# Chapter 2

# The Australian Defence Force and Network Centric Warfare

## Gary Waters

## Introduction

The global economy continues to be more networked through information and communication technologies that are fast becoming ubiquitous. Decision-to-action cycles are reducing to cope with the increasing pace of change, which is placing a premium on innovation, information sharing and collaboration. At the same time, national security is being broadened, large quantities of information are flowing along with calls for better quality information, and connectivity is increasing, all of which leads to an increase in the strategic value of information. Ed Waltz expresses it well as:

> the role of electronically collected and managed information at all levels has increased to become a major component of both commerce and warfare. The electronic transmission and processing of information content has expanded both the scope and speed of business and military processes.[1]

In June 2002, Defence released its doctrinal statement on Australia's approach to warfare.[2] In looking at how the Australian Defence Force (ADF) would prepare itself to cope with increasing and rapid change, the focus of the document turned initially to what the Information Age heralded. Attacks on information systems were cited as potential security threats to which the ADF would need to respond.[3] Furthermore, the ADF should expect to find itself increasingly operating in 'small, dispersed combat groups',[4] which would be facilitated in part through technological advances in communications.

Defence also released its long-term vision statement in June 2002—known as *Force 2020*. In articulating a vision of a seamless force—internally with each other (the three Services) and externally with the range of providers, supporting entities and the community[5] —the ADF also highlighted the fundamental need to transform from a platform-centric force to a network-centric one.

The ADF argued that 'the aim of Network-Enabled Operations is to obtain common and enhanced battlespace awareness, and with the application of that

awareness, deliver maximum combat effect'.[6] Furthermore, the fundamental building block of networked operations would be a comprehensive 'information network' that linked the sensor grid (for detection), the command and control (C2) grid (offering flexible, optimised decision-making), and the engagement grid (for precision engagement).[7]

Through network-enabled operations, the ADF would be conferred with what it termed 'decision superiority'—'the ability to make better, faster decisions, based upon more complete information than an adversary'.[8] The ADF cited operations in Afghanistan where Unmanned Aerial Vehicles (UAVs) passed real-time targeting information (via video) to aircraft, epitomising the effectiveness of Network Centric Warfare (NCW), through the direct sensor-to-shooter link that allowed rapid engagement of targets. This is what the ADF means by seamless integration of platforms through the information network.[9]

In May 2003, the Chief of the Defence Force, General Peter Cosgrove, noted to an NCW conference that

> while it is likely that some type of crude kinetic effect will still be the ultimate expression of violence in war, it is also likely that as information and network-related war fighting techniques start to mature and to predominate, outcomes will be swifter, as dramatic and paradoxically less bloody than the classic force-on-force attritionist, paradigm of the past.[10]

Indeed, Cosgrove cited the 2003 Iraq War, from which he observed that 'in the main, the Iraqi forces were beaten quickly, spectacularly and comprehensively by a force using what were, on balance, mostly first generation network-centric technologies and concepts'.[11]

The seamless integration called for in *Force 2020* and inferred by Cosgrove has necessitated the ADF moving away from a focus on individual weapon platforms towards exploiting the effectiveness of linked, or networked, forces and capabilities. Networking will allow the sharing of a common and current relevant picture of the operational environment across all components of the joint force. This will, in turn, improve a force's situational awareness, coordination, and importantly, decision-making ability. The joint force will exploit this as it is able to prepare for and conduct operations more smoothly and quickly.

Operations will rely on linking sensors, weapons and commanders, via an appropriate information network, to enable the timely and precise application of military force. By embracing a 'networked' approach to military operations, the ADF will be able to generate greater combat effectiveness than belies its relatively small size—be able to 'punch well above its weight'.

These notions have been reinforced through the release in 2007 of Defence's *Future Joint Operating Concept* (*FJOC*).[12] The *FJOC* starts with Air Chief Marshal Angus Houston's vision for the ADF, which is 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'.[13] The *FJOC* goes on to argue that the force must operate in the seamless manner described in *Force 2020*, not only to maximise the ADF's collective warfighting capabilities but also its ability to operate with interagency and coalition partners. Improved networking will enhance the ADF's capability advantage over potential adversaries as it also relies on its people to generate the underlying capability advantage and the 'knowledge edge' needed for the future.

Increasingly, the ADF must be capable of both executing effective combat operations and providing military support to national responses in more complex environments. The ADF must move to develop a hardened, networked, deployable joint force that is characterised by adaptability and agility to handle the full range of military operations across the full spectrum of conflicts.

In the information dimension, future adversaries will utilise informal communications technologies that are cheap, ubiquitous and difficult to trace, and increasingly secure and sophisticated networked C2 and intelligence, surveillance and reconnaissance (ISR) systems, leveraging commercial satellite capabilities and improved geospatial information.

The *FJOC* adopts a national effects-based approach, which involves taking a whole-of-nation view of security to find the most appropriate tool to achieve national objectives—the military is but one of the tools. It is underpinned by the NCW Concept that will help link ADF, Australian and coalition sensors, engagement systems and decision-makers into an effective and responsive whole. NCW seeks to provide the future force with the ability to generate tempo, precision and combat power through shared situational awareness, clear procedures, and the information connectivity needed to synchronise friendly actions to meet the commander's intent.

The ADF and Defence will work in cooperation with other government and non-government agencies (where appropriate) to develop the capability for an integrated multi-agency response capability, extending the network to other agencies as appropriate.

In the Future Warfighting Concept,[14] the ADF adopted Multidimensional Manoeuvre (MDM) as its approach to future warfare. MDM seeks to negate the adversary's strategy through the intelligent and creative application of an effects-based approach against an adversary's critical vulnerabilities. It uses an indirect approach to defeat the adversary's will, seeking to apply tailored strategic responses to achieve the desired effects.

MDM operations are designed to focus on specific and achievable effects through integrating joint warfighting functions (force application, force deployment, force protection, force generation and sustainment, C2, and knowledge dominance). A fundamental of MDM is the ability to employ NCW and operate in joint task force, interagency and/or coalition arrangements to conduct effective operations. The joint operational concept underlying MDM are best described in terms of the ability to *reach*, *know* and *exploit* as follows:

- *Reach*—Reach describes the future force's ability to operate in multiple dimensions both inside and outside the operational area and across the physical, virtual and human domains in order to understand and shape the environment; deter, defeat and deny the adversary; and provide military assistance in support of national interests. Reach is best accomplished as part of an integrated whole-of-government approach across the spectrum of military, diplomatic, economic and informational actions.[15]

- *Know*—The future force will build and sustain sufficient knowledge from national and international sources to allow it to identify required actions and assess the effects of those actions. It will understand itself and its capabilities, those of its adversaries, as well as the operating environment, which will enable the force to better carry out those actions that create decisive effects. Information is at the base of knowledge dominance, and knowing requires that the future force is able to utilise and integrate information from strategic, operational and tactical sources, both military and civilian. However, information must be turned into knowledge that is timely, relevant and accurate. This knowledge must be acquired, prioritised, refined and shared across the strategic, operational and tactical levels and within the joint force and as part of multi-agency and multinational efforts.[16]

- *Exploit*—The future force will integrate its joint capabilities with other elements of national power in order to achieve effects in support of national strategic objectives. Effects are the outcomes of the actions taken to change unacceptable conditions and behaviours, or to create freedom of action to achieve desired objectives. The force will identify, create and exploit effects through acquiring knowledge and establishing reach. To exploit its capability to produce effects, the future force will continually assess its effects and adjust its actions to take into account the iterative interaction of military, diplomatic, economic and informational actions that are taken as part of Australia's whole-of-government approach.[17]

The following attributes define the ADF of the future:[18]

- *Balanced*—The future force must possess an appropriate mix of capabilities in order to mount the range of operations envisaged. It must offer a multiplicity of responses and not rely on 'niche' capability.

