses technology to link sensors, decision-makers and weapon systems, helping people to work more effectively together to achieve the commander's intent.

The 2009 NCW Roadmap updates the 2007 roadmap. It outlines the requirements, future directions and actions to be taken to transition the ADF to a networked force, with particular emphasis on four key actions:

- **setting NCW milestones** to establish structured goals and time frames for NCW-related initiatives, which will progressively build to achieve the networked force;
- **establishing an integrated network** to link sensor, command and control, and engagement systems across the ADF, to integrate and exchange information between those systems, and to provide the underlying information and communications infrastructure that the networked ADF will be built-on;
- **developing the human dimension** of NCW to prepare the ADF and its people for operating in an increasingly networked battlespace, through changes in doctrine, organisation, training and education, with an emphasis on 'learning by doing'; and
- **accelerating the process of change and innovation** to take advantage of advances in knowledge, processes and technology, refining these aspects through increased experimentation.

The ADF also needs to develop and deploy fully integrated services that are interoperable with other government agencies, allies and coalition partners. Some legacy systems in the ADF will also need to function in that integrated environment until replaced. Critically, for the best effect and cost, a networked ADF must be based on capabilities that are designed to be interoperable from inception, not as an afterthought in the development process.

While the 2009 NCW Roadmap provides a broad approach for the achievement of the networked ADF, a planned NCW Integration and Implementation Strategy (NCWIIS) will detail the actual ways and means to develop capabilities that are effectively integrated within a networked force.

Warfighting in the information age requires the use of modern technology and networked capabilities, but it remains a human endeavour. It is critical that Defence balances the science of war (technological capabilities) and the art of war (human capability) in the development and implementation of NCW in Force 2030.

Contents

Part 1 **Introduction** 1

Background 1

Purpose, scope and structure 2

Roadmap Development 3

Alignment with other roadmaps 4

Further reviews 4

Part 2 **Development of NCW within Defence** 7

Current strategic guidance 7

The NCW concept 9

NCW target states 13

The NCW development path 15

Current force status 17

Recent operational experience 22

Part 3 **Advancing NCW within Defence** 25

Required actions 25

Action 1 - Setting NCW Milestones 25

Operational test and evaluation of NCW milestones 40

Operational vignette for 2020 Networked Force 42

Action 2 - Establishing the integrated network 45

Action 3 - Developing the human dimension 47

Action 4 - Accelerating the process of change and innovation 50

NCW integration and implementation 52

Opportunities and threats 61

Part 4 **Key messages** 65

References and abbreviations 66

1

Part 1 Introduction

> *Defence will release a 2009 Roadmap that will clearly articulate the steps to be taken in transitioning the Australian Defence Force to the networked force. These steps will go beyond technical network initiatives to embrace the cultural, procedural and training enhancements needed to transform the Australian Defence Force into a balanced, networked and deployable force.*
>
> Minister for Defence, 2009 Defence White Paper Media Release, 2 May 2009

Background

1.1 In early 2003, the Chief of the Defence Force (CDF) announced that the Australian Defence Force (ADF) would pursue Network Centric Warfare (NCW). The aim was to adapt to the emerging needs of information age warfare and enhance the ADF's warfighting effectiveness through the development of the 'Seamless Force' (as described in *Force 2020*). Since then, Defence has released three successive NCW Roadmaps and three associated 'capstone' documents and, most importantly, the ADF has developed nascent NCW-enabled capabilities and employed them on operations.

1.2 The first NCW Roadmap in 2003 was an internal Defence document that sought to unify initial efforts to set the ADF on the road to becoming a networked force. The 2003 NCW Roadmap also set long-term goals (out to 2020) for the implementation of NCW within the ADF.

1.3 In 2004, Defence released *Enabling future warfighting: Network Centric Warfare*, a capstone document that introduced the concept of 'multidimensional manoeuvre' (MDM) and set out how NCW would enable warfighters to employ MDM in warfighting. Positioning NCW in this context established the guiding principle that NCW was not an end in itself, but a means to an end – a way of enhancing warfighting capability and enabling the capacity to fight in the future.

1.4 The 2005 NCW Roadmap was a public document that clarified how the long-term goals set in 2003 would be accomplished – they would be linked to projects in the Defence Capability Plan (DCP) through a series of milestones. Launching the roadmap, the Chief Capability Development Group noted the need to develop partnerships with industry, other government agencies and our allies to gain maximum leverage for the development of NCW within the ADF. That principle has been an integral part of NCW development ever since.

1.5 In 2007, Defence released *Joint operations for the 21st century*, which built on Force 2020 but introduced the Future Joint Operating Concept (FJOC). The subsequent 2007 NCW Roadmap refined the 2005 roadmap, but grouped the NCW milestones into six domains: maritime; land; air; intelligence, surveillance and reconnaissance (ISR); joint force; and networked coalition.

1.6 In May 2009, the Government released the Defence White Paper, *Defending Australia in the Asia Pacific Century: Force 2030*. The 2009 White Paper explains how the Government plans to strengthen the foundations of Australia's defence and, in particular, lays out plans for the development of Force 2030, including the major investments in capability that will need to be made in the coming years.

1.7 The 2009 NCW Roadmap has been developed in line with the Government's new plans. Together with the Defence Capability Plan (DCP) 2009 and the operational lessons learned since 2007, it is the basis for the development of Force 2030.

1.8 From an ICT perspective, the Defence Information and Communication Technology Strategy will strengthen the relationship between the capabilities needed to meet Defence's strategic objectives and the final products and services delivered by Defence ICT. That relationship will be enhanced by ensuring stakeholders can prioritise relevant ICT investments and by fostering a more responsive and agile ICT organisation.

Purpose, scope and structure

1.9 The purpose of the 2009 NCW Roadmap is to clearly articulate to Defence, industry, other government agencies and our allies the requirements, future direction and actions to be taken to transition the ADF to a networked force as part of Force 2030.

1.10 Compared to its 2007 predecessor, the 2009 NCW Roadmap places greater emphasis on explaining the framework and logic of the NCW concept and the NCW 'target states' (Part 2) and on advancing NCW within Defence (Part 3). Of course, because the roadmap is a public document, there are some limits on the information it provides.

1.11 In Part 2, the roadmap shows the linkages between current strategic guidance and the NCW concept, from which Defence's NCW target states and the NCW development path have been derived. Part 2 also provides an overview of NCW achievements since 2007 and future intentions for NCW development.

1.12 Part 3 focuses on the actions needed to continue the ADF's transition to a networked force:

- **Action 1 – Setting NCW milestones** — to establish structured goals and time frames for NCW-related initiatives that will progressively build to achieve the networked ADF and the NCW target states.
- **Action 2 – Establishing an integrated network** — to link sensor, command and control (C2) and engagement systems across the ADF, effectively integrate and exchange information between these systems, and provide the information and communications infrastructure upon which the networked force will be developed.
- **Action 3 – Developing the human dimension** — to prepare the ADF and its people for operating in a networked battlespace through changes in doctrine, organisation, training and education, with an emphasis on 'learning by doing'.
- **Action 4 – Accelerating the process of change and innovation** — to take advantage of advances in knowledge, processes and technology, which will require tapping into the broadest possible knowledge and ideas base across Defence and industry, and refining that knowledge through increased experimentation.

1.13 Part 3 also describes NCW integration and implementation requirements and introduces the NCW Integration and Implementation Strategy (NCWIIS). When completed, the NCWIIS will detail the proposed 'systems of systems' architecture approach to the integration and alignment of existing and future ADF capabilities in the networked battlespace. Part 3 concludes by summarising the opportunities that can be exploited and the threats that must be addressed to advance NCW within Defence.

Roadmap development

1.14 In developing the 2009 NCW Roadmap, Defence conducted a series of reviews of the 2007 NCW Roadmap to consider changes in strategic direction (as informed by the 2009 Defence White Paper), alterations to the DCP (as informed by the DCP 2009) and emerging insights from recent operations, particularly in the development of the human dimension.

1.15 Due to the type of information that had to be considered, most of the reviews were restricted to Defence stakeholders. However, a representative group from Australian industry participated in a Rapid Prototyping Development and Evaluation (RPDE) Program 'Quicklook', providing insights and perspectives on the opportunities and threats involved in transitioning the ADF to a networked force.

1.16 The 2009 NCW Roadmap continues to reflect White Paper and DCP guidance to transition towards the integrated capability envisaged for Force 2030. While recognising that implementing the networked force has resource requirements, the NCW Roadmap does not implicitly provide additional funds for this purpose. This is achieved through the DCP.

Alignment with other roadmaps

1.17 Three Defence capability roadmaps and the ICT Strategy influence the development and advancement of NCW in Defence and should be read together with the 2009 NCW Roadmap:

- The *ISR Roadmap 2007–2017* provides a framework for developing a Defence ISR system that is operationally focused, integrated and interoperable. The ISR domain milestones in the 2009 NCW Roadmap are aligned to the 'establish', 'ensure' and 'extend' phases in the ISR Roadmap.
- The *Defence Simulation Roadmap 2006* sets the course for achieving Defence's vision for the use of simulation through to 2021. Simulation is seen as a low-cost and robust way to test networked capability against Defence military objectives.
- The *Defence Test and Evaluation Roadmap 2008* reviews current Defence test and evaluation (T&E) capability, Defence's strategic planning for future operating environments, and the DCP, to ensure that T&E direction and resources will be adequate to deliver a balanced, networked and deployable force. T&E is essential to demonstrate the achievement of NCW milestones.
- The *Defence Information and Communication Technology Strategy 2009* will provide the framework for achieving one network connecting fixed and deployed locations built on a single set of standards and products. Among many other initiatives, this strategy also identifies the introduction of a Common Operating Picture that will allow deployed commanders and decision makers to have a single view of the battle space through accessing a wide range of data from sensors and sources.

Future reviews

1.18 NCW is integrally linked with dynamic, continuously evolving technology, so the NCW Roadmap must also evolve. It requires regular review and updating to ensure that it remains credible, relevant and aligned with current strategic guidance to meet the emerging needs of the ADF. Therefore, the NCW Roadmap will be reviewed in line with the Government's requirement for a five-yearly Defence White Paper planning cycle.

F3

2

Part 2 Development of NCW within Defence

> *In this complex information age, we must take maximum advantage of the range of sensors, weapons and other systems available to us and must ensure that we adhere to a centrally coordinated plan with execution occurring at the lowest level possible. This requires networking where command and lower level elements can synchronise their efforts to achieve the mission.*
>
> Minister for Defence, 2009 Defence White Paper Media Release, 2 May 2009

Current Strategic Guidance

The 2009 Defence White Paper

2.1 The 2009 Defence White Paper is the most comprehensive statement on Defence ever produced by an Australian Government. It affirms the Government's commitment to the defence of Australia, the protection of our sovereign interests, and the security and stability of our region. It also articulates the strategic priorities for all areas of Defence and lays out the Government's plans for the development of Force 2030.

2.2 The White Paper identifies 'networked capability' as a key attribute of Force 2030. It notes that the capability will help our people to work together more effectively, provide common battlespace awareness and, most crucially, achieve information superiority over an adversary, so that we can make critical decisions on the battlefield more quickly and with better knowledge than the adversary.

2.3 The Government has confirmed that Defence is to build a networked ADF, in which modern technology will be used to link sensors, weapons systems, and commanders and their personnel in a networked environment. We will do this by progressively delivering networked capability in the maritime, land, air and ISR domains. Success will depend on establishing a secure, high-capacity information network that allows personnel in different places to collaborate in real time and to synchronise their operational actions precisely.

2.4 Another crucial characteristic of Force 2030 will be a joint approach that binds single-service capabilities and systems into an operationally seamless whole. The ADF's standard mode of operating will be joint operations involving the three services, other Defence agencies and, in some cases, other government agencies.

2.5 The Government has also stated that Australia must have the capacity to use military power in collaboration with our allies and coalition partners. We must be willing to lead military coalitions when necessary to secure shared strategic interests, or to contribute to military coalitions when it is in Australia's clear interest to do so. To that end, it is important for the ADF to develop and maintain a network of Defence partnerships. This includes efforts to increase the ADF's interoperability with selected allies and partners, such as the United States (US), New Zealand (NZ) and our partners in the Five Power Defence Arrangements, which includes Singapore and Malaysia as well as the United Kingdom.

2.6 The Government has therefore decided that Defence is to have in place the: information, communication and technology (ICT) infrastructure; information tools; command support; battle management systems (BMS) and joint training programs necessary to provide a reliable battlespace network across the entire ADF, which will continue to evolve and mature in subsequent years.

The Future Joint Operating Concept

> *My vision is for the Australian Defence Force to be a balanced, networked and deployable force staffed by dedicated and professional people that operates within a culture of adaptability and excels at joint, interagency and coalition operations.*
>
> CDF, Joint Operations for the 21 Century, May 2007

2.7 The Future Joint Operating Concept (FJOC) is an overarching concept for the future operation of the ADF. It is supported by three concepts that describe the ADF's operation in the three major warfighting environments: the Future Maritime Operating Concept (FMOC), the Future Land Operating Concept (FLOC) and the Future Air and Space Operating Concept (FASOC).

2.8 As a component of the Strategy Planning Framework, the FJOC is also aligned with the Defence Planning Guidance, which articulates the strategic priorities that guide Defence to produce the military outcomes sought by government and the CDF's vision for a balanced, networked and deployable ADF.

2.9 As described in the FJOC, the networked ADF will need assured access to other agency, coalition and open source information capabilities. The networked ADF's ability to operate effectively will also depend on the forces' networks and decision-making infrastructures, early warning systems, communications, environmental monitoring and positional data.

2.10 A networked ADF will need to develop from an initial joint force construct to a force that has fully integrated services that are interoperable between all force elements, other government agencies, and our allies and coalition partners. Legacy systems within the ADF should (as far as possible) also be made to function within that integrated environment until replaced. As the degree of integration is increased, new training systems will also need to be established. Critically, a networked ADF must be based on military capabilities that are designed to be interoperable from the start, not as an afterthought during development.

2.11 Through linking the ADF's sensors, decision-makers and engagement systems to form an effective and responsive whole, implementation of NCW is central to achieving these integration requirements and continuing the ADF transition from a joint construct to an integrated force.

2.12 As part of the FJOC, the ADF has also adopted multidimensional manoeuvre (MDM) as its approach to future warfare. MDM seeks to apply strength against weakness and requires the ability to act fast, to reach out to the critical place at the right time, and to create simultaneous dilemmas that an adversary cannot resolve. The ability to employ the NCW concept, whether within a joint task force, multi-agency or coalition setting, is fundamental to MDM.

The NCW concept

> *NCW is a means of organising the force by using modern information technology to link sensors, decision-makers and weapon systems to help people work more effectively together to achieve the commander's intent.*
>
> Explaining NCW, December 2005

2.13 *Enabling Future Warfighting: Network Centric Warfare*[1] describes the 'NCW concept' in the context of enabling warfighters to employ MDM, which, enabled by information superiority, uses the warfighting attributes of tempo, agility and ability to fight asymmetrically.

2.14 Although NCW is not itself a warfighting concept, it will strengthen the warfighting capability of the ADF by linking sensor, command and control and engagement systems. At the centre, connecting those systems, is a network (as the name implies) (see figure 2-1).

[1] Australian Defence Doctrine Publication D.3.1.

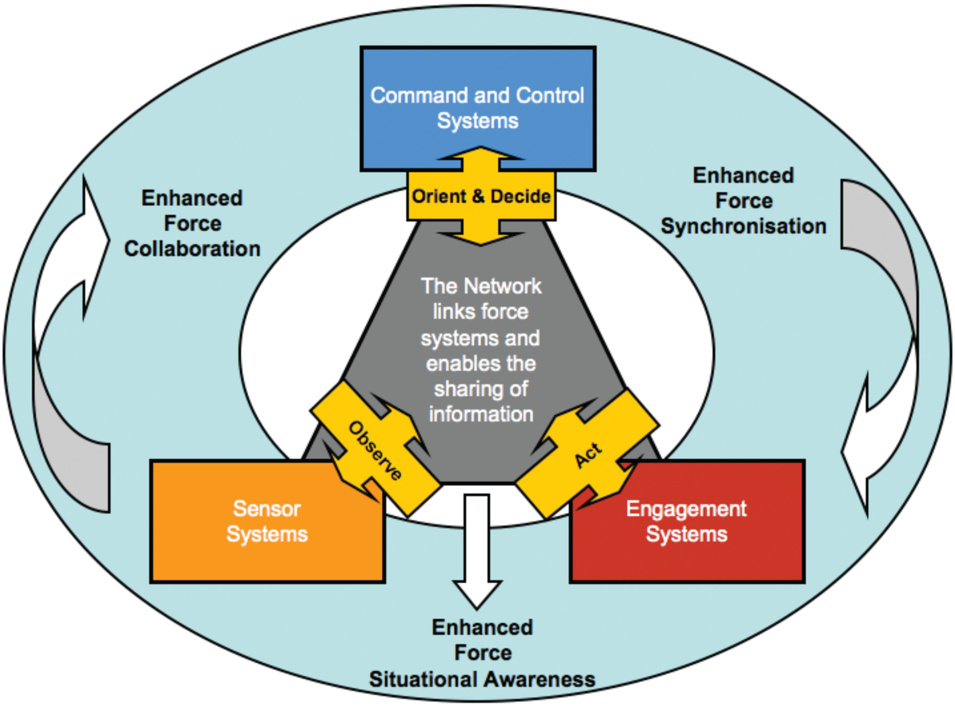

Command and Control Systems
Enhanced Force Collaboration
Orient & Decide
Enhanced Force Synchronisation
The Network links force systems and enables the sharing of information
Observe
Act
Sensor Systems
Engagement Systems
Enhanced Force Situational Awareness

Figure 2-1: The Network Dimension[2]

2.15 Linking systems across organisational and geographical boundaries through robust networking allows better sharing of information that is timely, relevant and, most importantly, trusted. Sharing information enhances force collaboration and synchronisation across the force which increases situational awareness. Ultimately, NCW will allow a force to act before an adversary acts, and to reach out to the right place at the right time with the right force to achieve the right effect.

