Assessing NCW Compliance: An Australian Perspective

Michele A. Knight[1], Les J. Vencel[2] and Terry T. Moon[1]

[1] Defence Science & Technology Organisation, PO Box 1500, Edinburgh, SA 5111, Australia
Michele.Knight@dsto.defence.gov.au
Terry.Moon@dsto.defence.gov.au

[2] VCORP Consulting Pty Ltd, PO Box 251, Henley Beach, SA 5024, Australia
ljv@internode.on.net

Abstract. The Australian Defence Organisation (ADO) is implementing Network Centric Warfare (NCW) concepts. To facilitate the development of a net-centric military force, an NCW Program Office (NCWPO) was established to guide NCW compliance in major acquisition projects, from their inception to the end of their System Life Cycle. This paper outlines an approach to NCW Compliance that enables NCW-related issues to be addressed at appropriate stages in the acquisition of a system and throughout its life cycle.

Introduction

The Australian Defence Organisation (ADO) is implementing Network Centric Warfare (NCW) concepts[1] through an *NCW Roadmap*[2]. In an effort to develop appropriate processes and methods to assist in the development of a future NCW force, the ADO has engaged a number of different groups to look at the problem from different perspectives.

One aspect of the problem is to ensure that, as future capabilities are being developed or procured, they are compliant to a set of net-centric requirements. An NCW Program Office (NCWPO)[3] was established to guide NCW compliance in major acquisition projects, from their inception to the end of their System Life Cycle (SLC)[4]. The NCWPO developed the following objective for the NCW Compliance Process:
"To ensure the ADO's Capability Development Process delivers projects that are integrated in support of Australia's future warfighting capability requirements."

This paper outlines an NCW compliance process that is based on a simple underlying conceptual model~~.~~ The process was designed to check that major acquisition projects have addressed NCW-related issues at each stage of the Defence Capability Development Process.[5]

Related Work

The foundational concepts of Network Centric Warfare are discussed at length by Alberts, Garstka & Stein[6] and Alberts[7]. There are subtle differences in the approaches taken by various countries, with a variety of terms such as Network Enabled Capability (NEC), Network Based Defence (NBD) and Network Centric Operations (NCO) currently in use; however they all appear to have similar underlying aims. In particular, all of these net-centric approaches exploit modern information and communications technologies to share information so as to achieve better situational awareness, improved decision-making and enhanced collaboration across all elements of a military force. The attendant goal is to coordinate the various elements of a net-centric force to achieve decisive, swift, effective and efficient military outcomes.

The US and UK have developed their own processes for checking the congruence of the characteristics of major military systems with the attributes desired for net-centric operations. The US has established a

[1] Directorate of Future Warfighting, *Enabling Future Warfare: Network Centric Warfare*, March 2004.
[2] Capability Development Group, *NCW Roadmap*, October 2005.
[3] Director Capability Options and Plans, *Defence Capability Development Manual* 2006, 2006, p. 95.
[4] System Life Cycle processes: ISO/IEC 15288.
[5] Director Capability Options and Plans, *Defence Capability Development Manual* 2006, 2006, p. 5 and 95-97.
[6] Alberts, Garstka & Stein, *Network Centric Warfare*, 2nd ed., 1999.
[7] Alberts, *Information Age Transformation*, 2002.

Net-Centric Checklist, the purpose of which is to “assist program managers in understanding the net-centric attributes that their programs need to implement to move into the net-centric environment as part of a service-oriented architecture in the Global Information Grid”.[8] The UK has taken a different approach in developing “NEC Benefit Analysis” so as to understand the relationship between investment and force effectiveness. [9,10] In both countries, the method for checking the congruence of military capabilities with net-centric attributes has been constructed with their capability development and materiel acquisition processes in mind.[11]

In Australia a methodology was developed for checking the state of NCW readiness in the Land Force and applied it successfully to a collection of capabilities known as *LAND 5000*. This has been recently expanded into a NCW Prioritization and Integration (NPI) methodology used for detailed analysis of groups of projects or collections of capabilities in a joint force context. While useful for identifying cross-capability integration problems and risks, the NPI approach was not originally designed to check the compliance of individual projects. Development of the NPI continues.