- *Networked*—The future force will need assured access to other agency, coalition and open-source information. The ability to operate effectively will be contingent on the integrated forces' networks and decision-making infrastructures, early warning systems, communications, environmental monitoring and positional data. Adversaries may exploit any vulnerability in the nation's network to undermine cohesion and effectiveness.

- *Deployable*—In the future, the ADF will need to operate at a distance from established bases in Australia, either independently or with coalition forces, potentially involving deployments with regional or global reach. Force elements will need to be configured and prepared for short-notice deployments that can be sustained with limited infrastructure support. This will require either a capability to lift forces into the contingency area or basing rights close to the contingency area. A forced-entry capability will also be critical to the ADF's ability to respond.

- *Integrated and Interoperable*—The ADF must continue the transition to a force (with fully integrated services) that is interoperable with other agencies of the government and its coalition partners and allies. Legacy systems should, to the extent possible, be made to function in the integrated environment until replaced. As the degree of integration and synchronisation is increased, new training and systems will need to be established. Military capabilities should be designed to be interoperable from conception, not as an afterthought in the development process.

- *Survivable and Robust*—Each element of the future force must be able to protect itself against the range of existing and evolving threats. Timely investment in lower signatures, protection, countermeasures and redundancy to match likely threats will be required.

- *Ready and Responsive*—The future ADF must observe, anticipate and be prepared to serve Australia's global interest in an evolving strategic and geopolitical situation.

- *Agile and Versatile*—The future ADF must be able to respond rapidly to a diverse range of missions and tasks. This will require versatile forces that are tailored and scalable for deployment. They will need an ability, the extent of which will be dictated by force structure, to re-form, reconstitute, regroup and re-engage, especially during periods of concurrent operations.

- *Precise and Discriminating*—The goal for future operations is to achieve precise effects, with minimum planning and response time, from a distance if required. For the future ADF, precision must not be limited to the application of kinetic force, but also be incorporated into executing information operations (IOs) and minimising unintended consequences. While traditional technology will initially provide the potential to improve precision, emergent technology must be used to support widespread cross-platform responses that ensure maximum flexibility and discrimination.

Enhanced discrimination capabilities will permit high-value targets to be struck with greater certainty.

- *Lethal and Non-lethal*—The ADF must increase its capability to produce desired effects through the considered and coordinated use of both lethal and non-lethal methods, using both kinetic and non-kinetic means. These effects will be enhanced by leveraging technology advances which improve precision and discrimination, and by employing a whole-of-nation approach.

- *Persistent and Poised*—Persistence ensures that the joint force has the required endurance at all levels to generate and deploy forces for long periods, while poise ensures that critical fighting elements are within range of a potential target area. Persistence incorporates force protection, logistics, infrastructure development and sustaining the capacity of ADF people to work and fight. The persistence of the future ADF may necessitate a greater level of force dispersal, leading to a requirement to generate effects from dispersed locations, while at the same time being poised to project force at short notice. Poise is achieved through either expanding deployability or securing basing rights close to likely contingency areas.

- *Sustainable*—The increasing mobility, tempo and changeability of future force operations will require an adaptive, modular, network-enabled logistic system operating in a contiguous and non-contiguous mission space.

- *Capable of Concurrency*—The future force must be able to conduct operations in more than one location simultaneously. The Defence Planning Guidance provides guidance on the number and nature of deployed operations across the maritime, land, air and space environments. The major capabilities underpinning these operations will be the effective use of information to C2 forces, the ability to conduct strike operations, and the ability to generate and sustain military forces.

- *Legal and Ethical*—In accordance with ADF core values, the ADF operates within the Australian legal framework and the international Law of Armed Conflict. The future ADF must continue to take pride in operating within an ethical framework, derived from a strong warfighting tradition.

Armed with those insights into where the ADF is headed, this chapter discusses the ADF's NCW Concept, *NCW Roadmap*, and Information Superiority and Support (IS&S) Concept in more detail to set the ensuing discussion in subsequent chapters on the 'cyber' dimension, Information Warfare (IW), how information infrastructures can be targeted, how they can be protected, and how both offensive and defensive IOs can best be brought together via an Australian cyber-warfare centre.

## The ADF'S NCW Concept

In December 2003, the final NCW Concept Paper was produced by the Policy Guidance and Analysis Division, within the Strategy Group.[19] The Concept

Paper argued that NCW involved the linkage of engagement systems to sensors through networks and the sharing of information between force elements. Information is only useful if it allows people to act more effectively: this makes the human dimension fundamental to NCW. NCW thus has two closely related and mutually reinforcing dimensions—the human dimension and the network dimension. The NCW Concept argues that

> the human dimension is based on professional mastery and mission command, and requires high standards of training, education, doctrine, organisation and leadership. This dimension is about the way people collaborate to share their awareness of the situation, so that they can fight more effectively. It requires trust between warfighters across different levels, and trust between warfighters and their supporting agencies.[20]

The Concept continues:

> The second dimension, the network, connects major military systems, including engagement, sensor and command systems. The network dimension was the initial focus of development, but change here was always expected to have a profound influence on the human dimension.[21]

NCW is seen by the ADF as a 'means to realising a more effective warfighting ability. New technology will change the character of conflict, but war's enduring nature—its friction, fog and chaotic features—will persist'.[22] The Australian NCW Concept accepts this enduring nature of war, but does seek to reduce the effects of fog and friction.

The purpose of the NCW Concept was to provide a starting point for the identification and exploitation of the opportunities of NCW. It would inform and shape the conduct of Defence's NCW-related research and experimentation programs, which would further crystalise an understanding of the opportunities and risks associated with NCW. The ADF would continually revisit the concept in order to confirm its validity based on the lessons learned through research, experimentation and operational experience.

The ADF's NCW Concept is based on the following premises, which will be tested through experimentation:[23]

- Professional mastery is essential to NCW.
- Mission command will remain an effective command philosophy into the future.
- Information and intelligence will be shared if a network is built by connecting engagement systems, sensor systems, and C2 systems.
- Robust networks will allow the ADF, and supporting agencies, to collaborate more effectively and achieve shared situational awareness.

- Shared situational awareness will enable self-synchronisation, which helps warfighters to adapt to changing circumstances and allows them to apply MDM more effectively.

The last two are fundamental in transforming the way in which information is managed, used and exploited. These are expanded on below.

## Networks

Robust networks involve sharing information and intelligence through a connected network that also includes engagement, sensor and command systems. While we might look at these systems separately, many of the ADF's platforms perform across all four grids. There is an expectation that NCW will offer an ability to explore alternatives, whereby sensors may be separated from the engagement system, or the ADF might be able to reduce the size of its deployed force.