2.16 While the development of the network is a critical aspect in the implementation of NCW, it is only one aspect of a multidimensional environment.

[2] The systems shown here are not always distinct, and some systems are a combination of all. For example, an offensive fire support system, although mainly an engagement system, also includes sensor and C2 systems.

2.17 Implementing NCW to enhance a force's warfighting capability is also based on the human dimension of warfighting. Developing the human dimension is as important as building the network.

2.18 Two particularly important human qualities are the ability of individuals within a force to effectively apply their skills, knowledge and attitudes to the task at hand ('professional mastery'), and their ability to apply a unifying but decentralised command philosophy, based on the achievement of a commander's intent ('mission command'). To develop both, the ADF needs to maintain and build on its high standards of leadership, training, education and doctrine, while adapting its structures and organisational relationships to foster new ways of sharing information, building trust and expanding collaboration across the force.

2.19 The network and human dimensions of NCW are not mutually exclusive, although each has its own distinctive characteristics. Because trust and information sharing (and the influences they have on shared situational awareness, collaboration and decision-making) are interlinked, the network and human dimensions of NCW must be connected to each other, or 'networked'. These networking requirements are evident in the relationships between three warfighting 'realms' (as shown in figure 2-2):

- **The information realm** – where information is created, managed, stored and manipulated. In this realm, connectivity allows people to share, access and protect information.
- **The cognitive realm** – in the mind of the warfighter. In this realm, connectivity allows people to develop a shared understanding of the commander's intent, to identify opportunities in the situation and vulnerabilities in an adversary.
- **The physical realm** – the traditional realm of warfare, where a force is moved through time and space, spanning the environmental domains of sea, land, air and space, to execute an operation. In this realm, selected force elements are equipped to achieve secure and seamless connectivity and interoperability and, based on the shared understanding that is developed, synchronise their actions.

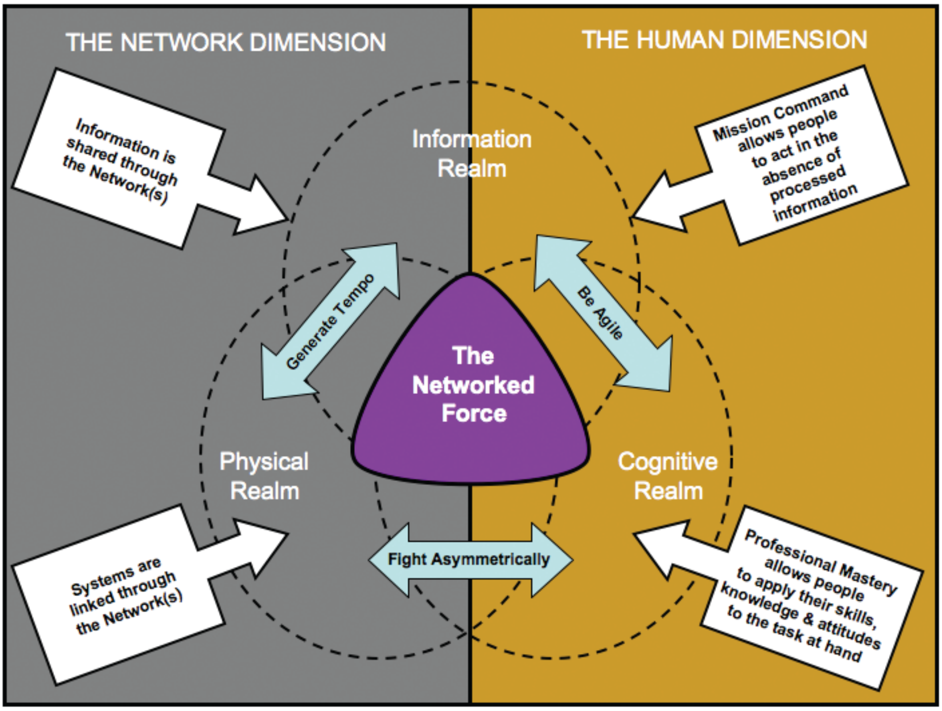

THE NETWORK DIMENSION
THE HUMAN DIMENSION
Information is shared through the Network(s)
Mission Command allows people to act in the absence of processed information
Information Realm
Generate Tempo
Be Agile
The Networked Force
Physical Realm
Cognitive Realm
Systems are linked through the Network(s)
Fight Asymmetrically
Professional Mastery allows people to apply their skills, knowledge & attitudes to the task at hand

Figure 2-2: Networking - connecting the network and human dimensions

2.20 The networks developed within these realms, and across the network and human dimensions, will result in a force that can generate tempo, be agile and fight asymmetrically. However, because the networks are inherently complex, there are significant challenges in building them.

2.21 Underlying these challenges is the added complexity of information management and information translation, which are necessary for the effective communication and exchange of information and data. Such requirements have typically been managed manually, but a dynamic networked force will need to take a more responsive and automated approach. That approach will require new policies, processes, procedures and mechanisms to ensure the accuracy, timeliness, accessibility, security and completeness of information shared within the networked force.

NCW target states

2.22 *Enabling Future Warfighting* also identifies future ADF warfighting functions that NCW implementation will strengthen: information superiority and support; command and control; force deployment; force application; force protection; and force generation and sustainment. The ADF's aspirations for a networked force (or 'target states') have been derived from the functions below:

- **Information superiority and support** – The ADF will have information superiority through ISR capabilities, intelligence collection and assessment systems, space-based surveillance systems (including intelligence-collecting satellites), cyber warfare, electronic warfare (EW), strategic communications, battlespace management and command support systems. The ADF will also have effective information management and continuous information connectivity to link sensors, decision-makers and fighting units in a way that provides comprehensive situational awareness and the ability to act both decisively and precisely. Typical attributes of information superiority and support are:
    - seamless interfaces between fixed and deployed elements within the 'Defence information environment' and between Australian and allied or coalition intelligence domains
    - all-source coordination of information collection and tasking across national, allied, coalition and ADF-controlled capabilities
    - processing and analysis of information to provide integrated intelligence products to the right people at the right time, giving friendly forces an awareness of the situation that is superior to an adversary's
    - an information architecture robust enough to ensure continuous system availability under demanding conditions, including frequent cyber attacks by an adversary.
- **Command and control** – Effective command and control (C2) of joint forces relies on information superiority. The ADF's C2 system will be a fully integrated command support system, covering all levels of operation and all environments, with the ability to participate in coalition operations and to collaborate with other agencies. Typical attributes of superior C2 systems are:
    - commanders with a virtual presence before senior decision-makers
    - decision support tools that are an integral and trusted element of decision-making by commanders and their staff, allowing rapid and effective decisions in all situations
    - trusted and capable commanders, able to adapt and employ highly flexible command arrangements to accomplish missions
    - the ability to filter information to speed decision-making in ambiguous circumstances.

- **Force deployment** – The ADF will be capable of rapid and accurate identification, and the protected deployment, of an optimised force. Typical attributes are:
  - deployable assets with access to appropriate areas of the 'common operating picture' (COP) and the tactical information environment
  - deployment of forces with maximum efficiency and minimal risk of interdiction en route
  - deployment agility through self-synchronisation.
- **Force application** – The ADF will be capable of applying force precisely to minimise unintended consequences. Precision targeting and discrimination technologies and systems are particularly important. Typical attributes are:
  - the ability to accurately apply an appropriate level of force in close combat and from standoff ranges in complex environments
  - the ability to identify friendly, hostile and neutral forces in the battlespace with greater accuracy
  - through use of the COP there is a greatly reduced possibility of fratricide, fewer platforms are deployed or on standby, and supporting friendly forces are more effective on the battlefield
  - a robust ability to obtain and securely share data on the effects of the ADF's application of force in demanding environments.
- **Force protection** – The ADF will be capable of protecting itself against a range of threats. Forces deployed or not, will have a pervasive network of active and passive sensors automatically fused into a COP for better shared situational awareness. Typical attributes are:
  - the ability to predict and identify a wide range of environmental threats and protect forces against them
  - a network continuously available in the face of determined attacks on it
  - the fusion of information and intelligence to provide automatic early warning through secure protected networks
  - the ability to counter an adversary's information operations to the point at which those operations have minimal capacity to prevent the ADF's desired result
  - NCW enabled capabilities that positively contribute to the protection of the force and are designed to not detrimentally affect the vulnerability of force elements.

- **Force generation and sustainment** – Key ADF logistic networks in the national support area are linked to those in the field, allowing us to securely connect to and exchange information with industry and our allies and coalition partners. Typical attributes are:
    - end-to-end visibility of the logistic system for commanders, allowing them to quickly allocate resources to generate and sustain deployed force elements
    - automated ordering and replenishment of supplies and ordnance as they are consumed
    - minimal vulnerability and much greater mobility through more effective supply chains, optimum force presence and precise sustainment of most logistic requirements.

The NCW development path

> *Force 2030 will be a joint force. Our single service capabilities and systems will be bound together in a seamless whole. Joint task forces will be the standard. Force 2030 will be networked. Maritime, land, air and the intelligence, surveillance and reconnaissance elements will share information that will provide unprecedented situational awareness. Force 2030 will be balanced and flexible—a force with depth that is able to adapt rapidly to diverse tasks.*
>
> CDF Order of the Day, Release of the 2009 Defence White Paper, 4 May 2009

2.23 Defence's path to achieve its NCW target states follows three development phases (see figure 2-3):

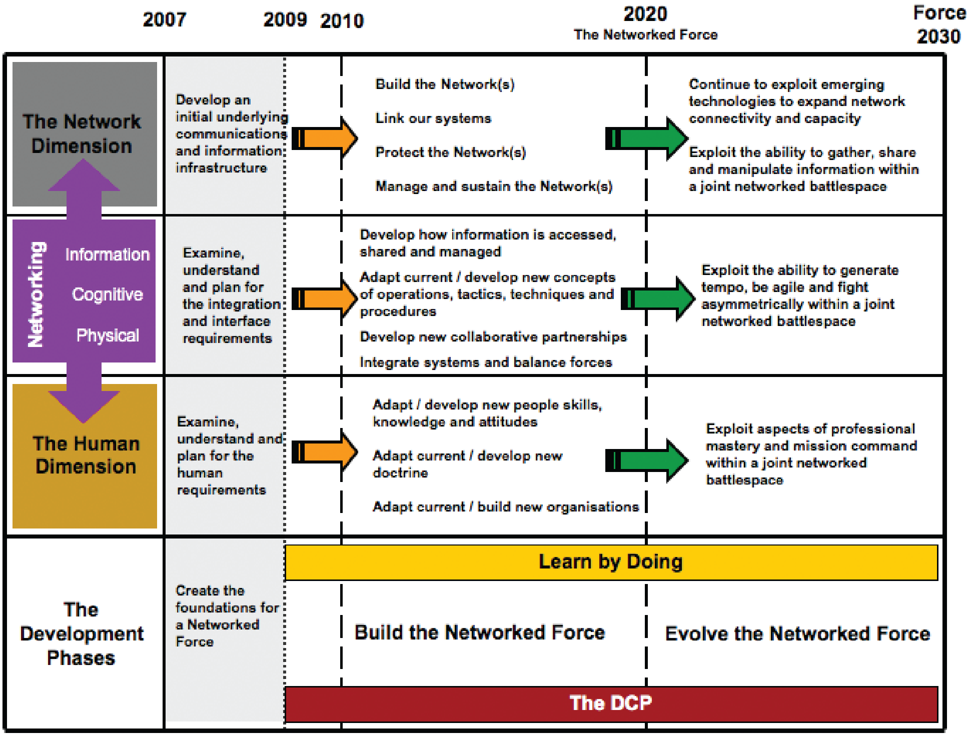
- creating the foundations for the networked force
- building the networked force
- evolving the networked force towards Force 2030

2.24 Within the three phases, a series of development actions must be taken in the two dimensions of NCW (network and human), and in the networking of the information, cognitive and physical realms. The DCP underpins those development actions by developing and delivering the necessary military capabilities across the ADF.

2.25 Defence has adopted a 'learn by doing' approach to build the networked force. That approach draws on improved information sharing, enabled by better connectivity, to identify further opportunities for collaboration and synchronisation.

2.26 The creation of a Single Enterprise Architecture to support the networked force build is fundamental to achieving the necessary collaboration and synchronisation. A key aspect of architectural design is the development and use of architecture framework views to establish a 'common language' between diverse stakeholders, to manage the inherent complexity of system of systems, particularly under the influence of diverse mission requirements, and to enable incremental capability development and integration into the force structure.

2.27 The willingness to adapt and to develop new ways of doing Defence business is essential if we are to ensure that such opportunities do not result merely in the automation of current processes.



2007 2009 2010 2020 The Networked Force Force 2030

The Network Dimension

Develop an initial underlying communications and information infrastructure

Build the Network(s)

Link our systems

Protect the Network(s)

Manage and sustain the Network(s)

Continue to exploit emerging technologies to expand network connectivity and capacity

Exploit the ability to gather, share and manipulate information within a joint networked battlespace

Networking: Information, Cognitive, Physical

Examine, understand and plan for the integration and interface requirements

Develop how information is accessed, shared and managed

Adapt current / develop new concepts of operations, tactics, techniques and procedures

Develop new collaborative partnerships

Integrate systems and balance forces

Exploit the ability to generate tempo, be agile and fight asymmetrically within a joint networked battlespace

The Human Dimension

Examine, understand and plan for the human requirements

Adapt / develop new people skills, knowledge and attitudes

Adapt current / develop new doctrine

Adapt current / build new organisations

Exploit aspects of professional mastery and mission command within a joint networked battlespace

The Development Phases

Create the foundations for a Networked Force

Learn by Doing

Build the Networked Force

Evolve the Networked Force

The DCP

Figure 2-3: Developing the networked force

2.28 The effectiveness of learning by doing depends critically on the development of the network dimension, which involves specific DCP initiatives:

- **Enabling communications infrastructure** – includes projects that will deliver the communications network required to achieve the connectivity and interoperability we need across sensor, C2 and engagement systems.
- **Enabling information systems** – includes projects that will deliver the information systems needed to support and share information across the functions of C2, ISR, imagery and geospatial information.
- **Enabling common information services** – includes projects that provide the coordination and information assurance infrastructure needed to manage system access, data exchange, data security and integration across developed information systems.

Current force status

2.29 Since the release of the 2007 NCW Roadmap, the ADF has made steady progress in creating the foundations for NCW in Defence. An initial information and communications infrastructure has been established and is being used to link geographically separated force elements and selected systems.

2.30 However, progress across the ADF varies. The maritime and air domains are most advanced because of their longstanding experience with data links, satellite communications and network-type operations with our allies and coalition partners.

2.31 The section below sets out the current status, achievements since 2007, and future plans[3] of the lead services and groups for each of the environmental domains that make up the networked ADF.[4]

[3] The NCW milestones that describe future capability increments within each of the domains are described in Part 3.

[4] Further detail on the specific projects referred to below for lead Services and Groups can be found in the Defence Capability Plan.

Joint Operations Command and the Joint Force Domain

2.32 The Headquarters Joint Operations Command (HQJOC) Bungendore was designed, fitted and staffed to enable it to transform how the ADF supports its deployed force elements in the 21st century.

2.33 The critical enabler of that interaction has been the development of HQJOC's command, control, communication, computing and intelligence systems and their networking into the strategic, operational and tactical levels of Defence. This has been achieved through innovations in the system infrastructure, such as real-time C2 systems, enabling tactical data links (TDL) and data network management for the evolving Joint Interface Control Officer and Joint Data Network Officer capabilities. Other assets include remote tactical radios, an all informed 'knowledge wall' and 12 multi-level security video conference briefing/contingency rooms.

2.34 Within the operational theatres, the use of traditional and legacy systems alongside emerging technologies has required changes in how the ADF conducts operations. New systems, providing force tracking, force protection, enhanced ISR and improved command, control and communications (C3), enable commanders at all levels to make informed, rapid decisions. These systems are true 'force multipliers'.

2.35 The human dimension of HQJOC's transformation is vital. Desktop video conferencing, multi-level security instant messaging and other technologies allow the commander to talk face to face with key staff and other stakeholders. Liaison officers from whole-of-government, Defence and coalition organisations can now be virtually embedded, enabling the fusion of information for the conduct and planning of operations.

2.36 HQJOC will continue to mature as the infrastructure and staff are stabilised and procedures refined. The merging of the strategic, operational and tactical levels of Defence's communications is critical to that maturity. There are a number of Defence projects referred to in part three that will contribute to the development of a networked joint force.

The Navy and the maritime domain

2.37 The efforts of the Royal Australian Navy to maintain a knowledge edge are resulting in some of the greatest changes to maritime communications since the early 1960s.

2.38 Major projects in such areas as military satellite capability (JP 2008) and the modernisation of maritime and high-frequency communications (SEA 1442, JP 2043), have changed the way information is managed and used in the maritime domain. Conducting seamless joint and coalition operations in widely dispersed theatres will require significant new technologies, such as broadband communications bearers with global reach, networks secure at many levels, and a suite of applications tailored for the maritime war fighter.

2.39 This knowledge edge will become critical with the delivery of the landing helicopter dock (LHD) in 2015 (JP 2048) and the air warfare destroyer (AWD) (SEA 4000) in 2016. These platforms will need a high level of situational awareness to be effective. They will depend heavily on communications and timely access to all contributors to the surveillance picture, including value added data from sensors such as unmanned aerial vehicles (UAVs), submarines and airborne early warning and control (AEW&C) aircraft. They will also need rapid access to complex imagery from satellites and intelligence and hydrographic assets. There are a number of other Defence projects referred to in part three that will contribute to the development of a networked maritime domain.