Additionally, an NCW Risk Mitigation Review (RMR) Framework, referenced to an Australian instantiation of the SLC process, was developed to determine “the level of risk of a project not achieving a required level of NCW integration”.[12,13] In the absence of an agreed NCW architecture or Technical Reference Model (TRM) for Australian Defence, the RMR Framework may be used to assess cross-project interactions and the NCW characteristics of a project. When complete, the framework would include an assessment of the project’s Fundamental Inputs to Capability (FIC)[14], i.e. all elements of capability to which the project contributes from a Systems-of-Systems perspective.

The NCW compliance process described in this report is based on the model proposed by Keus[15] and calls for the establishment of a reference model with agreed standards, rather than allowing systems to evolve without particular reference to a set of standards.

An NCW Enterprise Model

Keus (2005) has made significant progress towards defining the properties of a net-centric military force for which he has coined the term *netforce*[16]. He takes a Systems-of-Systems (SoS) approach and starts with the concept of providing adequate information for better situational awareness, self-synchronization and enhanced collaboration and then introduces the Network-Node Paradigm: “All entities in a net-centric operation can be regarded as nodes interacting with each other through a communications network.” This view is similar to that of McKenna et al.[17] who treat net-centric military systems as “a network of nodes and links where information is the key currency of exchange”.

Keus’s SoS approach may be summarized as follows:

- An NCW SoS comprises a reconfigurable group of nodes, where each node performs one or more basic functions (collection, information processing, decision-making, communications, taking action, providing support);
- Each node has some elementary properties that enable it to be modeled and connected in an NCW environment. These properties are defined as identity, status, capability, structure,

[8] US Department of Defense, *Net-Centric Checklist*, 2004.
[9] Dstl, *Distillation*, UK MoD, 2004.
[10] UK Ministry of Defence, *Network Enabled Capability*, 2005.
[11] Boyd, Williams, Skinner & Wilson, *SETE 2005 – A Decade of Growth and Beyond*, 2005.
[12] Richer, Kohn & Kingston, *11th ICCRTS*, 2006.
[13] Kingston, Richer & Kohn, *11th ICCRTS*, 2006.
[14] Director Capability Options and Plans, *Defence Capability Development Manual* 2006, 2006, p. 4.
[15] Keus, *10th CCRT Symposium*, 2005.
[16] Keus, *10th CCRT Symposium*, 2005, p. 3.
[17] McKenna, Moon, Davis & Warne, *Australian Defence Force Journal*, 2006.

control, security, integration and interaction. For legacy systems, a *wrapper* is required to enable interfacing to the network;

- Higher-level capabilities (such as situation awareness, collaborative planning, decision-making and cooperative action) emerge from the interactions between groups of nodes.
- Dynamic functions and services influence the behavior of the *netforce*. Keus (2005) proposes eight generic functions and services: Collector Management, Picture Compilation, Situation Evaluation, Effecter Assignment, Effectuation, Planning and Coordination, Resource Management and *netforce* Management.

The NCW compliance approach described in this paper is based on Keus's concept that NCW capabilities will emerge from the interactions between groups of nodes that are connected via a communications network. The distinctive feature of this compliance approach is the premise that a node (i.e. a system or specific acquisition project) will not exhibit net-centric behavior until it is connected as part of a *netforce*. Therefore NCW compliance should be checked in three stages:

1. Can the node (i.e. system or acquisition project) be connected, interfaced and integrated as part of a *netforce*?
2. What behavior will it exhibit as part of that *netforce*?
3. Will the *netforce* support the envisaged military activities?

To adequately encompass these considerations, an NCW compliance process can be established that is based on the three-layer NCW Enterprise Model shown in Figure 1.