The ADF aims to develop and integrate an advanced sensor system, ranging from space-based assets to humans, to gather widely disparate information. In doing this, the ADF expects a certain amount of redundancy (without wasteful duplication) to ensure persistent battlespace awareness. That said, the integration of information from sensors will not provide complete understanding of the battlespace, although greater analytic capacity to produce intelligence is anticipated. In the end, commanders will still have to decide whether to fight for more information or to work with the information and intelligence available.[24]

Advanced command support systems will bring together information about the adversary, own and friendly forces, other parties, and the environment into a Common Relevant Operating Picture (CROP). In addition, these systems will allow different levels of the ADF, relevant government agencies, and coalition partners to work together. Through these advanced command support systems, the ADF would expect to enhance its capacity for mission rehearsal, wargaming and development, and analysis of possible courses of action. Essential logistic information between the warfighters and support bases should also be able to be exchanged more effectively.[25]

In terms of its engagement systems, the ADF will aim for its decision-makers to have timely access to the most useful engagement systems for the mission, noting that different systems have different levels of mobility, firepower and self-protection. The intent will be to shorten the time between detection, identification, engagement and assessment. The network dimension of NCW assists forces to:[26]

- *collect* relevant information;
- *connect* units and platforms through networking, doctrine, training and organisation;

- *use* the information and intelligence in a timely manner to achieve the commander's intent; and
- *protect* the network from external interference or technical failure.

The *collect-connect-use-protect* framework is the means through which the ADF can organise its effort to develop the network. This framework, which underpins the IS&S Concept, is discussed in more detail later.

The ADF will need to monitor carefully the way networks are progressing in the commercial sector, where developments will have a strong influence on what is available, noting that Defence will move increasingly to commercial off-the-shelf (COTS) solutions for its hardware and software.

As networks and people come together and the notions of trust and information sharing become integral to making decisions, the ADF will need to be aware of interactions across the information, cognitive and physical domains:[27]

- In the *information domain*, connectivity allows people to share, access and protect information.
- In the *cognitive domain*, connectivity allows people to develop a shared understanding of the commander's intent, and to identify opportunities in the situation and vulnerabilities in the adversary.
- In the *physical domain*, selected elements of a force are equipped to achieve secure and seamless connectivity and interoperability. This connectivity will allow some sensor systems to pass target acquisition information directly to engagement systems. Based on the shared understanding developed in the other domains, forces are able to synchronise actions in the physical domain.

These domains also apply to an adversary; hence, the NCW Concept also seeks to influence an adversary by disrupting their ability to function effectively within, and across, each of these domains.

## Shared situational awareness

Shared situational awareness develops as people absorb information, collaborate to understand its implications, and then acquire a shared view of the situation at hand. Thus, shared situational awareness brings together both the network and human dimensions of NCW.[28]

Collaboration is essential to shared situational awareness because it allows widely dispersed forces to use their battlespace awareness for mutual advantage in terms of analysis, decision-making, and application of force. The challenge for the ADF will be to cope with a shift from sequential planning activities through a hierarchy to an ongoing interaction between different levels, which will save time and provide opportunities for simultaneous action. Again, both

the network (technical means) and human dimensions (ability of people) are important for collaboration.[29]

Collaboration requires a high degree of trust throughout the chain of command. Hence, training and personnel development must provide opportunities for different elements of the ADF to become familiar with one another, the Defence organisation more broadly, and with other agencies.

## Self-synchronisation

Another challenge of NCW will be for the ADF to evolve from its top-down way of synchronising forces and actions. People will need to use their shared situational awareness to recognise changes and opportunities themselves, and to act without direction to meet the commander's intent. Self-synchronisation will thus lead to speedier decision-to-action cycles by capitalising on the shared understanding and collective initiative of lower-level commanders and staffs.[30]

## Balancing risks and opportunities

NCW will focus on warfighting through the concept of MCM. The network is only 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. The Concept identified five areas of potential risk:[31]

- The failure to incorporate the human dimension into thinking about NCW.
- The potential for disruption—through an adversary exploiting vulnerabilities, indirect attacks on networks, denial of communications, or misleading information. Network integrity will need to be assured.
- Pursuit of a 'transparent' battlespace, which is almost certainly unachievable. The ADF must not expect NCW to deliver an 'unblinking eye' across the whole battlespace. Commanders must cope with, and thrive in, ambiguity.
- The potential exists to be overloaded with information, threatening friendly forces with self-induced paralysis. Commanders may also become addicted to information, causing hesitation while waiting for the key piece of evidence.
- Commanders could attempt to micro-manage operations.

The real opportunities presented by NCW offer priorities and benchmarks for further development. These include people, operations, logistics, decision-making, training, organisation, doctrine, and major systems as follows:

- NCW will help the ADF's *people* conduct their individual and collective tasks better.

- NCW will help to make a small force like the ADF more efficient and effective on *operations*. NCW should assist the ADF to operate in a more dispersed manner, while permitting the concentration of combat power when required.
- NCW will allow technology to be used to automate *logistic* reporting, support sophisticated self-diagnostic systems that improve equipment reliability, and improve service delivery in areas such as medical support.
- NCW will help ADF commanders to make better *decisions* by improving their ability to command operations, control forces and conduct planning.
- The improved ability to conduct *training and education* will help to increase the confidence and skills of individuals, and enhance trust between individuals, even when they work in dispersed organisations.
- The ADF will use NCW to improve the *organisation*'s ability to shape or react to evolving situations, to collaborate better across organisational boundaries, and to exploit collective knowledge.
- The ADF will need to respond to an NCW-induced fast rate of change by adopting trial *doctrine*, which could leverage off lessons learned from experimentation, training and operations.
- Adopting a network-centric approach is intended to reduce incompatibilities between and within *major systems*, and allow each to be employed with maximum effect. New systems will need to fit seamlessly within an information infrastructure. Legacy systems that remain will need to be adapted for NCW. This has implications for coalition operations and for cooperation with other government agencies; hence clear standards will be crucial.[32]

The NCW Concept clearly supports *Force 2020* by teasing out these implications of NCW on the Fundamental Inputs to Capability. *Force 2020* argued:

> Our strategic advantage will come from combining technology with people, operational concepts, organisation, training and doctrine. We must be careful to ensure that technology does not give an illusion of progress—we cannot afford to maintain outdated ways of thinking, organising and fighting.[33]

*FJOC* continues in this theme, adding the ability to reach, know and exploit (as discussed earlier).

## The *NCW Roadmap*

The 2020 networked force will be an exceptionally complex organisation with a range of different relationships (machine and human) which will require careful and thorough integration. Conducting rapid prototyping and development (RPD) activities will allow Defence to mitigate the risks that are inherent in this integration. It will support experimentation and provide the ability to simulate future capabilities to aid in determining the optimum level of integration between

engagement, sensor and C2 systems. RPD will reduce the risk of implementing NCW and help accelerate change.[34]

The capacity to concurrently 'learn by doing'[35] is also important for implementing NCW. Hence, the way ahead, or the *NCW Roadmap*, centres on a 'learn by doing' strategy. A draft *NCW Roadmap* was also produced in December 2003, to plan and coordinate the implementation of NCW, but was not formally released until October 2005. This document set out the future requirement for NCW, the current level of networked capability, and the steps needed to realise a future networked force.[36] Defence also released a short document explaining NCW.[37]

The first step in 'learn by doing' involves constructing the foundation for enhanced collaboration and shared situational awareness. This foundation will, in the main, comprise the information infrastructure and the governance measures needed to improve connectivity for selected force elements. As this underlying infrastructure improves; so too will the collaborative ability of elements within the ADF.