2.40 The Navy's tactical data link (TDL) capabilities are essential to ensure that engagement quality data is available. The continued introduction of Link 16 TDL, and the maintenance of legacy Link 11 TDL capabilities for interoperability with our allies and legacy ADF platforms, will ensure that this capability evolves. The modernisation of the Navy's TDL capability needs to move ahead to maintain a terrestrial TDL capability when our forces operate with coalitions or allies in dispersed theatres over long distances.

2.41 An additional valuable benefit from the introduction of broadband services and local area networks at sea is that they improve the quality of life of our sailors deployed at sea, including the provision of access to the internet.

The Army and the land domain

2.42 Networking is a key component of the Australian Army's capabilities. Recent operational experience has confirmed the need to be able to link sensors to a command grid and to provide access to an engagement grid, but the number of 'nodes' (individual vehicles and dismounted soldiers, in the land domain) is a significant challenge. Almost any node has to have integration with joint and interoperability with coalition forces, so the Army faces a complex challenge. Relatively austere communications, the need for mobility, and difficult operating environments make it difficult to give our soldiers a tactical ISR capability and the ability to draw on strategic ISR resources.

2.43 The 'variable message format' standard will be the backbone of tactical data exchange for the Army, supporting networking and integration on the ground. Three key projects will deliver a networked capability to Army: the Battlespace Communications System – Land (JP 2072); the Battlefield Command Support System and Battle Management System (BMS) (Land 75); and the Soldier Enhancement (Land 125) project. These projects will provide a common BMS capability, linking vehicles and dismounted soldiers via digital communications. It is anticipated that any future protected mobility platform in the land domain will also contribute to the networking capability. There are a number of other Defence projects referred to in part three that will contribute to the development of a networked land force.

2.44 Through its operational experience, the Army knows that networking is a force multiplier. The ability to detect adversaries and pass information rapidly and seamlessly enables rapid decision-making, targeting and engagement. The establishment of a communications architecture that links all land elements allows them to synchronise more effectively and to perform more tasks more efficiently. However, ongoing operational deployments will challenge the Army's coordination and implementation of network enabled capabilities in the land domain.

The Air Force and the air domain

2.45 The Royal Australian Air Force's vision is to be a balanced expeditionary and networked air force able to achieve the Australian Government's objectives through the swift and decisive application of air and space power in joint operations or as a part of a coalition force. NCW is a key enabler of that aspiration.

2.46 Work to establish a networked air combat capability is continuing through several major Air Force projects, including Wedgetail – Airborne Early Warning & Control (AIR 5077), F/A-18 upgrade (AIR 5376) and Vigilare – Air Defence C2 system (AIR 5333). These projects are close to delivering the key C2, sensor and communications systems that the Air Force needs to contribute to joint or coalition operations more effectively. Other significant Air Force projects, including New Air Combat Capability (NACC) (AIR 6000) and Maritime Patrol Aircraft capability (AIR 7000 Phase 2), will also introduce enhanced ISR, EW and engagement capabilities.

2.47 The deployment of the Tactical Air Defence System, the Mobile Regional Operations Centre, and Surveillance and Response Group personnel to Afghanistan has provided a good opportunity to learn by doing. In particular, conducting Link 16 TDL operations as part of a coalition force is contributing to the Air Force's development of the human dimension of the networked force. Other Surveillance and Response Group personnel and AP-3C aircraft are developing their expertise in ISR operations. The knowledge gained by air force personnel is stimulating the development of the Air Force's doctrine, training and education. Knowledge and experience gained on operations will be essential to unlock the emergent capabilities of networked air assets.

2.48 Emerging knowledge being applied most immediately to enable a limited developmental Link 16 TDL capability will allow the development of shared doctrine, tactics and procedures between the Surveillance and Response Group and the Air Combat Group. This will also help prepare the Air Force for the introduction of Link 16 capabilities provided with Vigilare and Wedgetail. There are a number of other Defence projects referred to in part three that will contribute to the development of a networked air domain.

The Intelligence and Security Group and the ISR domain

2.49 The collection, analysis and dissemination of intelligence to support leadership decision-making are fundamental parts of developing an effective networked ADF. The Intelligence and Security (I&S) Group also has a critical NCW role in the provision of geospatial data and products to Defence.

2.50 The Deputy Secretary I&S, as the capability manager for intelligence, will drive the group's support for NCW, supported by the director of the Defence Imagery and Geospatial Organisation (DIGO), as the coordinating capability manager for geospatial information.

2.51 I&S Group will continue to develop its capabilities in line with the NCW roadmap. The group's projects will enable the collection of information about current and emerging threats, rigorous analysis of the threats, and timely dissemination of intelligence to decision-makers in Defence and elsewhere in the Government. These projects ensure that information is fused with other sources, wherever possible, and is delivered securely, clearly and in good time to allow essential all-source analysis.

2.52 The I&S Group must ensure that uniform applications are used to deliver intelligence and geospatial information to users, that data formats are interoperable with allied systems, and that intelligence can be released to the widest appropriate audience. The group has reviewed its classified ICT systems to improve information connectivity, promote collaboration and achieve efficiencies.

2.53 DIGO will implement a geospatial strategy that will acquire and manipulate geospatial information and disseminate it throughout Defence. DCP projects such as Geospatial Information Infrastructure and Services (JP2064) and Digital Topographical Systems Upgrade (JP 2044), will be necessary to ensure that this evolutionary process supports the implementation of NCW. There are a number of other Defence projects referred to in part three that will contribute to the development of a networked ISR domain.

2.54 DIGO has reviewed its operations at the Geospatial Analysis Centre in Bendigo and identified initiatives to double the productivity of the centre, in response to burgeoning requirements for geospatial data.

Recent operational experience

> *It is a law of war that the greater the dependency on a capability, the higher the payoff to an enemy who can lessen its utility, in effect turning our strength into a weakness.*
>
> Colin S. Gray, *The 21st century security environment and the future of war,*
> Winter 2008-09

2.55 The ADF has exploited opportunities to learn from experience in the Middle East Area of Operations (MEAO). The geographical spread of operations, their remoteness from Australia, the complexity of the network, and the variety of deployed force elements and their equipment have created both challenges and lessons.

2.56 The network systems in use across the MEAO vary from voice to data, unclassified to top secret, deployable to fixed, and through the radio spectrum from high frequency (HF) to microwave. Competition within the spectrum is also fierce, and good management, training and technical tools are needed to sustain efficient and effective network usage, particularly when bandwidth is limited. However, finding solutions to these technical problems is easier than supplying the training that will allow the ADF to support interdependent roles and the development of concepts of operations (CONOPs) and related doctrine.

2.57 Recent operational experience in the MEAO has also demonstrated that better information sharing and more collaboration through networks can improve decision-makers' understanding of the situation. There is a risk though of overreliance on 'the screen'. Information will not always be perfect, and judgement, tactical awareness and common sense are still required.

2.58 Large amounts of information can also lead to 'information overload', so it is critical for information management systems to be able to identify what is critical and ensure that such information is not lost. The 'battle for information' is becoming more important in the conduct of operations and is developing into a major activity in its own right, rather than an operation support activity.

2.59 As an information sharing tool, the US approach to web-browsing and the use of chat rooms has also gained much support.

2.60 Synchronisation across a force improves when resources and activities are focused to produce combat power at the decisive time and place. Commanders and individual combatants can recognise changes and opportunities, and can then act without direction to achieve a commander's intent.

2.61 In coalition operations, synchronisation depends on common procedures, a shared understanding of the commander's intent, collaborative planning and mission rehearsals, and a mutual appreciation of the cultural differences within the coalition. Effective force synchronisation in coalitions also depends greatly on having in place agile and adaptable C2 systems that accommodate the various force elements, effects and, most importantly, the adaptiveness of a 'thinking adversary'.

3

Part 3 Advancing NCW within Defence

The development of a networked ADF presents new challenges in the way Defence manages the projects which deliver our capability and will also require significant coordination, cross project collaboration and on-going liaison with industry.

The support of a comprehensive joint training and education program and a clear master plan with key milestones will be of particular importance in achieving these objectives.

Minister for Defence, 2009 Defence White Paper Media Release,
2 May 2009

Required actions

Action 1 – Setting NCW Milestones

3.1 Eighteen milestones have been established to set the program for NCW development out to 2020. Each milestone is dependent on successful completion of essential projects from the Defence Capability Plan. Figure 3-1 shows how the milestones are constructed across the environmental domains (maritime, land, air and ISR) and how from here they build toward the achievement of joint force and networked coalition domain milestones. 'Inter-domain' relationships are also an important component.[5]

[5] See paragraph 3.24 for further explanation on 'inter-domain' relationships.

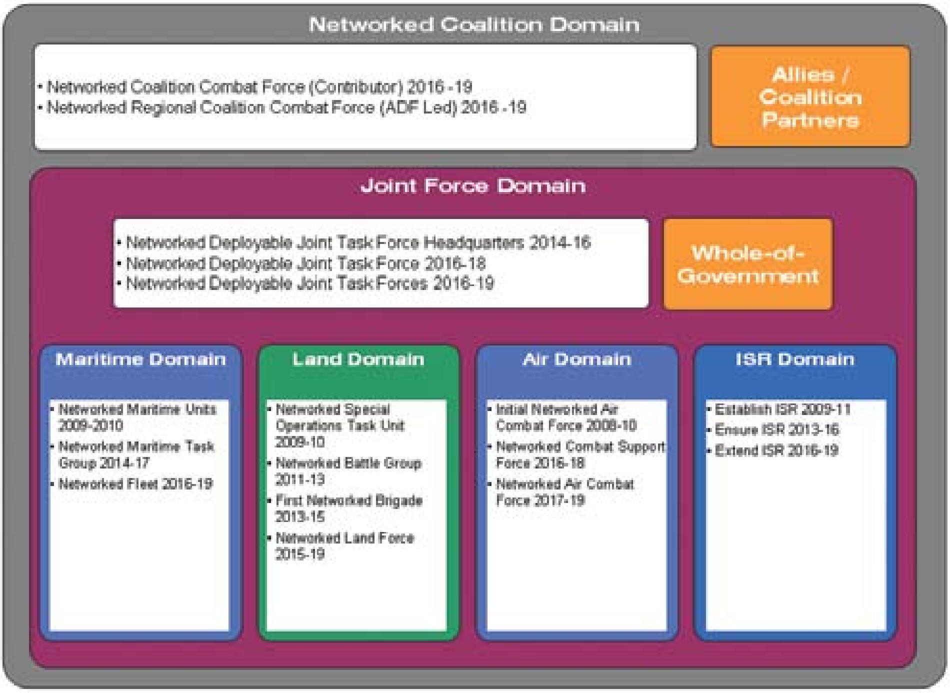

Networked Coalition Domain
• Networked Coalition Combat Force (Contributor) 2016 -19
• Networked Regional Coalition Combat Force (ADF Led) 2016 -19
Allies / Coalition Partners
Joint Force Domain
• Networked Deployable Joint Task Force Headquarters 2014-16
• Networked Deployable Joint Task Force 2016-18
• Networked Deployable Joint Task Forces 2016-19
Whole-of-Government
Maritime Domain
• Networked Maritime Units 2009-2010
• Networked Maritime Task Group 2014-17
• Networked Fleet 2016-19
Land Domain
• Networked Special Operations Task Unit 2009-10
• Networked Battle Group 2011-13
• First Networked Brigade 2013-15
• Networked Land Force 2015-19
Air Domain
• Initial Networked Air Combat Force 2008-10
• Networked Combat Support Force 2016-18
• Networked Air Combat Force 2017-19
ISR Domain
• Establish ISR 2009-11
• Ensure ISR 2013-16
• Extend ISR 2016-19

Figure 3-1: NCW milestones and the domain construct

3.2 Given the span and complexity of the capability systems that contribute to the NCW milestones, a slight variation to the formal target date definitions are required. Each milestone includes two target dates defined in this document as follows:

- **IOC** – achievement of an *initial operational capability*
  - when the delivery and effective integration of major contributing capabilities and exchange of information between them are complete
- **FOC** – achievement of the *final operational capability*
  - when the major contributing capabilities can securely and responsively exchange data, and support operational objectives and users across and between Defence information environment security domains; and all fundamental inputs to capability (FIC), including the human dimension aspects of NCW, have been achieved.

3.3 Because the building of the networked ADF is underpinned by the DCP 2009, the achievement of NCW milestones is based on the achievement of capability projects within the DCP. However, although many DCP projects contribute to the achievement of the milestones, only those that are primarily related to the development and delivery of critical communications and information network capabilities are considered 'essential'.

3.4 The NCW milestones allow Defence to monitor progress in building the networked ADF. Of the 18 milestones, the Initial Networked Air Combat Force milestone achieved an IOC in 2008. At the end of 2009, the Networked Maritime Units, Networked Special Operations Task Unit and Establish ISR milestones will be the next group to achieve IOC.

3.5 Descriptions of the NCW milestones within each of the domains and the mapping of the 'essential' DCP projects which contribute to their achievement are described below.

The maritime domain

3.6 Milestone 1 - Networked Maritime Units (IOC 2009 / FOC 2010):

- The Network Maritime Units milestone will deliver better information exchange capabilities, situational awareness and warfighting capability in the Navy's FFH/FFG platforms and amphibious ships.
- The Maritime Advanced SATCOM Terminal Information System (MASTIS) will provide, via satellite within a hub–spoke architecture, enhanced broadband connectivity between ships and between ship and shore. This will increase the ability of the networked units to exchange information and access the Defence Wide Area Communications Network through maritime gateways. The installation and integration of Link 16 TDL into FFG and FFH platforms will continue to improve situational awareness data.

3.7 Milestone 2 – Networked Maritime Task Group (IOC 2014 / FOC 2017):

- The Network Maritime Task Group will deliver an improved capability to autonomously exchange data between major fleet units operating in a localised area, increasing situational awareness and improving tactical warfare capability.
- This will be achieved by modernising communication systems, including the use of internet protocols for access to the Maritime Tactical Wide Area Network (MTWAN). The installation of Link 16 into FFH data communications will improve situational awareness.

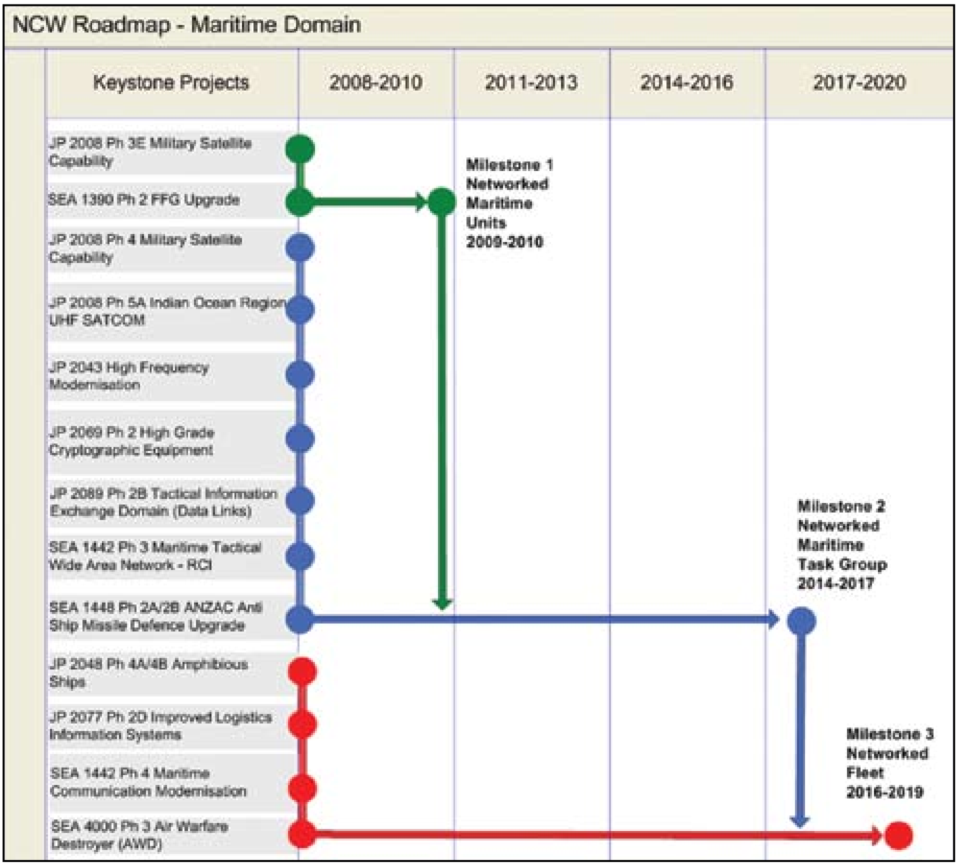

NCW Roadmap - Maritime Domain
Keystone Projects
2008-2010
2011-2013
2014-2016
2017-2020
JP 2008 Ph 3E Military Satellite Capability
SEA 1390 Ph 2 FFG Upgrade
JP 2008 Ph 4 Military Satellite Capability
JP 2008 Ph 5A Indian Ocean Region UHF SATCOM
JP 2043 High Frequency Modernisation
JP 2069 Ph 2 High Grade Cryptographic Equipment
JP 2089 Ph 2B Tactical Information Exchange Domain (Data Links)
SEA 1442 Ph 3 Maritime Tactical Wide Area Network - RCI
SEA 1448 Ph 2A/2B ANZAC Anti Ship Missile Defence Upgrade
JP 2048 Ph 4A/4B Amphibious Ships
JP 2077 Ph 2D Improved Logistics Information Systems
SEA 1442 Ph 4 Maritime Communication Modernisation
SEA 4000 Ph 3 Air Warfare Destroyer (AWD)
Milestone 1 Networked Maritime Units 2009-2010
Milestone 2 Networked Maritime Task Group 2014-2017
Milestone 3 Networked Fleet 2016-2019

Figure 3-2: DCP projects essential to maritime domain milestone achievements

3.8 Milestone 3 – Networked Fleet (IOC 2016 / FOC 2019):

- This Networked Fleet will deliver an enhanced capability to autonomously and seamlessly exchange data between geographically dispersed major fleet units, increasing situational awareness and improving tactical warfare capability.