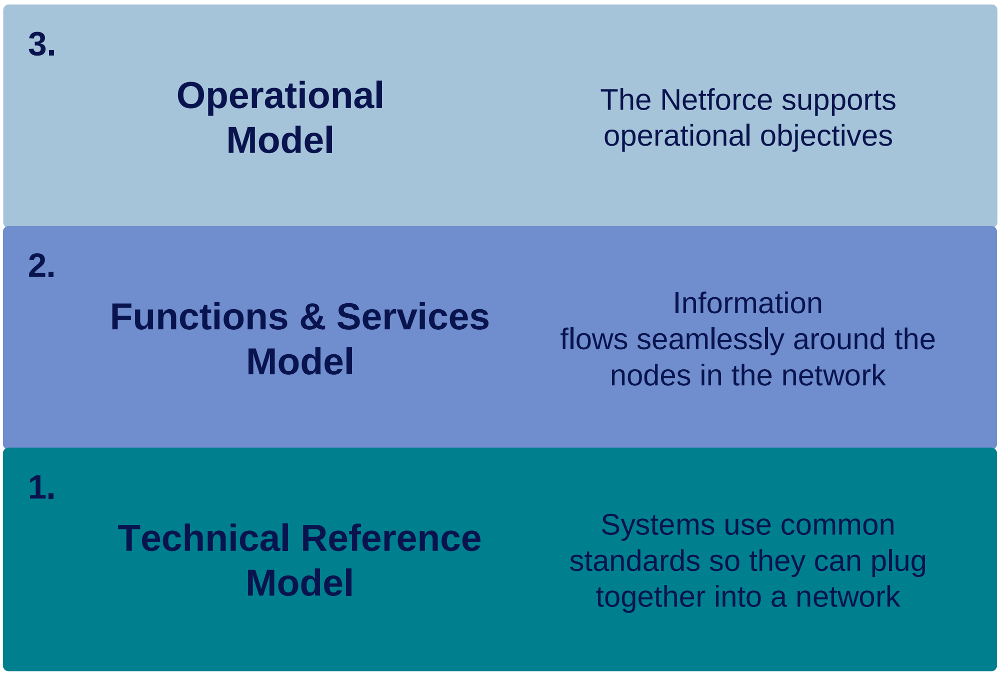
3.
Operational Model
The Netforce supports operational objectives
2.
Functions & Services Model
Information flows seamlessly around the nodes in the network
1.
Technical Reference Model
Systems use common standards so they can plug together into a network

Figure 1 - NCW Enterprise Model

The top layer represents the operational objectives of the *netforce* and includes strategic and policy guidance, and military objectives. The middle layer represents the essential functions and services (e.g. sensing, decision-making, tasking) that will provide the generic structures and emergent properties (e.g. situational awareness, collaborative planning and cooperative action) that support the military objectives. The bottom layer is a TRM for the envisaged force. Individual systems and projects that comply with the standards in the TRM should be compatible with one another, and therefore able to be connected more easily into structures that provide useful functions and services.

A way to think of the enterprise model is that the TRM guides the development of technical infrastructure for functions and services that support the desired military activities.

Structure of the Model

The Australian NCW Concept and Roadmap provide broad guidance as to the NCW behavior that would be exhibited by a Networked Joint Task Force (NJTF), assembled for a particular military operation. Systems and operational analysis techniques can be used to translate this NCW guidance for the whole-of-force into specific, measurable objectives. In particular, it is suggested that the top level of the NCW Enterprise Model would comprise specific NCW Principles, Roadmap milestones and target states for their achievement.

These NCW Principles can then be used to develop a SoS model for a *netforce*. This design approach would identify the architecture schema, characteristics and functional design attributes of the notional *netforce*. It would include a generic NCW functions and services model that could, for example, be based on a commander's sense-decide-act cycle.[18]

A *netforce* TRM could be developed to support the desired NCW functions and services. It would provide a common conceptual schema and vocabulary for guiding the integration of legacy and future systems into a *netforce*, with the aim of improving interoperability, portability, scalability and cost-effectiveness of materiel acquisitions. This approach of using a TRM provides a standards-based method for assessing technical interoperability.