As stated earlier, the long-term aspiration is to link all ADF elements into a 'single virtual network', where information is assembled and passed through a series of interlinked grids: sensor grids gather data; information grids fuse and process it; and engagement grids (overlaid by an appropriate C2 grid) allow warfighters to generate the desired battlespace effects.

NCW has the potential to facilitate the collaboration required for the ADF to employ MDM more effectively. It will assist the force to generate the tempo, agility and ultimately the warfighting advantage needed to prevail against a wide variety of adversaries. However, the ADF will also need to enhance the capacities of its people and its platforms for the future, ensuring they are networked to better exploit the chaotic conditions of the battlespace. The fog, friction and ambiguity will remain; the ADF must ensure that it is better able to exploit this than an adversary.[38]

The 2005 *NCW Roadmap* provides the direction, and initial steps, to implement the NCW Concept. It is Defence's guide to discovering and exploiting the opportunities of NCW; and identifies four key actions:[39]

- set the NCW-related targets for Defence to achieve;
- establish the Network to provide the underlying information infrastructure upon which the networked force will be developed;
- explore the human dimensions of the networked force and initiate changes in doctrine, education and training with appropriate support mechanisms; and
- accelerate the process of change and innovation through the establishment of a RPD capability in partnership with Industry.

Subsequent to publication of the 2005 *NCW Roadmap*, Defence released a publication entitled *Explaining NCW*. [40] Defence argues in this document that 'NCW is a means of organising the force by using modern information technology (IT) to link sensors, decision-makers and weapon systems to help people work more effectively together to achieve the commander's intent'.[41] Furthermore, NCW can 'contribute significantly to producing a warfighting advantage'.[42] The information network sits at the centre, linking the C2 systems, sensor systems, and engagement systems.

Defence identified the key capability development projects that would deliver the desired network capability and packaged them as a system, which also provided a model for future systems planning and capability integration. This included projects associated with communications in the maritime, land and air environments; a wide area communications network; network management and defence; satellite communications (SATCOM); tactical information exchange; information exchange in a coalition environment; and other information protection measures.[43]

Indeed, General Peter Cosgrove had already presaged some of these projects when he said, in May 2003,[44] that Defence would look at how it could harmonise sophisticated technology with people in networked systems, noting that the future maritime surveillance and response project and the Joint Command Support System showed great promise here. He also referred to other behind-the-scenes changes, such as the adoption of a standardised 'J series' message format (supporting tactical information exchange) as being critical pieces of the NCW puzzle.

He also foreshadowed that Defence would place key links, such as Airborne Early Warning and Control (AEW&C) aircraft, into the network over the next few years. And the recent move into space, through the Optus satellite, provides another part of an increasingly pervasive network. These systems, said Cosgrove, will magnify the pay-off from our network-centric approach.[45]

A governance system for the Defence Information Environment was implemented in 2003, led by the newly-created Office of the Chief Information Officer, to ensure that activity across the Department was aligned and enforced. This governance framework encapsulated the interrelationships and interdependencies in the development, management and operation of Defence's supporting information environment.[46]

Network protection was to be designed through the use of an Information Security Architecture, which is an integral component of a Defence-wide Information Architecture. The architecture would address the design of information systems, access control, data management and accountability frameworks.

## The human dimension

The examination of NCW's human dimension was to focus on the following areas:

- the nature of C2;
- transitioning to a new way of operating;
- nurturing innovation; and
- Defence culture.

As General Cosgrove had remarked in May 2003, 'it is vital that we keep people in our focus as we implement NCW. Anybody can buy technology. Anybody can copy concepts. But nobody can duplicate the advantage we get from our smart, dedicated and adaptable people'.[47]

The 2005 *NCW Roadmap* developed this human dimension further, with a focus on doctrine, education, training and development. It argued the need to raise NCW awareness, educate the senior leaders, prepare the future leaders, understand the future workforce, produce the NCW tools and plan for doctrine development, and develop a mechanism for evaluation and feedback of lessons learnt.[48]

## Accelerating change and innovation

In terms of accelerating change and innovation, Defence was to establish a RPD program by July 2004 to fulfill three functions:

- identify and test new technologies, concepts, procedures and organisations that could be implemented in the near term (6–18 months) to improve the ADF's networked warfighting capabilities;
- identify early problems with the implementation of NCW and use RPD as an intervention activity to redress the problem or mitigate risk; and
- provide for the rapid delivery of capability to warfighters to meet or anticipate emerging security challenges.

A Rapid Prototyping, Development and Evaluation (RPDE) capability was set up in 2005, with the mission of enhancing 'ADF warfighting capacity through accelerated capability change in the NCW environment'.[49] Importantly, RPDE allows collaboration across a wide range of organisations, more rapid fielding of capability improvements, and a focus on all fundamental inputs to capability—personnel, organisation, collective training, major systems, supplies, facilities, support, and command and management.[50]

## Defence's Information Superiority and Support Concept

In August 2004 Defence released its IS&S Concept, which articulated the key components of the concept, described the architectural approach to be taken,

identified the target states for the future and posed a key set of questions to be addressed.[51]

The key components of the concept (focused on connecting, collecting, using and protecting information) are outlined below:[52]

- *Ubiquitous network or information distribution (Connect)* enables effective sharing of information by people, systems, applications and sensors, whether it is by voice, data or video. It involves coordinating the infrastructure including fixed and mobile communications, computers, processes, systems and tools that enable the sharing of information throughout the force to achieve information and decision superiority. When the network is threatened, it must allow for a graceful degradation of service availability and access to information that ensures continuity of operations. Once the threat has been resolved, access to information and original service availability levels must be rapidly reconstituted.
- *Persistent awareness (Collect)* enhances situational awareness that allows better perception of battlespace elements in terms of time and space, the comprehension of their meaning and projected intent. Persistent awareness tools and systems help collect, collate and fuse disparate data and information, which requires greater attention to content management. Persistence does not mean continuous; it means sufficient awareness to enable the ADF to act in a way that is operationally responsive and appropriate.
- *Smart use or decision support (Use)* focuses on achievable intent. It involves planning and the provision of information and common processes and collaboration tools to facilitate timely and effective decision-making throughout the various levels of command.
- *Pervasive Security (Protect)* provides a secure information environment that offers a trusted and reliable flow of information to continuously support operations and business activities.[53]

## Networking issues

The IS&S Concept emerged from the observation that networking improves efficiency and effectiveness of operations. It depends on computers and communications to link people through information flows, which in turn depends on interoperability across all systems. Networking involves collaboration and sharing of information to ensure that all appropriate assets can be quickly brought to bear by commanders during combat operations.[54] In a 2004 report by the US Congress, a number of key networking issues were identified, the most relevant of which, for the purposes of this discussion, was network architectures.[55]

Because NCW is so highly dependent on the interoperability of communications equipment, data, and software to enable the networking of people, sensors, and platforms (both manned and unmanned), network

architectures are very important. Architectures are needed to bring together all the elements of NCW technology that rely on line-of-sight radio transmission for microwave or infra-red signals, or laser beams; as well as other technologies that aggregate information for transmission through larger network trunks for global distribution via fibre-optic cables, microwave towers, or both low-altitude and high-altitude satellites.[56]

The ADF architecture must enable rapid communications between individuals in all three Services, as well as rapid sharing of data and information between mobile platforms and sensors used across the ADF. As the ADF comes to depend on networking, the network itself must be able to re-form when any communications node is interrupted (the United States refers to this as dynamically self-healing).