- This will be achieved through modernised radio and communication management systems in current fleet units for improved ship-to-ship and ship-to/from-shore connectivity. The introduction of the LHDs, AWDs and advanced communication systems, such as 'Embarked TDL Network Management' and the Cooperative Engagement Capability, will also substantially increase the Navy's NCW-enabled warfighting capability.

3.9 Milestone 1 - Networked Special Operations Task Unit (IOC 2009 / FOC 2010):

- This Networked Special Operations Task Unit will deliver the Special Air Service Regiment (SASR) with the capability to deploy a vehicle-mounted task unit once the Special Operations Vehicle – Special Reconnaissance (SOV-SR) is delivered. This will improve communications interoperability within the task unit, between task units and with higher command.

3.10 Milestone 2 - Networked Battle Group (IOC 2011 / FOC 2013):

- The Networked Battle Group will deliver better communications and situational awareness within a battle group, from dismounted fire-team leaders through to a mounted battalion headquarters. The battle group will be based on a motorised infantry battalion organisation. It will also provide an element of combat identification for all dismounted and mounted elements of the battle group, based on shared situational awareness and a blue force tracking capability.
- Achieving the milestone requires development of a coherent battle management and communications infrastructure (blue force defined tactical picture).

3.11 Milestone 3 – First Networked Brigade (IOC 2013 / FOC 2015):

- The First Networked Brigade will deliver improved communications and situational awareness within a brigade, from dismounted fire-team leader through to brigade headquarters. It will provide an element of combat identification based on shared situational awareness and blue force tracking for all elements of the brigade.
- Achieving the milestone requires the development of a coherent battle management infrastructure, a robust federated C3 system, a mature fires network, and tactical ISR and logistic networks.

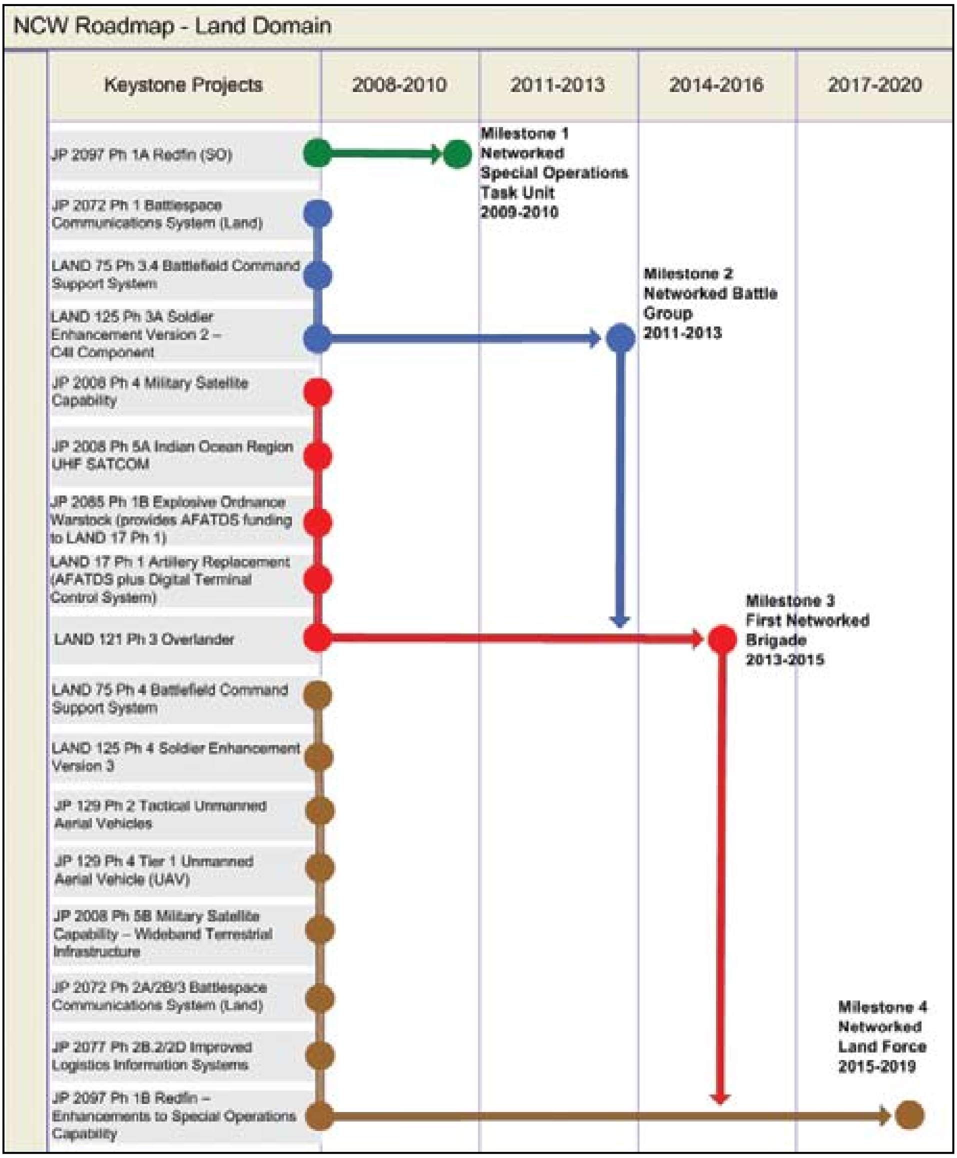

NCW Roadmap - Land Domain
Keystone Projects
2008-2010
2011-2013
2014-2016
2017-2020
JP 2097 Ph 1A Redfin (SO)
JP 2072 Ph 1 Battlespace Communications System (Land)
LAND 75 Ph 3.4 Battlefield Command Support System
LAND 125 Ph 3A Soldier Enhancement Version 2 – C4I Component
JP 2008 Ph 4 Military Satellite Capability
JP 2008 Ph 5A Indian Ocean Region UHF SATCOM
JP 2085 Ph 1B Explosive Ordnance Warstock (provides AFATDS funding to LAND 17 Ph 1)
LAND 17 Ph 1 Artillery Replacement (AFATDS plus Digital Terminal Control System)
LAND 121 Ph 3 Overlander
LAND 75 Ph 4 Battlefield Command Support System
LAND 125 Ph 4 Soldier Enhancement Version 3
JP 129 Ph 2 Tactical Unmanned Aerial Vehicles
JP 129 Ph 4 Tier 1 Unmanned Aerial Vehicle (UAV)
JP 2008 Ph 5B Military Satellite Capability – Wideband Terrestrial Infrastructure
JP 2072 Ph 2A/2B/3 Battlespace Communications System (Land)
JP 2077 Ph 2B.2/2D Improved Logistics Information Systems
JP 2097 Ph 1B Redfin – Enhancements to Special Operations Capability
Milestone 1 Networked Special Operations Task Unit 2009-2010
Milestone 2 Networked Battle Group 2011-2013
Milestone 3 First Networked Brigade 2013-2015
Milestone 4 Networked Land Force 2015-2019

Figure 3-3: DCP projects essential to land domain milestone achievements

3.12 Milestone 4 – Networked Land Force (IOC 2015 / FOC 2019):

- The Networked Land Force will deliver improved communications and situational awareness via a federated C3 system in remaining un-networked elements of high readiness brigades, from dismounted fire-team leader through to a land-deployable joint task force (JTF).

- The federated C3 system will be extended to joint force elements which are essential to provide the additional capability needed to sustain an enduring deployed brigade-sized JTF.
- The milestone will also include an enhanced ISR capability for the brigades, assigned land assets and at least one Special Operations Task Group (SOTG).
- A key effect will be to provide an element of combat identification based on shared situational awareness and blue force tracking for all elements of the brigade and force elements. The automated fires and logistic networks will be augmented by a mature ISR network across all brigade elements and assigned land assets. Interfaces to assigned joint assets will also be provided.

The air domain

3.13 Milestone 1 – Initial Networked Air Combat Force (IOC 2008 / FOC 2010):

- The Initial Networked Air Combat Force is delivering an initial Link 16 capability in the Mobile Regional Operations Centre, currently the Tactical Air Defence System under a rapid acquisition program, and to the F/A-18 A/B Hornets by AIR5376 Ph2.2 Hornet Upgrade.
- This milestone has provided enhanced situational awareness to the current fleet of F/A-18 aircraft. By replacing manual methods of passing a 'recognised air picture' to aircraft with more direct electronic transfer, the passage of more complete information can occur reducing radio traffic and the risk of misinterpretation.

3.14 Milestone 2 – Networked Combat Support Force (IOC 2016 / FOC 2018):

- The Networked Combat Support Force will deliver an improved ability to resource, support and protect ADF air bases.
- It will be achieved by enabling improved exchange of information between combat support elements, to provide networked C2, logistics and administration.

3.15 Milestone 3 – Networked Air Combat Force (IOC 2017 / FOC 2019):

- The Networked Air Combat Force will deliver better situational awareness and system integration to new and existing air combat elements and other ADF air platforms and assets through a comprehensive air and surface BMS. It will also deliver a reliable and trusted air picture to air, land and sea platforms, enhanced C2, and networked and integrated weapon systems.
- This milestone will realise linked surveillance systems (such as Mobile Regional Operations Centre (AIR 5405), air traffic control and AEW&C sensors) through a variety of data links to C2 and data fusion systems, and the linking of those (via Link 16) to ADF weapons systems, such as the Joint Strike Fighter (JSF), F/A-18F, AWD and joint stand off weapon (JSOW).

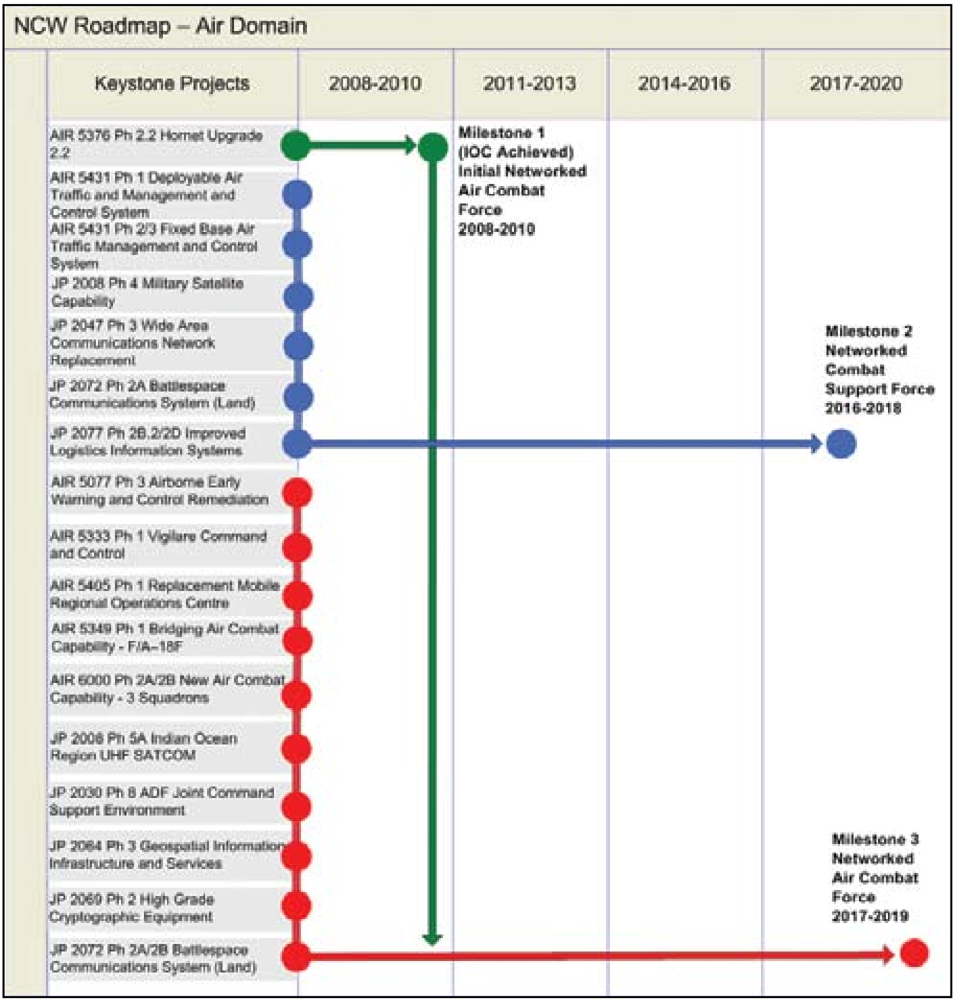

NCW Roadmap – Air Domain
Keystone Projects
2008-2010
2011-2013
2014-2016
2017-2020
AIR 5376 Ph 2.2 Hornet Upgrade 2.2
AIR 5431 Ph 1 Deployable Air Traffic and Management and Control System
AIR 5431 Ph 2/3 Fixed Base Air Traffic Management and Control System
JP 2008 Ph 4 Military Satellite Capability
JP 2047 Ph 3 Wide Area Communications Network Replacement
JP 2072 Ph 2A Battlespace Communications System (Land)
JP 2077 Ph 2B.2/2D Improved Logistics Information Systems
AIR 5077 Ph 3 Airborne Early Warning and Control Remediation
AIR 5333 Ph 1 Vigilare Command and Control
AIR 5405 Ph 1 Replacement Mobile Regional Operations Centre
AIR 5349 Ph 1 Bridging Air Combat Capability - F/A-18F
AIR 6000 Ph 2A/2B New Air Combat Capability - 3 Squadrons
JP 2008 Ph 5A Indian Ocean Region UHF SATCOM
JP 2030 Ph 8 ADF Joint Command Support Environment
JP 2064 Ph 3 Geospatial Information Infrastructure and Services
JP 2069 Ph 2 High Grade Cryptographic Equipment
JP 2072 Ph 2A/2B Battlespace Communications System (Land)
Milestone 1 (IOC Achieved) Initial Networked Air Combat Force 2008-2010
Milestone 2 Networked Combat Support Force 2016-2018
Milestone 3 Networked Air Combat Force 2017-2019

Figure 3-4: DCP projects essential to air domain milestone achievements

The ISR domain

3.16 Milestone 1 – Establish ISR (IOC 2009 / FOC 2011):

- The Establish ISR milestone will deliver improved use of existing ISR resources and give HQJOC the necessary ISR communication infrastructure and ISR systems to support sophisticated joint operations. This capability will also improve the coordination of interagency and coalition activities.

- The milestone will include the timely delivery of raw and aggregated situational awareness feeds from Defence and allied sources; better visibility and presentation of situational awareness information; greater accessibility to existing data collection assets; and an increased capability to exchange ISR information with allies, coalition partners and other government agencies.
- Achieving the milestone requires the introduction of appropriate CONOPS, policy, compliance and ISR governance; the development of communication infrastructure and networking applications, particularly those that support the effective operation of HQJOC; the improvement of mechanisms for the visualisation of ISR information; and the optimisation of ISR data delivery.

3.17 Milestone 2 – Ensure ISR (IOC 2013 / FOC 2016):

- The Ensure ISR milestone will deliver improved access to current and new sources of ISR data by investing in techniques and technologies that will develop a single, integrated, federated and distributed ISR information-sharing capability that links relevant Defence platforms, tactical units, operational headquarters and strategic agencies.
- The milestone will improve the transmission of ISR data to and between ISR assets and ADF tactical units, better present situational awareness information, and make available ISR data more accessible to Defence systems, commanders and other users.
- Achieving the milestone depends on the introduction of a range of collection assets and coordinated tasking processes, communication systems, and networked data repositories with searchable metadata indexes and management systems, including smart-push and user-pull tools for delivery of ISR data to integrate ISR collection and distribution. These will be underpinned by the establishment of universal data standards and protocols.

3.18 Milestone 3 - Extend ISR (IOC 2016 / FOC 2019):

- This Extend ISR milestone will deliver information connectivity and support through the continuous linking of force elements, sensors and decision-makers to increase situational awareness and enable decisive action.
- Effects include a greater ability to exchange ISR information and conduct combined ISR operations; further improvements to the delivery of sensor information; intelligence and other surveillance data that is more accessible to users at the tactical, operational and strategic levels.
- The milestone will be achieved through the introduction of additional responsive, persistent and networked ISR collection assets, which will provide some access to global ISR data.

- Achieving the milestone requires the development of information architectures robust enough to ensure continuous availability under demanding conditions; the establishment of controlled interfaces between fixed and deployed domains, and between Australian and allied intelligence domains; horizontal and vertical integration of ISR information in joint and combined operations; and the introduction of technologies that will improve the coordination of ISR-sourced information, collection and tasking.