## The ADF's capability planning for NCW

The ADF's concept is less about warfighting and more about how net-centric capability will enable future warfighting.[57] Defence has been moving steadily along the net-centric path for several years now in terms of developing the capability to provide the ability for data to be exchanged across linked networks. Some ships and aircraft as well as fixed and deployable communications systems have already achieved a degree of data connectivity.[58]

The ADF can deliver secure C2 to small-scale deployments around the world. It can use its 'Secret' and 'Restricted' fixed networks, as well as data-links (Link 11) and radios (*Parakeet*) to provide certain levels of connectivity.

It can draw information from multiple sources such as the over-the-horizon *Jindalee* Operational Radar Network (JORN) and radars on Royal Australian Navy (RAN) ships to generate a basic level of situational awareness. Major combat units are linked by voice communications, with some aircraft and ships data-linked. Secure SATCOM are available to select elements of the ADF, such as Special Forces, and secure satellite data-link provides connectivity between ground-based air defence systems and the Royal Australian Air Force (RAAF)'s Regional Operations Centre.[59] Defence has argued that it is developing its networked force by:[60]

- creating new doctrine, better training and a more agile organisation, all of which leads to people operating more effectively as a network;
- guiding force development through the release of the 2005 *NCW Roadmap* and Integration Plan (the latter is not available publicly);
- connecting broad areas of Defence so that information can be shared and used more cooperatively; and
- fast-tracking the introduction of new technology through its RPDE program.

The Chief of Capability Development Group is responsible for implementing NCW across Defence, which reinforces the earlier point that the ADF's network-centric focus is on developing capability to enhance future warfighting effectiveness.

The major network projects that have been identified for implementation thus far include:[61]

- A joint command support environment, which will link the air, maritime, land and special operations elements into the one single ADF command system.
- A similar project, which will integrate intelligence systems.
- Military SATCOM that will provide the ADF with coverage throughout the region.
- Tactical information exchange that will facilitate movement of information from sensors to weapon systems, starting with *ANZAC* frigates and *Hornet* fighters.
- Battlespace communications for air, land and maritime forces, which will provide the information backbone and tactical data distribution for deployed forces.
- A Defence wide-area communications network, which will provide the next-generation fixed infrastructure for secure computers and telephones. Linkages will be established between the fixed and deployable communications networks.
- A Defence network operations centre, which will enhance current computer network defence capabilities.
- Combined information exchanges with the United States, United Kingdom, Canada and New Zealand, which will provide a permanent system for exchanging information and enabling collaboration.
- A number of major systems that will connect to the 'network', such as the New Air Combat Capability, high-altitude long-endurance UAVs, the Air Warfare Destroyer (AWD), and a suite of other projects that will 'harden' and 'network' the Australian Army.

By 2020, a networked ADF should be able to generate a range of lethal and non-lethal effects that are timely, appropriate and synchronised. It will have continuous information connectivity to link fighting units, sensors and decision-makers that sees an ADF with increased situational awareness and the capacity to act decisively. The Defence C2 system will promote collaboration. Defence will be capable of rapidly deploying and protecting an optimised force. A pervasive network of active and passive sensors will improve awareness for force protection purposes. Key logistics networks will be linked and offer connectivity and collaboration.[62]

Defence has adopted a systems approach to improve the integration of many complex projects. Capability Development Group is focusing on three key areas of development in its Capability Plan. These are:

• the enabling infrastructure to deliver the robust communications network;
• the enabling information systems to support mission command, ISR, imagery and military geospatial information sharing; and
• the combat platforms and hardware to deliver combat effects enabled by the information systems and infrastructure.[63]

There has been some significant slippage in the milestones needed to evolve NCW capability that were articulated in the 2005 *NCW Roadmap*. The key milestones in that Roadmap were as follows:[64]

• 2008: Broadband Networked Maritime Task Group—initial capability.
• 2008: Networked Aerospace Surveillance and Battlespace Management (ASBM) capability.
• 2009: Interim Networked Land Combat Force.
• 2010: Networked Fleet—mature capability.
• 2010: Integrated Coalition Network capability.
• 2012: First Networked Brigade.
• 2013: Networked Air Warfare Force.
• 2014: Second networked Brigade.
• 2015: Robust Battlespace Network.
• 2015: Networked Joint Task Force.

The milestones in the 2007 *NCW Roadmap* are as follows:[65]

• 2008: Networked Special Operations Unit.
• 2008: Networked Air Combat Force.
• 2009: Networked Battle Group.
• 2009: Networked Rapid Mobility Force.
• 2011: Networked Maritime Task Group.
• 2011: Networked Combat Support Force.
• 2011: Networked Tactical ISR.
• 2012: First Networked Brigade.
• 2012: Networked Special Operations Task Group.
• 2012: Networked Deployable Joint Task Force Headquarters.
• 2014: Networked Fleet.
• 2014: Second Networked Brigade.
• 2014: Networked Aerospace Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance and Electronic Warfare (C4ISREW) Force.
• 2014: Networked Operational ISR.
• 2014: Networked Deployable Joint Task Force.

- 2014: Networked Coalition Combat Force.
- 2016: Networked Joint Force.

Notwithstanding the slippages, there has been some acceleration, and the 2007 *NCW Roadmap* certainly provides both a clearer and a more comprehensive view. For a start, the new Roadmap breaks these milestones into six domains as depicted in the following table:[66]

**Table 1—NCW Domain and Milestone Overview**

| Coalition | Joint Force | Maritime | Land | Aerospace | ISR |
|---|---|---|---|---|---|
| 2014:<br>Networked Coalition Combat Force | 2012:<br>Networked Deployable Joint Task Force Headquarters | 2011:<br>Networked Maritime Task Group | 2008:<br>Networked Special Operations Unit | 2008:<br>Networked Air Combat Force | 2011:<br>Networked Tactical ISR |
| | 2014:<br>Networked Deployable Joint Task Force | 2014:<br>Networked Fleet | 2009:<br>Networked Battle Group | 2009:<br>Networked Rapid Mobility Force | 2014:<br>Networked Operational ISR |
| | 2016:<br>Networked Joint Force | | 2012:<br>First Networked Brigade | 2011:<br>Networked Combat Support Force | |
| | | | 2012:<br>Networked Special Operations Task Group | 2014:<br>Networked Aerospace C4ISREW Force | |
| | | | 2014:<br>Second Networked Brigade | | |

(*Source*: Director General Capability and Plans, *NCW Roadmap 2007*, Defence Publishing Service, Canberra, March 2007, p. 22.)

A second improvement in the 2007 *NCW Roadmap* is that it breaks down each of the six domains into the grids—C2 capability, network capability, sensor capability, and engagement capability. Furthermore, in the two years between the roadmaps, Defence had come to understand the need for greater cooperation and coordination across projects to deliver a new networked ADF for 2016. These milestones are discussed in more detail below under each domain.

## Maritime

- *Networked Maritime Task Group—2011*: This capability will be principally delivered through three projects: JP 2008 Phase 3F (Military SATCOM Capability); SEA 1442 (Maritime Tactical Wide Area Network); and AIR 5276 (the AP-3C *Orion* upgrade). The outcomes of these projects—Maritime Advanced SATCOM Terrestrial Infrastructure System (MASTIS) terminals, wide area Local Area Networks (LANs), and new high-speed data-links for the AP-3C *Orion*—will provide broadband connectivity for major fleet units.[67]

- *Networked Fleet—2014*: SEA 1442 (Maritime Communications and Information Management Architecture Modernisation) equipment acquisition will enable Internet Protocol (IP) networking at sea between major fleet units via the expansion of the Maritime Tactical Wide Area Network (MTWAN). Phase 4 of SEA 1442 will deliver upgraded communications capabilities through replacement radios, antennas and other systems and will form the basis of the networked fleet. SEA 4000 (AWD) and JP 2048 (Helicopter Landing Dock) will significantly improve the warfighting capability of this force.[68]

## Land

- *Networked Special Operations Unit—2008*: JP 2097 Phase 1A (Project *Redfin*) will deliver a Special Operations Vehicle and Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) package to provide a network-enabled capability for Special Air Services Regiment (SASR) land operations.[69]
- *Networked Battle Group—2009*: This force will consist of a number of all arms sub-units based on a mechanised infantry battle group headquarters or a cavalry battle group headquarters. The force will be equipped with digital communications and battle management systems.[70]
- *First Networked Brigade—2012*: The Networked Battle Group 2009 capabilities will be extended to complete the rollout to other Brigade elements. This milestone will see the evolution of the 1st Brigade into a fully networked capability. The major activities during this period will include the introduction of a Battle Management System–Dismounted (BMS–D) (Land 125), introduction of the M1A1 (Land 907), new communications bearers (JP 2072 Phase 2 and 3), Battle Management System–Mounted (BMS–M) (Land 75 Phase 4) and improved logistics support (JP 2077).[71]
- *Networked Special Operations Task Group—2012*: Project *Redfin* (JP 2097 Phase 1B) and the delivery of JP 2030 (Special Forces Command Support Capability) will provide communications, sensors, C2 and engagement systems for a complete Special Operations Task Group. This will consist of Special Operations Command (SOCOMD) units and external units in direct support. Gateway interfaces will enable the exchange of information with other ADF and coalition networks.[72]
- *Second Networked Brigade—2014*: The Networked Brigade 2012 capabilities will be extended to a second Brigade (3rd Brigade). This milestone will result from the capability delivery of two major projects, LAND 75 (Battlefield Command Support System) and LAND 125 (Solider Combat System).[73]

## Aerospace

- *Networked Air Combat Force—2008*: The provision of Tactical Data Links to the *ANZAC* frigate and F/A-18 *Hornet* (through JP 2089 Phase 2) combined

with the force multiplier capabilities of the AIR 5077 (AEW&C aircraft) are key enablers in networking the Aerospace Domain.[74]

- *Networked Rapid Mobility Force—2009*: The delivery AIR 8000 Phase 3 (four Boeing C-17 *Globemaster III*) combined with AIR 5402 (Multi-Role Tanker Transporters—Airbus A330-200) will provide significantly increased capacity and range for operations. The new Mobile Regional Operations Centre (AIR 5405) will provide an enhanced deployable C2 capability that can be combined with the transportable Tactical Air Defence Radar System (AIR 5375) to improve the networking and protection of the rapid mobility assets.[75]

- *Networked Combat Support Force—2011*: The delivery of further applications for the JP 2030 Phase 8 (Joint Command Support System) coupled with advances to the Standard Defence Supply System (SDSS) provided by JP 2077 (Improved Logistics Information Systems) will enhance the ability to provide timely levels of resources to deployed forces.[76]

- *Networked Aerospace C4ISREW Force—2014*: Projects JP 5077 (AEW&C), AIR 7000 Phase 1B (Multi-mission Unmanned Aerial System), and the upgraded AP-3C *Orion* (AIR 5276) will provide highly capable long-range ISR sensors. The delivery of the JP 2065 Phase 2 (Integrated Broadcast System) will disseminate ADF and allied ISR and Blue Force Tracking information to deployed forces via Tactical Data Links (JP 2089) and SATCOM (JP 2008). The delivery of SEA 4000 (AWD) will bring with it for the first time Theatre Ballistic Defence capabilities as well as an improved ability to control airspace well beyond Australian landmass where required.[77]

## ISR

- *Networked Tactical ISR—2011*: Project DEF 7013 Phase 4 (Joint Intelligence Support System) provides intelligence to commanders from networked databases and applications. The Battlespace Communications System (Land) (JP 2072) and Maritime Communications and Information Management Architecture Modernisation (SEA 1442 Phase 4) projects provide the means for tactical information dissemination. Project AIR 7000 Phase 1B (Multi-role UAV) and JP 129 (Tactical UAV) will provide new tactical and strategic sensors.[78]

- *Networked Operational ISR—2014*: By 2014, common geospatial information data and products will be accessible to users across the network (JP 2064 Phase 3). Advanced operational ISR capabilities will provide enhanced views of the battlespace through the space-based surveillance capability delivered by JP 2044 Phase 3 and the JORN upgrade (JP 2025 Phase 5). The ability to conduct tactical electronic warfare (EW) will be improved through Force Level Electronic Warfare DEF 224 (*Bunyip*). The networking of the ISR capabilities, together with the means to fuse the information, will be delivered by JP 2096. The Multi-mission Maritime Patrol Aircraft and the Multi-mission

Unmanned Aerial System (AIR 7000 Phase 1B and Phase 2B) will complete the acquisition of advanced networked collection systems from the tactical to the strategic levels. The networking of Defence into national and coalition intelligence and ISR networks will be accomplished by the remaining deliverables of JP 2096.[79]

## Joint force

- *Networked Deployable Joint Task Force Headquarters—2012*: For Joint Operations Command, Projects JP 8001, JP 2008 and JP 2030 Phase 8 will enhance situational awareness and connectivity. Other enhancements include JP 2089 (Tactical Data Links) and JP 2065 (Integrated Broadcast System). The delivery of the Mobile Regional Operations Centre (JP 5405) will enhance the C2 capability of deployable headquarters.[80]
- *Networked Deployable Joint Task Force—2014*: Improved spaced-based surveillance (JP 2044 Phases 3A and 3B), various communications bearers (JP 2008, SEA 1442, JP 2072), and surveillance projects (JP 2025, AIR 5432, AIR 7000 Phase 1B) will contribute to enhanced joint task force operations. The delivery of the Amphibious Ships (JP 2048 Phase 4A/4B) will further enhance the C2 capability of deployable headquarters.[81]
- *Networked Joint Force—2016*: By 2016 the ADF will have achieved the infrastructure, tools and C2 systems (JP 2030, AIR 5333, and JP 2072) capable of providing a robust battlespace network across the whole ADF. Communications beyond line-of-sight will be improved through JP 2008 Phase 4. The achievement of this milestone will allow the ADF to conduct NCW operations, thereby greatly improving warfighting flexibility and combat effectiveness.[82]

## Coalition

- *Networked Coalition Combat Force—2014*: This milestone coincides with the achievement of one key milestone from each of the other five Domains:[83]
  - Networked Fleet 2014;
  - Second Networked Brigade 2014;
  - Networked Aerospace C4ISREW Force 2014;
  - Networked Operational Intelligence 2014, and
  - Networked Joint Task Force 2014.