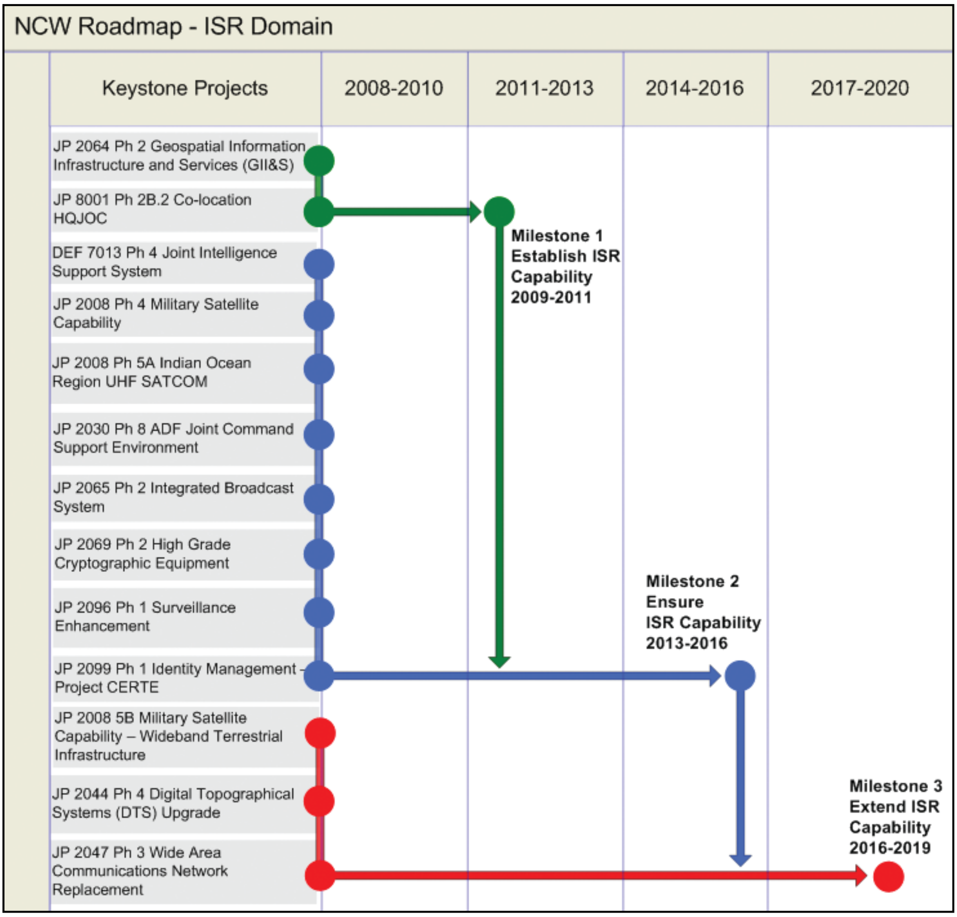

NCW Roadmap - ISR Domain
Keystone Projects
2008-2010
2011-2013
2014-2016
2017-2020
JP 2064 Ph 2 Geospatial Information Infrastructure and Services (GII&S)
JP 8001 Ph 2B.2 Co-location HQJOC
DEF 7013 Ph 4 Joint Intelligence Support System
JP 2008 Ph 4 Military Satellite Capability
JP 2008 Ph 5A Indian Ocean Region UHF SATCOM
JP 2030 Ph 8 ADF Joint Command Support Environment
JP 2065 Ph 2 Integrated Broadcast System
JP 2069 Ph 2 High Grade Cryptographic Equipment
JP 2096 Ph 1 Surveillance Enhancement
JP 2099 Ph 1 Identity Management Project CERTE
JP 2008 5B Military Satellite Capability – Wideband Terrestrial Infrastructure
JP 2044 Ph 4 Digital Topographical Systems (DTS) Upgrade
JP 2047 Ph 3 Wide Area Communications Network Replacement
Milestone 1 Establish ISR Capability 2009-2011
Milestone 2 Ensure ISR Capability 2013-2016
Milestone 3 Extend ISR Capability 2016-2019

Figure 3-5: DCP projects essential to ISR domain milestone achievements

The joint domain

3.19 Milestone 1 - Networked Deployable Joint Task Force Headquarters (IOC 2014 / FOC 2016):

- The Networked Deployable Joint Task Force Headquarters (DJTFHQ) milestone will enable the ADF to effectively command and control a deployed force consisting of two or more ADF service groups. The networked DJTFHQ will be on land or afloat.
- The DJTFHQ will deliver:
  - robust and integrated command, logistics and intelligence systems, operating between strategic and operational levels of command, with timely availability of information
  - an integrated command support system operating between the environmental components within the DJTFHQ
  - readily established and scalable connectivity between strategic level and operational HQs that can be made available globally within the readiness notice of the JTFHQ
  - situational awareness through the area of operations COP, primarily through enhanced TDL.
- Achieving the milestone requires the development of capabilities, communication infrastructure and networking applications that support the networked DJTFHQ.

3.20 Milestone 2 - Networked Deployable Joint Task Force (IOC 2016 / FOC 2018):

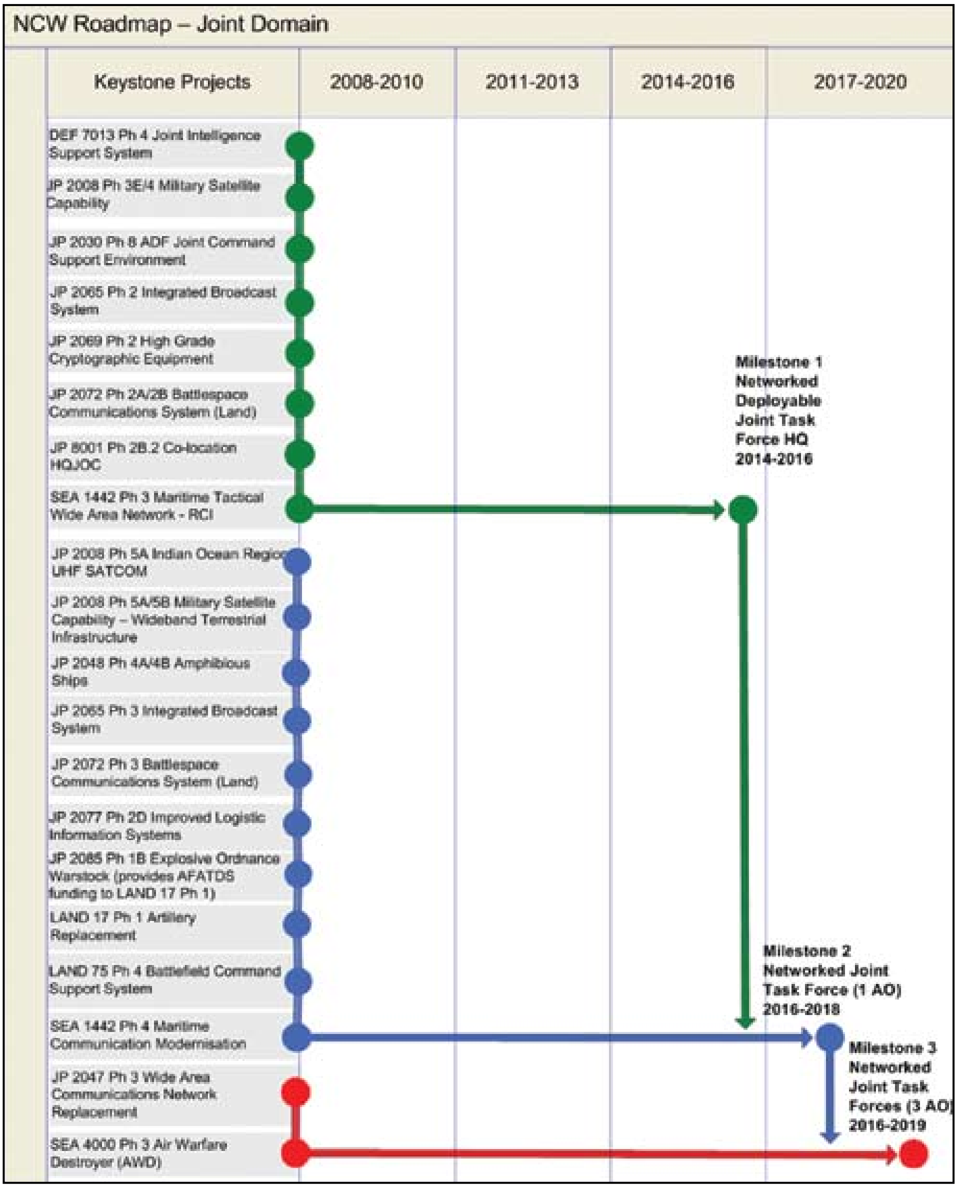
- The Networked deployable Joint Task Force will enable the ADF to better deploy a land force up to battalion group, operating with the support of air and / or maritime assets in one area of operations.
- The milestone will deliver:
  - robust and integrated command, logistics, intelligence, personnel and health systems between operational and tactical levels of command and service domains with timely availability of information
  - access to appropriate information, including ISR (in both directions) and situational awareness (through blue force tracking, combat identification, and adversary position information) in order to plan and conduct joint effects
  - robust and scalable connectivity between operational HQ and tactical elements across the environmental domains
  - enhanced, distributed, collaborative, deliberate and immediate planning functions

  - network services that can be managed and monitored by the theatre commander to meet task force requirements, such as multi-TDLs using a joint interface control officer
  - seamless transfer of data at the tactical level to facilitate coordinated effects, such as joint fires

- Achieving this milestone requires the development of capabilities, communication infrastructure and networking applications that support the Networked Deployable Joint Task Force.

3.21 Milestone 3 - Networked Deployable Joint Task Forces (IOC 2016 / FOC 2019):

- The Networked Deployable Joint Task Forces milestone extends capacity from one area of operations to three concurrent areas of operations.
- The milestone will enable the deployment of both a battalion group and a brigade group for a prolonged period and establish and maintain sea control and air superiority at key locations in the ADF's primary operational environment.
- The principal additional deliverables provided by this milestone are:
  - operational networks that are scalable and sustainable for the duration of the deployment
  - assured information availability in the most demanding environments, including a network attack by an adversary
  - the ability for network services to be reallocated by the theatre commander to meet emerging requirements
  - 'quality of service' metrics that are a parameter of deployed network operations
  - information sharing arrangements between Defence and key government agencies, including immediate planning interfaces
  - networks which can readily integrate other government agencies, to improve planning and direction, reduce the human and logistical size of deployments and match support to operational requirements.
- Achieving this milestone requires the development of capabilities, communication infrastructure and networking applications that support the Networked Deployable Joint Task Force (milestone two), but with tiered levels of network management and planning.



NCW Roadmap – Joint Domain

Keystone Projects	2008-2010	2011-2013	2014-2016	2017-2020

DEF 7013 Ph 4 Joint Intelligence Support System

JP 2008 Ph 3E/4 Military Satellite Capability

JP 2030 Ph 8 ADF Joint Command Support Environment

JP 2065 Ph 2 Integrated Broadcast System

JP 2069 Ph 2 High Grade Cryptographic Equipment

JP 2072 Ph 2A/2B Battlespace Communications System (Land)

JP 8001 Ph 2B.2 Co-location HQJOC

SEA 1442 Ph 3 Maritime Tactical Wide Area Network - RCI

JP 2008 Ph 5A Indian Ocean Region UHF SATCOM

JP 2008 Ph 5A/5B Military Satellite Capability – Wideband Terrestrial Infrastructure

JP 2048 Ph 4A/4B Amphibious Ships

JP 2065 Ph 3 Integrated Broadcast System

JP 2072 Ph 3 Battlespace Communications System (Land)

JP 2077 Ph 2D Improved Logistic Information Systems

JP 2085 Ph 1B Explosive Ordnance Warstock (provides AFATDS funding to LAND 17 Ph 1)

LAND 17 Ph 1 Artillery Replacement

LAND 75 Ph 4 Battlefield Command Support System

SEA 1442 Ph 4 Maritime Communication Modernisation

JP 2047 Ph 3 Wide Area Communications Network Replacement

SEA 4000 Ph 3 Air Warfare Destroyer (AWD)

Milestone 1
Networked Deployable Joint Task Force HQ
2014-2016

Milestone 2
Networked Joint Task Force (1 AO)
2016-2018

Milestone 3
Networked Joint Task Forces (3 AO)
2016-2019

Figure 3-6: DCP projects essential to joint domain milestone achievements

The coalition domain

3.22 Milestone 1 – Networked Coalition Combat Force (Contributor) (IOC 2016 / FOC 2019):

- The Networked Coalition Combat Force (Contributor) will enable the ADF to make tailored contributions to military forces led by selected allies or coalition partners, with minimal support from the lead nation.

- The result of this work will be ADF systems that interoperate effectively at the operational level with the command support systems, such as the Cooperative Engagement Capability and the Global Information Grid, used by a networked coalition combat force, enabling coalition joint effects and contributing to coalition situational awareness.

- Achieving the milestone requires capabilities, agreements, procedures, communication infrastructure and networking applications that support ADF element participation within a networked coalition combat force led by another country.

- In particular, this means:

  - establishing authenticated trust relationships within the coalition

  - the designation and use of agreed information, data, cryptographic and protocol standards

  - the use of standardised and integrated planning functions

3.23 Milestone 2 – Networked Regional Coalition Combat Force (ADF Led) (IOC 2016 / FOC 2019):

- The Networked Regional Coalition Combat Force will provide the coalition information environment (including infrastructure and equipment), enable situational awareness through the use of collaborative systems to lead and manage the production of a coalition COP, enable security (including tiered releasability), and give coalition partners access to adequate operational information and tiered services.

- Achieving the milestone requires the development of capabilities, agreements, procedures, communication infrastructure and networking applications that support a networked regional coalition combat force (ADF led).

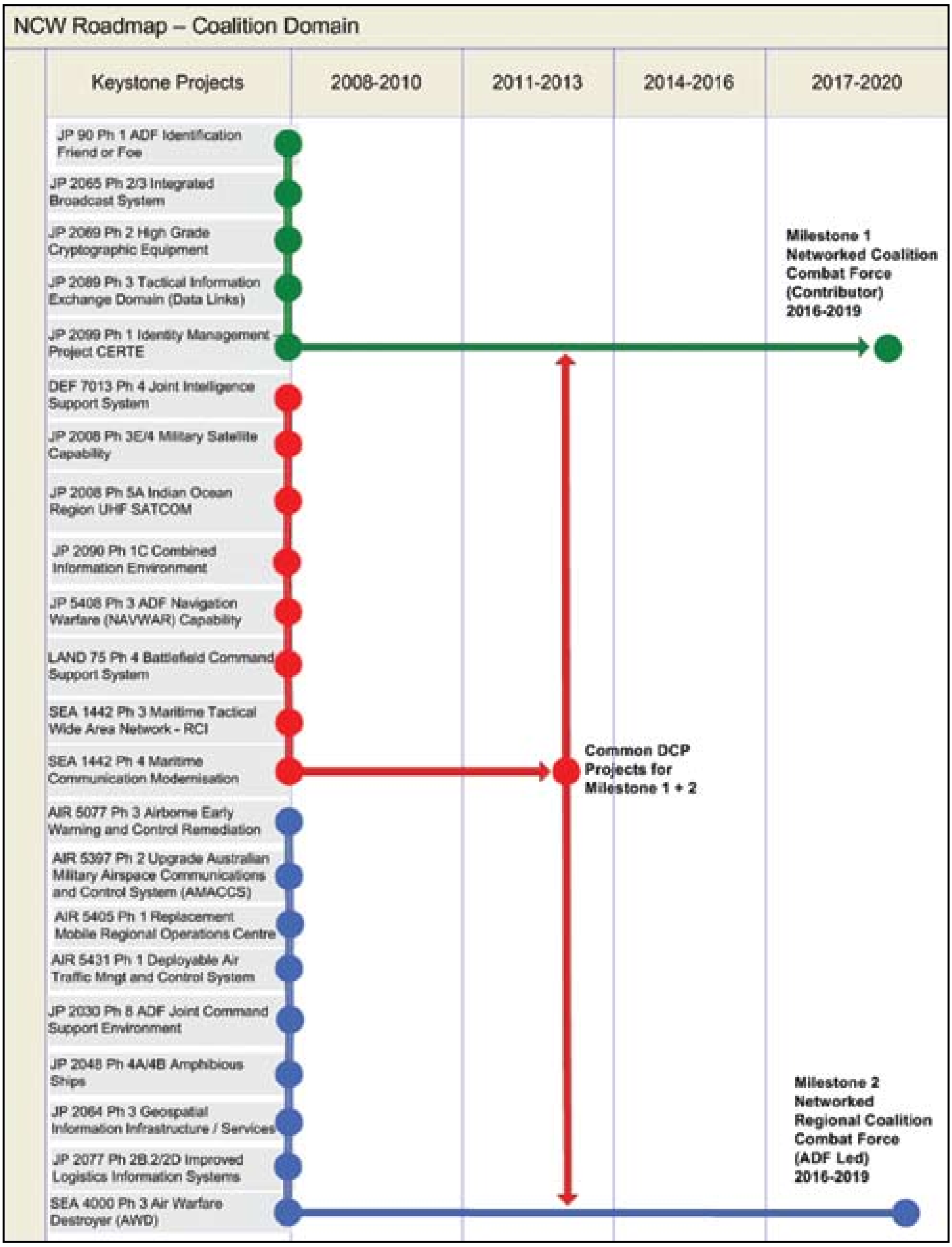
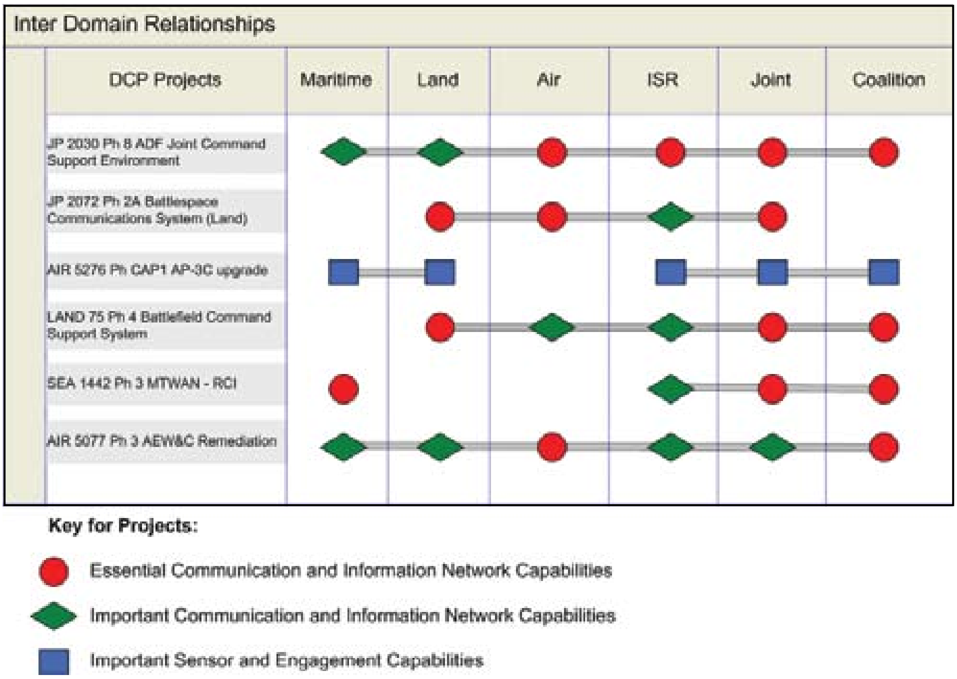