The Networked Coalition Domain focuses on how Defence integrates with Australia's allies and other government agencies. The integrated Coalition Network Capability will allow for the seamless integration of ADF C2, ASBM and communications into established coalition network architectures. A mature Networked Coalition Domain will also provide significant whole-of-government

benefits through integrating Defence with a range of other government agencies.[84]

## Conclusion

Defence is responding to the challenges of networking the future force in several ways, one of which is through an integrated Defence Information Environment. This is an environment where the Defence Information Infrastructure (DII) will need to be increasingly developed and managed as an integrated entity. Data, user applications, common information services, user devices, systems hardware, networks and data-links, and communications bearers will be integrated to form a foundation or backbone information capability.

A second and equally important way is through Capability Development Group's integrated capability development approach, which includes an NCW Program Office. Here, all capability projects are looked at through the lens of the particular domain (maritime, land, aerospace, ISR, joint force, and coalition); and then through the lens of the type of capability (C2, network, sensor, or engagement).

The degree of integration will be based on developing a robust communications network, supported by consistent joint doctrine and comprehensive training that should address and remove operational, intelligence and single Service stove-pipes. The approach is, of necessity, an incremental one that needs to be synchronised over time and defined through comprehensive architectures and technical standards, all underpinned by a focus on high levels of interoperability—particularly with Australia's close partners (especially the United States).

To achieve this, Defence will need to renew its efforts to better coordinate all aspects of NCW—the capability projects, the DII, the human element, the organisational element, the role of industry through RPDE, and research and development (R&D)—as well as further develop its NCW compliance process.

Delivery of the following would mean that a networked deployable joint task force should be possible by 2014, provided there is no substantial program slippage:

- key capability projects for maritime communications;
- military SATCOM;
- satellite surveillance;
- Mobile Regional Operations Centres;
- the ADF Air Defence System (known as *Vigilare*);
- the Joint Battlespace Communications System;
- the Battlefield Command Support System;
- Maritime Communications;

- the Tactical Information Exchange Domain (data-links);
- the Joint Command Support System;
- Integrated Broadcast System;
- Joint Intelligence Support System; and
- Project *Redfin*;

as well as the major capability projects such as:

- the Navantia-designed F100 AWD;
- the UAVs;
- the F/A-18 *Hornet* upgrade, the F/A-18E/F *Super Hornet*;
- the Headquarters Joint Operations Command (HQJOC) Project;
- the A330 multi-role tanker transport (MRTT) aerial refueling tankers;
- the *Wedgetail* AEW&C aircraft;
- the F-35 Joint Strike Fighter (JSF);
- the M1A1 *Abrams* tank;
- the soldier combat system program;
- the large *Canberra* class amphibious ships; and
- a network maintenance and upgrade program.

The ADF has learned a lot from recent operational experiences and experimentation, and is applying that to good effect.

In the networked ADF of the future, based on the capabilities outlined above, transparency of information and self-synchronisation must become key characteristics. This means that the various cultures and sub-cultures in Defence will have to converge, language will have to standardise, and collaboration will have to be the norm.[85]

NCW is as much an organisational and workforce phenomenon as it is a technological one. The ADF needs to prepare both its people and its organisation for the transition to this new technological base.

The omens are strong for achievement of a networked ADF in 2016, and realisation of the NCW vision. However much remains to be done, and serious intellectual effort needs to be devoted to realise an effectively networked ADF of the future. The capability milestones must be adhered to, the Network and its underlying infrastructure must be established, the human dimension must be developed (together with new doctrine, training and education programs), new organisational structures and processes must evolve, and the process of change and innovation must be accelerated through increased use of industry, experimentation and a more coherent and focused research program.

# ENDNOTES

[1] Edward Waltz, *Information Warfare: Principles and Operations*, Artech House Publications, Boston and London, 1998, p. 2.

[2] Department of Defence, *The Australian Approach to Warfare*, Department of Defence, Canberra, June 2002, available at <http://www.defence.gov.au/ publications/taatw.pdf>, accessed 4 March 2008.

[3] Department of Defence, *The Australian Approach to Warfare*, p. 12.

[4] Department of Defence, *The Australian Approach to Warfare*, p. 26.

[5] Department of Defence, *Force 2020*, Department of Defence, Canberra, June 2002, p. 17, available at <http://www.defence.gov.au/publications/f2020.pdf>, accessed 25 February 2008.

[6] Department of Defence, *Force 2020*, p. 19.

[7] Department of Defence, *Force 2020*, p. 19.

[8] Department of Defence, *Force 2020*, p. 20.

[9] Department of Defence, *Force 2020*, p. 20.

[10] Speech by General Peter Cosgrove to the Network Centric Warfare Conference on 20 May 2003, entitled 'Innovation, People, Partnerships: Continuous Modernisation in the ADF', available at <http://www.defence.gov.au/cdf/speeches/past/speech20030520.htm>, accessed 25 February 2008.

[11] General Peter Cosgrove, speech entitled 'Innovation, People, Partnerships: Continuous Modernisation in the ADF', available at <http://www.defence.gov.au/cdf/speeches/past/speech20030520.htm>, accessed 25 February 2008.

[12] Released as Department of Defence, *Joint Operations for the 21st Century*, Department of Defence, Canberra, May 2007, available at <http://www.defence.gov.au/publications/FJOC.pdf>, accessed 25 February 2008.

[13] Department of Defence, *Joint Operations for the 21st Century*, p. iii.

[14] Department of Defence, *Future Warfighting Concept*, Australian Defence Doctrine Publication (ADDP)-D.02, Department of Defence, Canberra, 2003, available at <http://www.defence.gov.au/publications/fwc.pdf>, accessed 25 February 2008.

[15] Department of Defence, *Joint Operations for the 21st Century*, p. 15.

[16] Department of Defence, *Joint Operations for the 21st Century*, pp. 15–16.

[17] Department of Defence, *Joint Operations for the 21st Century*, p. 16.

[18] Department of Defence, *Joint Operations for the 21st Century*, pp. 20–22.

[19] This work, that involved close collaboration across Defence was led by the then Head of the Policy Guidance and Analysis Division, Air Vice-Marshal John Blackburn. It was published as *Enabling Future Warfighting: Network Centric Warfare* (ADDP-D.3.1) in February 2004, but not released until May 2004.

[20] Department of Defence, *Enabling Future Warfighting: Network Centric Warfare*, ADDP-D.3.1, Australian Defence Headquarters, Canberra, February 2004, p. v.

[21] Department of Defence, *Enabling Future Warfighting: Network Centric Warfare*, p. v.

[22] Department of Defence, *Enabling Future Warfighting: Network Centric Warfare*, p. v.

[23] Department of Defence, *Enabling Future Warfighting: Network Centric Warfare*, p. 2-2.

[24] Department of Defence, *Enabling Future Warfighting: Network Centric Warfare*, p. 2-4.