NCW Roadmap – Coalition Domain
Keystone Projects
2008-2010
2011-2013
2014-2016
2017-2020
JP 90 Ph 1 ADF Identification Friend or Foe
JP 2065 Ph 2/3 Integrated Broadcast System
JP 2069 Ph 2 High Grade Cryptographic Equipment
JP 2089 Ph 3 Tactical Information Exchange Domain (Data Links)
JP 2099 Ph 1 Identity Management Project CERTE
DEF 7013 Ph 4 Joint Intelligence Support System
JP 2008 Ph 3E/4 Military Satellite Capability
JP 2008 Ph 5A Indian Ocean Region UHF SATCOM
JP 2090 Ph 1C Combined Information Environment
JP 5408 Ph 3 ADF Navigation Warfare (NAVWAR) Capability
LAND 75 Ph 4 Battlefield Command Support System
SEA 1442 Ph 3 Maritime Tactical Wide Area Network - RCI
SEA 1442 Ph 4 Maritime Communication Modernisation
AIR 5077 Ph 3 Airborne Early Warning and Control Remediation
AIR 5397 Ph 2 Upgrade Australian Military Airspace Communications and Control System (AMACCS)
AIR 5405 Ph 1 Replacement Mobile Regional Operations Centre
AIR 5431 Ph 1 Deployable Air Traffic Mngt and Control System
JP 2030 Ph 8 ADF Joint Command Support Environment
JP 2048 Ph 4A/4B Amphibious Ships
JP 2064 Ph 3 Geospatial Information Infrastructure / Services
JP 2077 Ph 2B.2/2D Improved Logistics Information Systems
SEA 4000 Ph 3 Air Warfare Destroyer (AWD)
Milestone 1 Networked Coalition Combat Force (Contributor) 2016-2019
Common DCP Projects for Milestone 1 + 2
Milestone 2 Networked Regional Coalition Combat Force (ADF Led) 2016-2019

Figure 3-7: DCP projects essential to coalition domain milestone achievements

Inter-domain relationships

3.24 NCW domains and milestones are not developed in isolation. Many DCP projects contribute in essential or important ways to more than one domain. Figure 3-8 provides examples of projects that contribute to multiple NCW domain milestones.



Inter Domain Relationships

DCP Projects	Maritime	Land	Air	ISR	Joint	Coalition
JP 2030 Ph 8 ADF Joint Command Support Environment	◆	◆	●	●	●	●
JP 2072 Ph 2A Battlespace Communications System (Land)		●	●	◆	●	
AIR 5276 Ph CAP1 AP-3C upgrade	■	■		■	■	■
LAND 75 Ph 4 Battlefield Command Support System		●	◆	◆	●	●
SEA 1442 Ph 3 MTWAN - RCI	●			◆	●	●
AIR 5077 Ph 3 AEW&C Remediation	◆	◆	●	◆	◆	●

Key for Projects:

● Essential Communication and Information Network Capabilities

◆ Important Communication and Information Network Capabilities

■ Important Sensor and Engagement Capabilities

Figure 3-8: Selected inter domain relationships

Operational test and evaluation of NCW milestones

3.25 Operational test and evaluation (OT&E) determines the operational effectiveness of capability systems and their suitability to carry out their expected role and fulfil the requirements of the milestone.

3.26 OT&E of NCW milestones will be conducted under realistic operational conditions through single-service exercises and the Program of Major Service Activities.

3.27 OT&E criteria, which will be detailed in the NCWIIS, have been developed for each of the NCW milestones. The criteria include critical operating issues, measures of effectiveness and measures of suitability.

3.28 Examples of critical operating issues for the NCW milestones include:

- Does the capability enhance situational awareness and decision-making?
- Does the capability enhance the ability to plan, conduct and support operations?
- Does the capability improve human interaction and understanding?
- Does the capability have the ability to operate under demanding operational conditions and threats?
- Does the capability have sufficient interoperability to operate effectively with allies and other agencies within the limitations of information exchange agreements?
- Does the capability exchange data in a seamless, accurate, secure and timely manner?
- Does the capability have the agility to adapt to technological and operational changes and innovations?

3.29 Prior to first and second pass, projects contributing to NCW milestones are required to incorporate NCW milestone OT&E criteria and develop their own measures of performance in meeting those criteria.

Operational vignette for 2020 Networked Force

An Amphibious Task Group with a Battle Group embarked in a CANBERRA Class LHD sails for an area of operations in Australia's Primary Operational Environment. During the transit, distributed collaborative planning is undertaken by the Commander Amphibious Task Force (CATF) in response to the rapidly changing situation enabled by the Joint Command Support System delivered by JP 2030, Coalition Command and Support Systems delivered by JP 2090 and the broader ADF information environment. During the transit, layered, networked and integrated protection against multiple air, surface and under sea threats is facilitated through linked communications between assigned forces[6], using the Tactical Information Environment delivered by JP2089 to achieve an optimised and synchronised sensor to shooter networked defence. A Combat Team Commander (as part of the Battle Group) embarked in the LHD, is given his orders to proceed ashore by landing craft. In preparation, he accesses National and Coalition networks provided by JP 2030 and JP 2090 to gain situational awareness and plan for his mission. His Battle Group Commander remains sea based in the LHD with its extensive and modern C2 capability.[7]

Proceeding ashore, the Combat Team Commander exchanges messaging and location data with the other land component, joint and coalition force elements using his Battle Management System delivered by LAND 75 and voice and data communication systems delivered by JP 2072. Army's fleet of combat vehicles provides the Combat Team Commander with not only mobility and protection but, importantly, extends the range of his communications and provides him with the necessary situational awareness as he manoeuvres to his objective. The Combat Team Commander is able to exchange secure information with maritime and air platforms operating in his area to synchronise activities[8]. Moving further from his headquarters, he is able to utilise MILSATCOM delivered by JP 2008 to maintain communications beyond line of sight.

[6] Air Warfare Destroyer (SEA4000) incorporating the AEGIS Combat System for Area Air Defence, enhanced ANZAC Frigate (SEA 1448), Maritime Patrol Aircraft (AIR 7000), New Air Combat Capability (AIR 6000) and Airborne Early Warning and Control Aircraft (AIR5077).

[7] Such as the systems delivered through JP 2048 Amphibious Ships, LAND 75 Battle Management System, JP 2072 Battlespace Communications Systems, JP 2030 Joint Command Support System, JP 2008 Military Satellite Capability, et al.

[8] Through JP 2069 High Grade Cryptographic Equipment, JP 2072, SEA 1442 Maritime Communications Modernisation and JP2089 Tactical Information Exchange Data Links et al.

During his mission, the Combat Team Commander is provided ISR information from tactical unmanned aerial vehicles delivered by JP129 and manned ISR aircraft delivered by AIR 7000 through either a direct tactical common data link or the Battle Management System. This ISR information can be passed to a Processing, Exploitation and Dissemination facility provided by AIR 7000 and other projects for further analysis and fused into the COP to contribute to situational awareness. In order to neutralise threats, the Combat Team Commander request's joint fires support through the Advanced Field Artillery Tactical Data System delivered by LAND 17 and controlled by Joint Terminal Attack Controllers utilising Variable Message Format links. The joint fires can be provided by Naval Gunfire Support, Artillery, and Close Air Support [9]. The logistic support requirements of the Combat Team Commander and the Task Force are met by a networked logistics capability delivered by JP 2077 which ensures the precise and timely delivery of logistics support.

Information collected during the mission is rapidly available to strategic organisations. The Task Force is provided with an enhanced range of networked broadband capabilities to facilitate operational command and control and access strategic services through delivery of JP 2047, the Defence Wide Area Communications Network. The Command Support Systems delivered by JP 2030 and JP2090, enterprise systems managed by CIOG and information provided by JP 2065, the Integrated Broadcast System, are extended into the deployed environment utilising a secure information network, delivered by JP 2069, JP 2072 and SEA 1442 over multiple communication paths and systems.

[9] Such as ANZAC Frigate (SEA 1448), Artillery Replacement, (LAND 17) and AIR 6000.

Beyond 2020 Networked Force - Force 2030

3.30 DCP 2009 provides an account of major capital equipment proposals that are currently planned for government consideration (either first or second pass) in the period from 2009 to 2013. However, the 2009 Defence White Paper outlines a number of 'emerging capabilities' beyond that period, which need to be considered as part of the ongoing development of Force 2030:

- **The maritime domain** – The Government has decided to acquire 12 new Future Submarines, capable of tasks including strategic strike, gathering battlespace data to support operations, and intelligence collection. The Government has also decided to acquire eight new Future Frigates, with a strong emphasis on submarine detection and response operations. The Future Frigates will be equipped with an integrated sonar suite that includes a long-range, active, towed-array sonar, and will be able to embark a combination of naval combat helicopters and maritime uninhabited aerial vehicles. Defence will also develop proposals to rationalise the Navy's patrol boat, mine countermeasures, hydrographic and oceanographic forces into a single, modular, multi role class of vessel. This concept relies on the use of modular unmanned underwater systems for the mine countermeasures and hydrographic tasks.
- **The land domain** – Defence intends to acquire a fleet of 1,100 deployable protected vehicles, including enhanced communications, networking and BMSs, along with new friendly-force identification systems, in response to the Government's high priority on the survivability and mobility of land forces.
- **The air domain** – The Government has stated that a fourth JSF squadron will be introduced into service to replace the Super Hornet aircraft. The JSF's combination of stealth, advanced sensors, networking and data fusion capabilities, when integrated into the networked ADF, will ensure that Australia maintains its strategic capability out to 2030.
- **The ISR domain** – The Government has decided to improve Australia's intelligence collection capabilities by acquiring a satellite with remote sensing capabilities, most likely based on a high-resolution, cloud-penetrating, synthetic aperture radar. Maritime surveillance and response will also be improved through the acquisition of eight new maritime patrol aircraft to replace the AP-3C Orion fleet. Seven large high-altitude, long-endurance UAVs will supplement the manned maritime patrol aircraft. Strategic UAVs will provide persistent ISR, enhancing situational awareness in the land and maritime domains.
- **The joint force domain** – A joint approach will bind single-service capabilities and systems into an operationally seamless whole. The ADF will continue to enhance the joint command support system, as well as protected high-speed communication systems and associated networking capabilities. This will enable a fully integrated command support system to cover all levels of operations and all environments, allowing participation with coalition operations and collaboration with other agencies. The ADF has placed a priority on space situational awareness, and Defence is required to explore how to strengthen space situational awareness and mission assurance.

- **The networked coalition domain** – Defence will continue to develop interoperable capabilities where it is cost effective to do so and supports our alliances and international relationships. The US alliance will remain the most important Defence relationship, and will continue to provide significant access to materiel, intelligence, communication systems, skills and expertise, substantially strengthening ADF capability.

Action 2 - Establishing the integrated network

> *Defence must move towards a single operating environment supported by a high speed broadband IP network and a uniform applications suite to sustain a single common operating picture…Defence's efforts in this direction will be sustained by Defence's new ICT Strategy and ICT Architecture which will include a single Enterprise Architecture…*
>
> Head ICT Operations / Strategic J6, IDLS Conference, November 2008

Requirements

3.31 The establishment of the network, and the integration and exchange of information across it, are fundamental to the development and implementation of NCW within the ADF. In the simplest sense, the network will consist of a collection of nodes that are linked to each other to allow the interconnection of users (or systems), the sharing of resources, access to information and the integration of information (or data) and processes (or applications).

3.32 Underlying this simplistic description is the reality that the network will be required to connect a vast and diverse array of joint, interagency and coalition systems, all of which will be required to operate seamlessly across all environmental domains and over an equally diverse array of communication means and linkages. A range of enterprise-level common services, including governance and compliance mechanisms, will also be needed to support information integration and exchange within and between those domains and with allies, coalition partners and other government agencies operating outside the Defence information environment.

3.33 The network will also be required to pass various forms of information and data at various transmission rates and security levels. The information will then be processed through a combination of machine and human interfaces. In addition to meeting these operational requirements, the network must also meet high requirements for security, robustness, capacity, congestion management and topology.

3.34 **The radio frequency (RF) spectrum** – The RF spectrum is a finite resource. In Australia, it is both a national and a Defence asset, and demand for access to it is growing due to the proliferation of new devices, services and, in Defence's case, military threats. Balancing Defence's requirements with commercial and civil demand is therefore a growing issue that requires close management and a long-term perspective. The Australian Defence Spectrum Strategic Plan describes the strategy for providing and maintaining access to the RF spectrum, and is sponsored and managed by the Chief Information Officer Group on behalf of Defence.

3.35 **Protecting the network** – Along with the requirement to establish the network is the requirement to protect it. In the past decade, the growing importance of operations in cyberspace has become apparent, along with the growing potential for cyber attacks, particularly given the increasing reliance on networked operations. Defence's current approach to network protection reflects the wider civil and military organisational approach to security, in which systems are protected by both physical means (e.g. restricted access environments) and non-physical measures (e.g. firewalls). Integral to the future protection of the network is the requirement for security architecture as part of Defence-wide enterprise architecture. As stated in the 2009 Defence White Paper, the Government has decided to meet that requirement by investing in an enhanced cyber situational awareness and response capability, which includes a Cyber Security Operations Centre within the Defence Signals Directorate (DSD).

Current status

3.36 Defence has continued to evolve its strategic, operational and tactical networks to sustain the conduct of operations and management of its business. Currently, the core of the strategic communications network that links major Defence sites provides an effective capability to support current operations.

3.37 The Chief Information Officer Group has also established important networking capabilities, primarily in the satellite communications area, to sustain vital operational and tactical links across each of the operational theatres where Australian forces are currently deployed. However, additional effort is needed to improve information assurance practices and to adopt more comprehensive information management policies and practices.

The way forward

3.38 The Chief Information Officer Group is committed to an ICT strategy that will continue to provide the infrastructure and supporting information capabilities that the ADF needs. In conjunction with the Defence ICT reform program, the group will deliver a secure and robust ICT capability that supports both warfighting and business requirements to Defence by 2012.

3.39 The Defence information environment will also provide an integrated network, connecting fixed and deployed locations, built on a single set of standards and approved products encompassing all security levels and the ability to determine that the right person has the right authority to access all required information and services.

3.40 The ICT strategy includes developing and supporting the enterprise-level common services (services-orientated architecture) needed for the newer information technologies embedded in most NCW-related DCP projects. This enterprise approach improves the assurance, availability and integrity of those services, allowing the projects to focus on their own specific requirements within the common infrastructure.

3.41 Secure voice and video will be available to the desktop in most fixed and deployed locations. Deployed commanders and strategic decision-makers will have a single view of the battlespace through a single COP, accessing a wide range of data from various sensors and sources.

3.42 Logistic ICT systems will be able to support improvements in warehousing, supply chain management and stocktaking, to best meet operational needs. Tactical data networks will provide integrated and timely access to essential sensor and engagement information needed by commanders and war fighters in their respective battlespaces.

Action 3 - Developing the human dimension

> *The network is an enabler to warfighting effectiveness; it supplements but cannot replace the skill, intuition and willpower of the ADF's people. The focus on training, doctrine, leadership and organisation will balance the technical aspects that often dominate discussion of NCW.*
>
> Enabling future warfighting: Network Centric Warfare, February 2004

Requirements

3.43 NCW has a human dimension because warfighting is essentially a human activity. The human dimension of NCW identifies the importance of the human element in warfighting and places human decision-making and battle direction at the heart of weapons and systems. The quality and performance of people are the key drivers of warfighting success, aided by weapons, systems and networks. The foundation of human performance is character, and the pillars of performance are education, training, values, culture, weapons, networks and systems.

3.44 Successful matching of the human and network dimensions requires:

- **A capacity for organisational learning, innovation and adaptation** – NCW requires an environment in which the Defence organisation is willing and able to learn, innovate and adapt its structures, doctrine and practices, based on research evidence and the lessons of experience.
- **Leadership** – NCW presents significant challenges to the organisations, traditions and culture of senior and junior commanders. It requires the development of the locus of decision-making, independence, empowerment and confidence in decision-makers of all levels, and the requisite intelligence and skills for continual self-synchronisation.
- **Individual skills and knowledge** – Our people at all levels need the skills and knowledge to manage and exploit information and to network and collaborate effectively within and across the services. The skills required include generic networking, information management and information exploitation skills, as well as skills that are specific to operational systems and processes.
- **Collective capability** – NCW is essentially a collective activity. There is a greater need to develop the collective warfighting capability of our people through joint, integrated and single-service collective training and increased use of larger scale simulation.
- **A culture of collaboration** – Networking requires the development of a culture that values the need to share knowledge and collaborate, based on trust and reinforced through leadership, education and training.
- **Systems matched to people** – Technical systems and organisational structures need to be designed to take account of human cognitive, social and physical characteristics. Conversely, the Defence workforce will need to be adapted to the networked environment in numbers, composition, aptitudes, organisation and disposition. This will be achieved through existing systems for capability development, workforce planning, recruiting, career management, doctrine, training and human systems research, which may need to be strengthened to meet those requirements fully in the future.
- **Doctrine** – The doctrine for future joint operations will be developed to incorporate the NCW concept, which has potential applications across most aspects of the FJOC. Key areas of focus will include:
    - provision of C2 (including aspects such as situational awareness, decision-making and self-synchronisation) to the networked force
    - integration and delivery of effects by the networked force
    - coordinated collection, processing, dissemination and visualisation of information and intelligence across networks.

Current status

3.45 As technical aspects of the network dimension become more sophisticated, a greater emphasis on matching the human with the NCW environment is needed. A number of initiatives to achieve this have commenced in the ADF, including:

- the Joint Combined Training Capability
- the New Generation Navy
- the Adaptive Army
- the Air Force Adaptive Culture Program.

The way forward

3.46 The main change driver will be the education and training system for current and future leaders, where particular emphasis will be given to the skills needed for them to drive the necessary changes at all levels.

3.47 Knowledge derived from operations, exercises, experimentation and research will continuously inform joint doctrine, education and training. Established systems for workforce planning, capability development, human factors research, recruitment, career management, performance management, education and training policy, and doctrine development will continue to be refined to meet NCW requirements. They will remain the principal vehicles for matching people, organisations and technical systems.

3.48 All aspects of NCW, including the human dimension, will need to be informed by valid human systems research and knowledge. Defence will continue service-sponsored and joint research and experimentation, and to learn from operations and exercises. The Defence Science and Technology Organisation (DSTO) will also conduct research, in accordance with current tasking processes, and provide access to research to meet joint and service knowledge requirements. Research will include the use of the Program of Major Service Activities to explore and test human dimension issues and concepts. Simulation will play a key role in supporting concept development, research and training for future networked operations.

3.49 The human dimension of NCW will benefit from a realistic, operationally focused training environment that brings together the elements of the ADF and coalition capability that would be expected to work together in operations. The ADF will use the Joint Combined Training Capability and the Joint Integrated Simulation Project to achieve an environment that integrates live, virtual and constructive entities for focused operational training.

3.50 Human systems integration will be required to integrate functional areas (human factors engineering, crewing, personnel, training, systems safety, health hazards and survivability) into the design, development, procurement and ongoing support of NCW systems, to ensure safe and effective operability and supportability.

Action 4 - Accelerating the process of change and innovation

> *A continued focus on the exploitation and application of new advanced technologies will be crucial in ensuring that the ADF has access to highly advanced and networked capabilities, and has a winning edge in terms of information superiority.*
>
> Minister for Defence Science and Personnel, 2009 Defence White Paper Media Release, 2 May 2009

The Rapid Prototyping, Development and Evaluation Program

3.51 The Rapid Prototyping, Development and Evaluation (RPDE) program is a significant Capability Development Group (CDG) initiative that accelerates the introduction of network centric environment solutions into the ADF. The RPDE mission statement has matured to reflect the ADF's priority of enhancing its warfighting capability in the broader context of networking to support whole-of-government and coalition approaches.

3.52 To meet this challenge, RPDE has established competence in rapid task delivery through partnering with government and industry. In effect, RPDE brings together Defence and industry knowledge, experience and intellectual property in order to understand problems, identify potential solutions and provide valid evidence in support of decision and change management recommendations.

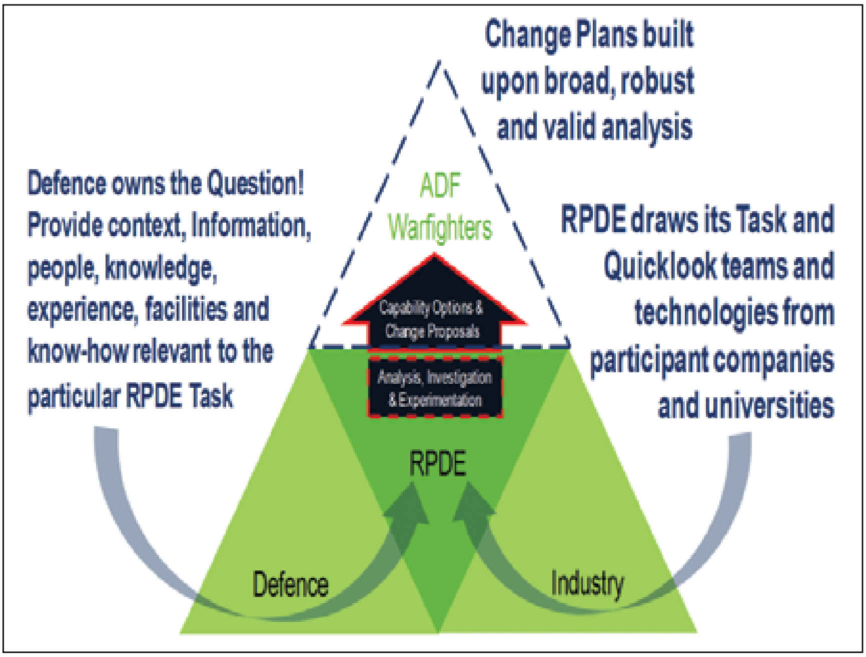

Change Plans built upon broad, robust and valid analysis
Defence owns the Question! Provide context, Information, people, knowledge, experience, facilities and know-how relevant to the particular RPDE Task
ADF Warfighters
RPDE draws its Task and Quicklook teams and technologies from participant companies and universities
Capability Options & Change Proposals
Analysis, Investigation & Experimentation
RPDE
Defence
Industry

Figure 3-9: RPDE linkages to Defence, industry and the warfighter

3.53 Since 2007, RPDE has provided 13 Tasks (which deliver a prototyped solution to Defence) and 23 Quicklooks (which deliver industry advice to Defence in the form of a report). Tasks are developed and delivered within a period of 12 to 18 months and Quicklooks are developed and delivered within a period of two to three months. The process of providing a prototyped solution to Defence or delivering industry advice in quick time is a catalyst for accelerating change and innovation.

3.54 A key strategy to deliver value to the ADF is to proactively identify appropriate activities-based capability problems and opportunities that directly affect the warfighter. To implement this strategy, RPDE focuses on engagement with operational organisations. The key outcome sought is an increased awareness of the capacity of the program to provide network-centric solutions to problems occurring in any ADF domain, group or organisation.

3.55 RPDE also takes into account the ADF's need to operate in conjunction with domestic and international government agencies and Defence forces. Although RPDE's mission is to enhance the ADF's warfighting capability, it does so in the broader context of networking to support whole-of-government and coalition approaches in both warlike and non-warlike activities, such as peacekeeping, border protection and disaster recovery. RPDE has been directly engaging other government agencies to ensure that whole of government issues are not overlooked.

NCW Integration and Implementation

> *The ADF has to be able to operate in joint, interagency and coalition environments. So the individual capabilities being acquired for the Navy, Army and Air Force need to be able to work seamlessly with each other.*
>
> CCDG, Australian Defence Magazine Conference, February 2009

Governance, Roles and Responsibilities

3.56 Integrating and implementing NCW to build Force 2030 will require some changes to structures and relationships in Defence and to relationships between Defence and other players.

Capability Development Group

3.57 The Defence Committee has given the CDG responsibility for ensuring that the ADF develops into a comprehensive networked force. Therefore, each project in the DCP must be integrated with all other ADF force elements so that they are compatible and consistent with this objective.

3.58 Critical to the achievement of this objective is the requirement to develop logical, traceable systems of systems and project architectures that are compliant with the Australian Defence Architectural Framework.[10]

3.59 NCW-specific matters in CDG are managed through:

- **The Capability Development Committee process** – Critical integration, coordination and implementation requirements of NCW-enabling activities in the DCP will be reviewed, considered and authorised in conjunction with the higher-level Capability Development Committee process within CDG.
- **The NCW Development Directorate (NCWDD)** – The NCWDD is responsible for providing advice and direct assistance to achieve cross-project integration in the wider DCP/NCW construct. The NCWDD's main integration tool is the Defence NCW compliance framework, which has been developed to assess DCP projects against a series of NCW-specific criteria (see figure 3-10).

[10] Architecture is the fundamental organisation of a system embodied in its components, their relationships to each other and the environment, and the principles guiding the system's design and evolution.

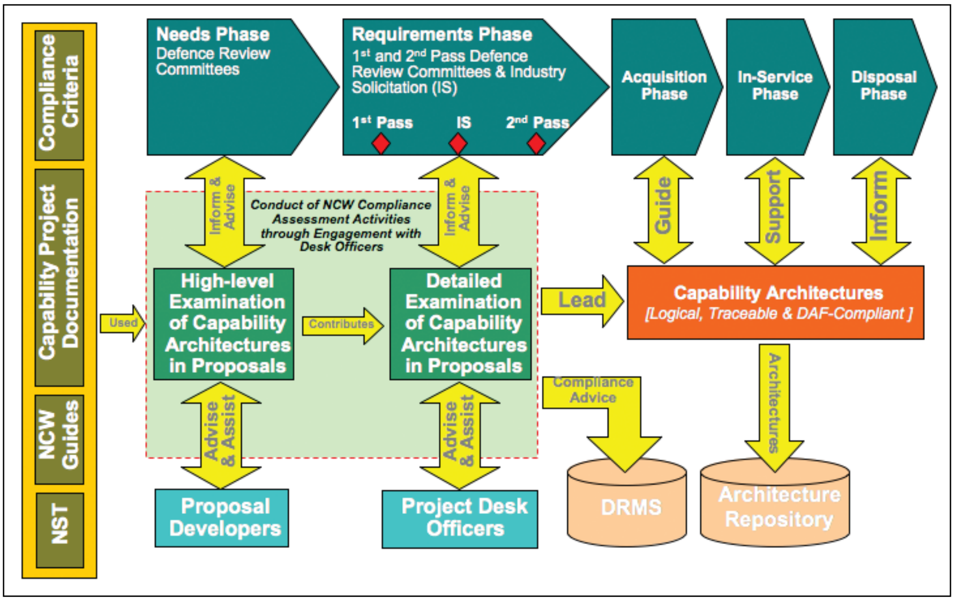

Compliance Criteria
Capability Project Documentation
NCW Guides
NST
Used
Needs Phase
Defence Review Committees
Requirements Phase
1st and 2nd Pass Defence Review Committees & Industry Solicitation (IS)
1st Pass
IS
2nd Pass
Acquisition Phase
In-Service Phase
Disposal Phase
Inform & Advise
Conduct of NCW Compliance Assessment Activities through Engagement with Desk Officers
Inform & Advise
Guide
Support
Inform
High-level Examination of Capability Architectures in Proposals
Contributes
Detailed Examination of Capability Architectures in Proposals
Lead
Capability Architectures
[Logical, Traceable & DAF-Compliant]
Compliance Advice
Architectures
Advise & Assist
Advise & Assist
Proposal Developers
Project Desk Officers
DRMS
Architecture Repository

Figure 3-10: The Defence NCW compliance framework

3.60 Although the Chief CDG is responsible to the CDF for implementing NCW across the ADF, whole-of-Defence collaboration and coordination is needed to ensure that all aspects of the networked ADF are effectively integrated and implemented throughout the capability lifecycle.

Strategic Policy Division

3.61 Strategic Policy Division (SP Div) is part of the Strategy Executive within the Office of the Secretary and Chief of the Defence Force Group. It provides Defence with overarching strategic guidance and supporting plans to inform Defence decision-making, including on the development and use of Defence capability. SP Div responsibilities also include the management of Australian export controls, Defence's involvement in domestic counter-terrorism, space, cyberspace, missile defence, strategic strike capabilities and effects, and international collaborative programs.

3.62 As one of the key outcomes of strategic planning reform, and as directed in the 2009 Defence White Paper, Defence is required to establish a force structure and capability development process to ensure stronger linkages between strategic guidance, force development and capability decisions. The Force Structure Development Directorate (FSDD) has been established in the Military Strategy Branch of SP Div to deliver this capability.

3.63 The vision for the FSDD is to 'institutionalise' the force structure process within the current five-yearly Defence White Paper planning cycle, with an emphasis on translating strategic guidance into concrete ADF tasks and force structure guidance, where that needs to be done at a higher level of detail. The FSDD will be critical in setting the strategic context required for detailed force options testing, and joint or service experimentation work, but will not conduct that work or replicate the CDG function.

Vice Chief of the Defence Force Group

3.64 The VCDF Group undertakes Defence business at the strategic level, a key task of which is to improve Defence's ability to deliver joint capability. Joint Capability Coordination (JCC) Division undertakes this task for the VCDF.

3.65 The Head of JCC works with the capability managers in the single services and other Defence groups to address the inherent challenges of creating a joint force. JCC operates at the conceptual and policy level of joint capability management, allowing the services and groups to perform their important role as capability managers. JCC helps to optimise the benefits of joint enabling capabilities already in the VCDF Group, particularly joint logistics, joint health and joint education, doctrine, training and warfare. JCC contributes to the strategic interoperability of Australia's joint forces by working with relevant government agencies and coalition partners.

3.66 JCC also manages and reports on the current joint force through an accurate and timely preparedness management system. It works with SP Div, CDG and the Chief Information Officer Group to develop future joint force capabilities. JCC validates the readiness of the current joint force and options for the future force by using the results of joint and combined exercising, experimentation and simulation activities in HQJOC, CDG, SP Div, DSTO and the Joint Education Training and Warfare Centre.

3.67 JCC also provides a policy and coordination lead in discrete joint capabilities including counter improvised explosive detection, joint ISR, joint EW, joint fires (including air/land integration) and chemical, biological, radiation and nuclear defence. JCC also works closely with HQJOC as its capability manager to progress its capability requirements for a variety of current and near-future operations.

3.68 JCC maintains a strong interest in the development of NCW concepts, policies and governance arrangements, as well as the practical implementation of NCW-related joint systems and platforms. In particular, JCC will support the implementation and development of a joint operational architecture (JOA) that maintains the joint warfighter as its point of focus. It will also maintain an interest in operations-enabling enterprise ICT and architecture for logistics and health services.

3.69 VCDF Group will collaborate with the People Strategies and Policy Group (PSPG) in determining common learning and development requirements and strategies and the delivery of joint education, training and doctrine. It will consult with the services on complementary and enabling single-service education, training and doctrine.

Capability Managers

3.70 The Service Chiefs and the Deputy Secretary Intelligence and Security Group, as the designated capability managers, have a primary interest in raising, training and sustaining capabilities for operational deployment, and providing a whole-of-Defence capability to meet the Government's broader strategic requirements.[11]

3.71 Capability managers are responsible and accountable, within the capability lifecycle, for:

- recommending, in conjunction with the Chief CDG, to the CDF and Secretary the appropriate capability to meet Defence Planning Guidance within agreed funding guidance, including changes to force structure and appropriate capital investments
- providing professional advice, including information on fundamental inputs to capability (FICs) to the Chief Capability Development Group and Defence committees, to ensure that the capability development process and options put to the Government for approval will meet the Government's capability objectives and will be implementable and sustainable
- ensuring, for each major capital project, that all FICs are appropriately addressed before second pass approval, and are coordinated and delivered after second pass approval
- reporting, in conjunction with the Chief CDG, and after second pass approval, to the Government on the operational and capability consequences of any failure by FIC providers to deliver agreed outputs, any failure to coordinate the whole of capability management, and any changed circumstances that might affect the capability
- reaching an agreement with the Defence Materiel Organisation (DMO) and other FIC providers on the level of support needed to maintain in-service capabilities to the level of funded preparedness, as directed by CDF, to meet government priorities.

[11] As agreed by the Defence Capability Investment Committee on 4 March 2004.

People Strategies and Policy Group

3.72 The role of PSPG is to focus on policy, planning and evaluation in relation to human resources, the essential drivers of Defence. This activity includes recruiting, retention, remuneration and reward, people development, leadership and the working environment. PSPG is therefore responsible for the development and enhancement of strategies, policies, processes and systems to enable Defence to attract, select, develop, conserve and retain its future networked workforce. In collaboration with VCDF Group (and as noted above), PSPG will also determine common learning and development requirements and strategies.

Chief Information Officer Group

3.73 The CIO is the coordinating capability manager for the Defence information environment and is responsible for all assets and capabilities involved in information exchange across all security domains used for military operations and Defence business. The CIO is supported in this role by the Defence ICT Committee, which considers, reviews and prioritises all ICT initiatives and expenditure across Defence, within the context of the agreed Defence ICT strategy.

3.74 At the core of the Defence ICT strategy is a governance framework that will ensure that all ICT investments are aligned with the priorities set by the CDF and Secretary, articulated through a single portfolio of work. In essence, the strategy provides a holistic, end-to-end view of ICT as a key capability relevant to NCW outcomes. The ICT strategy also sees the Chief Information Officer Group providing a single enterprise architecture and the enterprise-level information and communications common services needed for an NCW-capable Defence information environment.

3.75 Two elements of the ICT strategy critical for the successful delivery of an integrated network are the stakeholder engagement teams (to obtain and prioritise warfighter and business requirements) and the Chief Technology Officer Division (CTOD) to define and implement a single Defence information environment with a single integrated Defence architecture strategy and defined standards.

Defence Science and Technology Organisation

3.76 DSTO has conducted and continues to conduct a range of NCW science and technology activities, from applied research through to support of current operations, in direct support of NCW integration and implementation. These activities have included:

- developing and testing NCW measures of effectiveness for the NCW Implementation Progress Evaluation Activity – Exercise Talisman Sabre 2007

- developing 'Net Warrior', an NCW research capability that aims to address future NCW and mission systems technologies
- identifying issues and potential solutions associated with the practical implementation of NCW technology in the areas of bandwidth limitations and connectivity
- technical risk assessments for first and second pass projects that include an assessment of the systems integration (including NCW) risks.