[25] Department of Defence, *Enabling Future Warfighting: Network Centric Warfare*, p. 2-4 to p. 2-5.

[26] Department of Defence, *Enabling Future Warfighting: Network Centric Warfare*, p. 2-5.

[27] Department of Defence, *Enabling Future Warfighting: Network Centric Warfare*, p. 2-6.

[28] This is a fundamental point and I am indebted to Lieutenant Colonel Mick Ryan for his insight and persistence in teasing this out.

[29] Department of Defence, *Enabling Future Warfighting: Network Centric Warfare*, p. 2-6.

[30] Department of Defence, *Enabling Future Warfighting: Network Centric Warfare*, p. 2-7 for further elaboration.

[31] Department of Defence, *Enabling Future Warfighting: Network Centric Warfare*, p. 3-3 for expansion.

[32] Department of Defence, *Enabling Future Warfighting: Network Centric Warfare*, p. 3-4 to p. 3-6.

[33] Department of Defence, *Force 2020*, p. 11.

[34] Department of Defence, *Enabling Future Warfighting: Network Centric Warfare*, p. 4-1.

[35] Department of Defence, *Enabling Future Warfighting: Network Centric Warfare*, p. 4-2 for greater elaboration on this notion of 'learn by doing'.

[36] Department of Defence, *NCW Roadmap*, Department of Defence, Canberra, October 2005; updated in Director General Capability and Plans, *NCW Roadmap 2007*, Defence Publishing Service, Canberra, March 2007, available at <http://www.defence.gov.au/capability/ncwi/docs/2007NCW_Roadmap.pdf>, accessed 25 February 2008.

[37] Department of Defence, *Explaining NCW*, Department of Defence, Canberra, 21 February 2006, available at <http://www.defence.gov.au/capability/NCWI/docs/Explaining_NCW-21feb06.pdf>, accessed 25 February 2008.

[38] Department of Defence, *Enabling Future Warfighting: Network Centric Warfare*, p. 5-1.

[39] See Director General Capability and Plans, *NCW Roadmap 2007*, p. v.

[40] Department of Defence, *Explaining NCW*.

[41] Department of Defence, *Explaining NCW*, p. 5.

[42] Department of Defence, *Explaining NCW*, p. 5.

[43] The NCW milestones are described in Director General Capability and Plans, *NCW Roadmap 2007*, pp. 22–31.

[44] General Peter Cosgrove, 'Innovation, People, Partnerships: Continuous Modernisation in the ADF'.

[45] General Peter Cosgrove, 'Innovation, People, Partnerships: Continuous Modernisation in the ADF'.

[46] Patrick Hannan, as the first Defence Chief Information Officer, showed great insight and leadership in bringing an architectural approach and strong governance to the Defence Information Environment, ably supported by his chief architect, John Sheridan, and Sheridan's team of experts.

[47] General Peter Cosgrove, 'Innovation, People, Partnerships: Continuous Modernisation in the ADF'.

[48] Director General Capability and Plans, *NCW Roadmap 2007*, pp. 14–15.

[49] Department of Defence, *NCW Roadmap*, p. 32.

[50] Department of Defence, *NCW Roadmap*, p. 34. RPDE is discussed in some detail in NCW Roadmap 2007, pp. 43–45.

[51] Department of Defence, *A Concept for Enabling Information Superiority and Support*, Department of Defence, Canberra, August 2004.

[52] These core elements have been agreed by Defence and released publicly in *A Concept for Enabling Information Superiority and Support*, p. 11.

[53] Colleagues Andrew Balmaks, Mike Banham, Jason Scholz, and Anna McCarthy worked with me in developing these definitions, prior to public released of the IS&S Concept.

[54] US Department of Defense, *Report on Network Centric Warfare*, 2001, available at <http://www.defenselink.mil/nii/NCW/ncw_sense.pdf>, accessed 25 February 2008; and Ret. Admiral Arthur Cebrowski, Speech to Network Centric Warfare 2003 Conference, January 2003, available at <http://www.oft.osd.mil>, accessed 25 February 2008.

[55] Congressional Research Service (CRS) Report for Congress (received through the CRS Web), entitled 'Network Centric Warfare: Background and Oversight Issues for Congress', 2 June 2004, by Clay Wilson (Specialist in Technology and National Security Foreign Affairs, Defense, and Trade Division), available at <http://www.fas.org/man/crs/RL32411.pdf>, accessed 25 February 2008.

[56] CRS Report for Congress, 'Network Centric Warfare: Background and Oversight Issues for Congress'.

[57] See Department of Defence, *Explaining NCW*, p. 9.

[58] Department of Defence, *Explaining NCW*, p. 15.

[59] Department of Defence, *Explaining NCW*, pp. 15–16.

[60] Department of Defence, *Explaining NCW*, p. 17.

[61] Department of Defence, *Explaining NCW*, Figure 2.2, p. 19.

[62] Department of Defence, *Explaining NCW*, p. 18. These target states for 2020 relate to the future warfighting functions described in Department of Defence, *Future Warfighting Concept*, pp. 36–38.

[63] Director General Capability and Plans, *NCW Roadmap 2007*, p. 21.

[64] Department of Defence, *NCW Roadmap*, p. 20.

[65] Director General Capability and Plans, *NCW Roadmap 2007*, p. 22.

[66] Director General Capability and Plans, *NCW Roadmap 2007*, p. 22.

[67] Director General Capability and Plans, *NCW Roadmap 2007*, pp. 23–24.

[68] Director General Capability and Plans, *NCW Roadmap 2007*, p. 24.

[69] Director General Capability and Plans, *NCW Roadmap 2007*, p. 25.

[70] Director General Capability and Plans, *NCW Roadmap 2007*, p. 25.

[71] Director General Capability and Plans, *NCW Roadmap 2007*, pp. 25–26.

[72] Director General Capability and Plans, *NCW Roadmap 2007*, p. 26.

[73] Director General Capability and Plans, *NCW Roadmap 2007*, p. 26.

[74] Director General Capability and Plans, *NCW Roadmap 2007*, p. 27.

[75] Director General Capability and Plans, *NCW Roadmap 2007*, p. 27.

[76] Director General Capability and Plans, *NCW Roadmap 2007*, p. 27.

[77] Director General Capability and Plans, *NCW Roadmap 2007*, p. 27.

[78] Director General Capability and Plans, *NCW Roadmap 2007*, p. 28.

[79] Director General Capability and Plans, *NCW Roadmap 2007*, p. 28.

[80] Director General Capability and Plans, *NCW Roadmap 2007*, pp. 29–30.

[81] Director General Capability and Plans, *NCW Roadmap 2007*, p. 30.

[82] Director General Capability and Plans, *NCW Roadmap 2007*, p. 30.

[83] Director General Capability and Plans, *NCW Roadmap 2007*, p. 31.

[84] Director General Capability and Plans, *NCW Roadmap 2007*, p. 31.

[85] David Schmidtchen, *The Rise of the Strategic Private: Technology, Control and Change in a Network Enabled Military*, The General Sir Brudenell White Series, Land Warfare Studies Centre, Canberra, 2006, p. 49, where he refers to the four cultures as Navy, Army, Air Force, and Australian Public Service, and the sub-cultures as trades and professions.