3.77 A more recent DSTO initiative to support the advancement of NCW is the Joint Decision Support Centre (JDSC), which is a CDG and DSTO collaboration that facilitates decision-making, exploration of new concepts and the understanding of future capability requirements, using a wide range of analytical, gaming and experimentation tools.

3.78 The JDSC has been successfully used to 'operationalise' the concept of NCW, explore requirements for Australia's future amphibious and air combat capabilities, reduce the risk posed by improvised explosive devices (IEDs) and explore the complexities of whole-of-government approaches to warfighting. The JDSC also played a key role in the development of the 2009 Defence White Paper, providing high-fidelity simulations in which the various threats and force structure options that evolved during force structure options testing were modelled. In the future, the JDSC will be linked with similar systems overseas, with RPDE, and with the Joint Combined Training Capability.

3.79 Another initiative that commenced in 2008 is the Capability Technology Demonstrator Extension Program. The program identifies successful capability technology demonstrators and provides funding to take them quickly to the next stage of development, so that they can be moved into service with the ADF more quickly. The current program is investing in technologies such as robots for counter-IED detection and management, innovative body armour, anti-ship missile detection and motion-detection sensors for use in UAVs.

The Defence Materiel Organisation

3.80 DMO is committed to improving acquisition and sustainment of materiel systems that support NCW objectives. It is actively developing policies, business processes and implementation guidance to make this possible.

3.81 DMO is also collaborating with CDG (NCWDD) and CIOG (CTOD) to develop the NCWIIS and update existing capability development guidance, including the Capability Definition Documentation Guide, to promote better definition of NCW requirements.

3.82 DMO is increasingly engaged on NCW issues with other external stakeholders, such as the Chief Information Officer Group, to facilitate the delivery of interoperable systems. Internationally, the DMO is working with the United States Department of Defense (US DoD) on the concept of 'systems of systems', the management of which is integral to NCW outcomes.

3.83 A key integrating organisation within DMO is the Tactical Information Exchange Integration Office (TIEIO), which supports the ongoing development and sustainment of the tactical information exchange domain (TIED) to deliver an interoperable and compliant networked force to the ADF. The TIEIO has been involved with a number of important initiatives that contribute directly to the development of an NCW-enabled Defence.

3.84 The more significant of those initiatives are the development of new policy for joint and combined interoperability within the TIED; review of project delivery schedules and capabilities against the NCW Roadmap; contribution to the Gate Reviews of DMO acquisition projects; management of the TIED Project (JP 2089), with its planned deliveries of improved ANZAC and F/A 18 capabilities; improved compliance planning and testing; and engineering support initiatives, such as NETWARS and the Systems Integration Support Project for the Land TIED.

3.85 A recent strategic initiative between DMO and DSTO has seen the establishment of the Defence Systems Integration Technical Advisory (DSI–TA). This new organisation forms part of the DMO, with support provided by DSTO. The main objective of the DSI–TA is to provide independent identification, assessment and mitigation strategies for 'systems' and 'systems of systems' integration risks in current and future major DCP projects.

3.86 The DSI–TA provides advice and assists in the establishment of initial systems concepts, and examines complexities of systems integration. It also performs systems engineering analysis to assist in developing performance specifications research and development, and to test or assess alternative solutions to problems. The DSI–TA will also act as an adviser in the monitoring, assessment and provision of knowledge on systems integration risks as required.

3.87 Other typical tasks for the DSI–TA will include the following:

- Establish a risk architecture, comprising sources of both internal and external risks (including strategic international relations) for key projects before entry into the DCP and first pass.
- Perform metric-based analysis of future and existing projects in terms of integrated edge versus cost and world's best practice.
- Establish and implement DMO's systems integration policy and a systems integration code of best practice, and advocate the code of best practice within Defence procurement and sustainment.

- Conduct systems integration risk reviews, as directed by the CEO DMO/GM Programs and/or the Chief Defence Scientist.
- Report annually to the CEO DMO and the Chief Defence Scientist about key systems integration challenges facing 'projects of concern'.
- Facilitate sponsored or direct research, development, testing and simulation to investigate problems, investigate alternative technical approaches, and evaluate design agent achievements.
- Facilitate rapid transition of innovative research and development projects into the ADF, in consultation with the Chief Defence Scientist, using DSTO systems integration labs.
- Engage with international systems integration communities to benchmark Defence's systems integration performance and establish mutually beneficial collaborations.
- Engage with the university sector on systems integration expertise and training.

Industry

3.88 The Government recognises the vital role of Australian industry in supporting ADF capability. Industry is a key stakeholder in the development of a networked ADF, and has a particular role in helping to enable newly acquired or modified equipment to be interfaced into existing systems at the platform and network levels and in providing overarching communications architectures. Accordingly, involvement by Defence with industry forums, such as the Australian Defence Industry Electronic Systems Association, is strongly encouraged.

3.89 Outside Australia, Defence joined the Network Centric Operations Industry Consortium (NCOIC) in 2007. NCOIC is a prominent Defence-focused industry group. It was founded in the US in September 2004 and is supported by US and European defence (and other) industry groups, whose products rely on network connectivity. The NCOIC focuses on 'open standards for connectivity' and aims to provide a framework that establishes standards, principles, processes and trends to underpin the integration of existing and emerging open standards, to achieve interoperability across all classes of information systems.

Allies and coalition partners

3.90 Many of our allies and coalition partners are also examining, developing and implementing responses to the challenges and opportunities of the information age. Most notable are the efforts of the US DoD in the development of joint net-centric operations and the UK Ministry of Defence in the development of networked enabled capability. Both have gained considerable experience in the deployment and evaluation of network-enabled forces. Their experiences offer an opportunity to the ADF to learn from them and collaborate with them in further activities.

3.91 One example is the Coalition Warrior Interoperability Demonstration – an annual US-led initiative, involving US combatant commands, military forces and national civil agencies, and selected coalition partners. The demonstration identifies, investigates and assesses C4ISR (command, control, communications, computing, intelligence, surveillance and reconnaissance) solutions to enhance interoperability. Achieving this goal requires partnering with industry to provide and demonstrate solutions that are then evaluated through unbiased and relevant technical, security and warfighter assessments.

3.92 As the alliance with the US is Australia's most important defence relationship, the conduct of coalition operations between Australia and the US is a primary consideration in planning for and building interoperability. The publicly available *Australia / US Capability Development Liaison Handbook* provides strategic-level oversight of the requirements that will drive the development of our respective future forces, among a number of forums in which interoperability and 'requirements harmonisation' can be progressed.

NCW Integration and Implementation Strategy

3.93 While the 2009 NCW Roadmap provides a broad approach to the achievement of the networked ADF, the developing NCW Integration and Implementation Strategy (NCWIIS) will provide detailed ways, means and end states to develop capabilities that effectively integrate the information exchange systems into the future operation of our joint force. The NCWIIS is planned to be released within Defence by mid 2010.

3.94 The NCWIIS will also lay out the ADF methodology for the development of integrated capabilities, maximising the alignment of each individual element of capability with existing and future overall ADF capabilities. An integral feature of this methodology will be the introduction of the Joint Operational Architecture (JOA), to facilitate standardisation and enhance interoperability (see figure 3-11). The JOA is seen as a key enabler in the transition of Defence to Force 2030, and from a platform orientation to whole-of-capability planning.

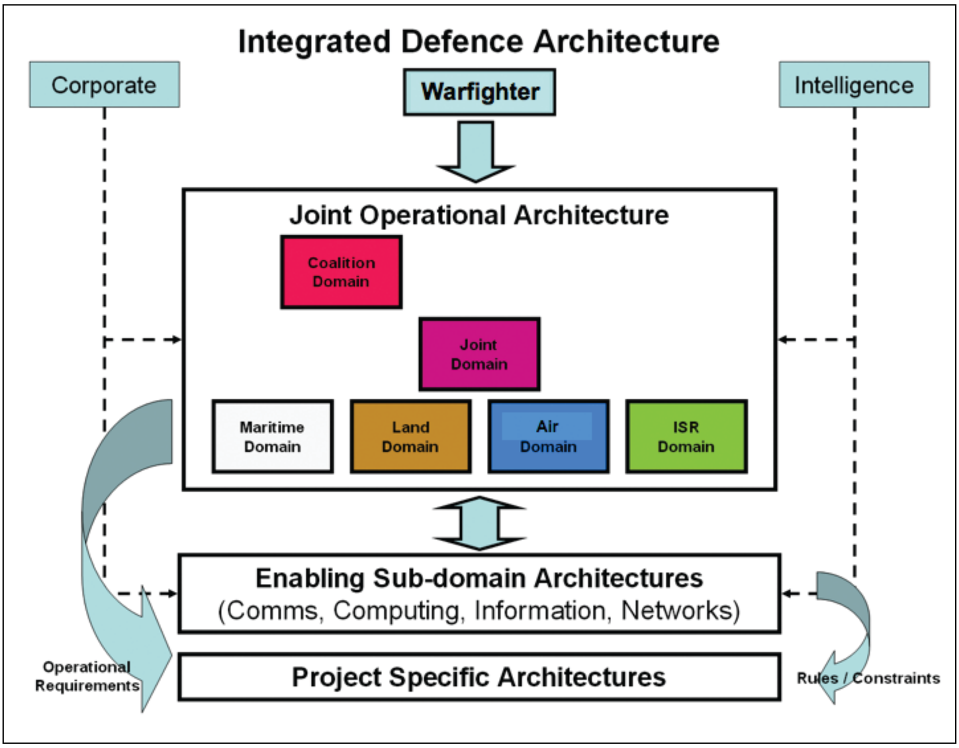

Integrated Defence Architecture
Corporate
Warfighter
Intelligence
Joint Operational Architecture
Coalition Domain
Joint Domain
Maritime Domain
Land Domain
Air Domain
ISR Domain
Enabling Sub-domain Architectures
(Comms, Computing, Information, Networks)
Operational Requirements
Project Specific Architectures
Rules / Constraints

Figure 3-11: The Joint Operational Architecture within the Integrated Defence Architecture

Opportunities and threats

3.95 Table 3-1 outlines key opportunities and threats posed by the development and implementation of NCW in Defence. This analysis was undertaken through a RPDE 'Quicklook', in conjunction with a representative group from Australian industry.

Opportunities	Threats
• Emerging technological innovations • The establishment of Head Joint Capability Coordination within VCDF Group for joint capability management • The Defence ICT Strategy and Reform Program • The development of an integrated defence architecture • The use of common enterprise services to improve information sharing • The ability to better share and fuse information across a force • Enhanced situational awareness leads to better decision-making • NCW will assist ADF people to conduct their individual and collective tasks better • The 'learn by doing' approach • The US DoD Global Information Grid and partnership in the Wideband Global Satellite Program • Lessons learnt from allied and coalition planning and conduct of net-centric operations • The establishment of Defence Systems Integration Technical Advisory within the DMO for systems integration • The use of experimentation, modelling and simulation • Collaboration with industry through the RPDE Program • Demonstrations through Capability Technological Demonstrator and Coalition Warrior Interoperability Demonstration programs • The Network Centric Operations Industry Consortium and its associated frameworks and assessment tools • Lessons learnt from allies and coalition partners in achieving effective NCW governance arrangements • Improving information assurance	• Pursuing a transparent battlespace • The vulnerability and integrity of the network • Competition within the RF spectrum • An overreliance on technology • Failure to plan for force integration (and its complexities) at the outset • Failure to optimise the network dimension through poor information management • Not achieving the required levels of integration with and between legacy systems • Failure to develop the human dimension in line with the network dimension • Adopting a service/platform centric mindset in capability development • Failure to understand and develop network-centric CONOPs • Being 'risk averse' as opposed to 'risk aware' as part of the 'learn by doing' approach • A lack of willingness to adapt our doctrine, tactics, structures and organisation in line with new CONOPs • Not remaining interoperable with our allies and potential coalition partners across the global and regional continuum • Extending the network to other government agencies • Continued use of proprietary / closed standards • Not achieving the required balance of assets and systems across the ADF • Not understanding how to measure enhancements to warfighting advantages through NCW

Table 3-1: NCW opportunities and threats – a summary

4

Part 4 Key messages

4.1 The Australian Government has acknowledged the need for Defence to adapt to the warfighting complexities of the information age and to harness the warfighting advantages offered through the use of modern technology.

4.2 The CDF has also set a clear vision for the future ADF. Fundamental to it is a networked force, which has access to fully integrated services that are also interoperable with other government agencies and our allies and coalition partners.

4.3 The implementation of NCW is a key enabler to develop the networked ADF. Although NCW is not a warfighting concept, it aims to enhance the warfighting capability of the ADF by linking sensor, C2 and engagement systems through the network.

4.4 The ADF needs to take the following actions to build the network:

- Set NCW milestones to establish structured goals and timeframes for NCW-related initiatives that will progressively build to achieve the networked force and the NCW target states.
- Establish an integrated network to link sensor, C2 and engagement systems across the ADF, effectively integrate and exchange information between those systems, and provide the underlying information and communications infrastructure upon which the networked ADF will be developed.
- Develop the human dimension of NCW to prepare the ADF and its people for operating in a networked battlespace, by changes in doctrine, organisation, training and education, with an emphasis on a 'learn by doing' approach.
- Accelerate the process of change and innovation to take advantage of advances in knowledge, processes and technology, refining them through an increased use of experimentation.

4.5 The development and building of the networked ADF across a range of human and system interfaces will be a complex undertaking that will require the engagement of expertise from outside Defence, and extensive collaboration and coordination across the whole of Defence. Deliberate and thorough planning will also be required to ensure that all new and, where required, legacy capabilities are integrated if the networked ADF is to form an effective and responsive whole.

4.6 Finally, although NCW is based on the use of modern technology, a balance must be achieved between the 'science of war' (technological capabilities) and the 'art of war' (human capabilities). Warfighting in the information age, although requiring the employment of networked and integrated capabilities, remains a human endeavour, where the ability of decision-makers to command must be supported by technology rather than be constrained by it.

References & Abbreviations

References

2009 Defence White Paper, *Defending Australia in the Asia Pacific century: Force 2030*, Department of Defence, May 2009

Defence Capability Plan 2009, Public Version, Department of Defence, July 2009

Defence Simulation Roadmap 2006, Department of Defence, 2006

Defence Test and Evaluation Roadmap 2008, Department of Defence, 2008

Enabling future warfighting: Network Centric Warfare, Australian Defence Doctrine Publication D.3.1, Department of Defence, February 2004

Explaining NCW, Department of Defence, December 2005

Defence Capability Development Manual, Department of Defence, July 2009

Force 2020, Department of Defence, June 2002

ISR Roadmap 2007–2017, Department of Defence, July 2007

Joint operations for the 21 Century, Australian Defence Doctrine Publication D.3, Department of Defence, June 2007

Abbreviations

ADF	Australian Defence Force
ADIESA	Australian Defence Industry Electronic Systems Association
AEW&C	airborne early warning and control
AWD	air warfare destroyer
BMS	battle management system
C2	command and control
C3	Command, Control and Communications
CDF	Chief of the Defence Force
CDG	Capability Development Group
COP	common operating picture
DCP	Defence Capability Plan
DIGO	Defence Imagery and Geospatial Organisation
DJTFHQ	Deployable Joint Task Force Headquarters
DMO	Defence Materiel Organisation
DSD	Defence Signals Directorate
DSI–TA	Defence Systems Integration Technical Advisory
DSTO	Defence Science and Technology Organisation
EW	electronic warfare
FICs	fundamental inputs to capability
FASOC	Future Air and Space Operating Concept
FJOC	Future Joint Operating Concept
FLOC	Future Land Operating Concept
FMOC	Future Maritime Operating Concept
FOC	final operational capability
FSDD	Force Structure Development Directorate
HF	high frequency
HJCC	Head Joint Capability Coordination
HNA	Hardened and Networked Army
HQJOC	Headquarters Joint Operations Command
ICT	information communications technology

IED	improvised explosive device
IO	information operations
IOC	initial operational capability
I&S	Intelligence and Security Group
ISR	intelligence, surveillance and reconnaissance
JCC	Joint Capability Coordination
JDSC	Joint Decision Support Centre
JDNO	Joint Data Network Officer
JICO	Joint Interface Control Officer
JOA	Joint Operational Architecture
JSOW	Joint Stand-Off Weapon
JSF	Joint Strike Fighter
JTF	Joint Task Force
LHD	landing helicopter dock
MASTIS	Maritime Advanced Satellite Terminal Information System
MDM	multidimensional manoeuvre
MEAO	Middle East Area of Operations
MILIS	Military Logistics Information System
MILSATCOM	Military Satellite Communications
MTWAN	Maritime Tactical Wide Area Network
NACC	New Air Combat Capability
NAVWAR	navigation warfare
NCOIC	Network Centric Operations Industry Consortium
NCW	network centric warfare
NCWDD	NCW Development Directorate
NCWIIS	NCW Integration and Implementation Strategy
NSA	National Support Area
OT&E	operational test and evaluation
PSPG	People Strategies and Policy Group
RPDE	Rapid Prototyping, Development & Evaluation Program

RF	radio frequency
SASR	Special Air Service Regiment
SATCOM	satellite communications
SP	strategic policy
SO	Special Operations
SOTG	Special Operations Task Group
SOV-SR	Special Operations Vehicle – Special Reconnaissance
T&E	test and evaluation
TDL	tactical data link
TIED	tactical information exchange domain
TIEIO	Tactical Information Exchange Integration Office
UAV	uninhabited aerial vehicle
US DoD	United States Department of Defense
VCDF	Vice Chief of the Defence Force