In Australia, the establishment of an NCW TRM, and endorsed standards with which Defence projects should comply, is at an embryonic stage but the existing Australian Defence Information Environment (DIE) Approved Technical Standards List (ATSL)[19] provides an interim means for assessing technical interoperability.

Applying the Model

From an Australian perspective a *netforce* is viewed as a selection of capability components configured as a military task force that exhibits the desired NCW behavior. An individual military system with a defined capability may then only be expected to exhibit NCW behavior when deployed as part of such a *netforce*. However, individual systems should be *net-ready* so that they can be readily integrated with other military capabilities to be deployed as part of such a *netforce*.

A 'net-readiness' approach tests whether individual projects comply with endorsed *netforce* design principles and minimum net-readiness standards and that, *prima facie*, they are ready to be integrated without needing to develop new interfaces for them to interact with other systems in the *netforce*. This is contrasted with the more traditional system-centric approach in which customized one-to-one interfaces are developed to connect each pair of interacting systems.

In addition to checking for net-readiness, there should be an assessment of the net-centric behavior and performance of the project when it is integrated into a *netforce*. This NCW assessment stage would have links to existing Test and Evaluation (T&E) processes with overall net-centric behavior determined through a program of experimentation. These broader processes may be used to check whether the *netforce* as a whole will support the envisaged military activities.

Three broad stages have been identified for NCW compliance:

1. A net-readiness component to look at an acquisition project in isolation.
2. An NCW assessment component to look at each project in the context of other systems.
3. Experimentation to assess the overall behavior of the *netforce*.

[18] Moon, *Journal of Defense and Security Analysis*, 2007.
[19] Office of the Chief Information Officer, *ATSL*, 2005.

The following sets of NCW compliance net-readiness and assessment components are proposed (Table 1). While the four net-readiness components have already developed, further work is needed to develop the three assessment components.

Table 1 – Proposed NCW Compliance Components

Net-Readiness Components	
NCW Priority	Checks whether the project should be evaluated for its net-readiness. This depends on the type of system to be delivered, its information flows and its timeframe. The priority component is used as a filter, to identify acquisition projects that need to be checked for NCW compliance.
Other elements	Checks that the project has identified and addressed the impact of NCW compliance on all elements of a system including organization, doctrine, personnel, training and facilities.
NCW Traceability	Checks that the project's design and documentation support NCW guidance and provide a traceable path from NCW guidance to operational activities, system functions and services and then to the necessary technical standards.
Technical Interoperability	Checks that the project complies with agreed technical standards for data, information and network interoperability.
Netforce Assessment Components	
System Linkages and Information Exchanges (to be developed)	Would be used to identify legacy and future systems that will need to exchange information with the system under consideration. This component could also be used to prioritize those legacy systems for which a wrapper must be developed to enable them to interface to the *netforce*.
Netforce Design Component (to be developed)	Would be used to ensure that projects are consistent with *netforce* design attributes, e.g. architecturally and functionally consistent.
Experimentation and T&E Component (to be developed)	Would be used to test and assess the delivered capability's behavior in a *netforce* environment.

The main information sources that would be used to undertake NCW compliance checking include:

- The System Life Cycle processes as applied to materiel acquisition.
- Operational Concepts and Architectures developed for the systems under consideration.
- Function and Performance Specifications (FPS).
- Plans for Test and Evaluation (T&E).
- Requests for Proposal/Tender (RFP/RFT).

Particularly useful sources of information during the NCW compliance process are the architectural views (operational, systems and technical) and their supporting information. In applying this approach to NCW compliance, Requests for Tender (RFT) and Requests for Proposal (RFP) could be required to specify an appropriate TRM, the list of NCW-related standards to which the proposal complies and an assessment of the impact of any areas of non-compliance.

Ongoing Development

As technologies, international standards and NCW concepts continue to evolve over the next ten to fifteen years, it is important for NCW compliance processes to track and adapt to such changes. An NCW compliance process should thus be viewed as a learning model, so that it can be iteratively updated and improved. It should also include provision for adding compliance checks that would be introduced as NCW Principles and their supporting TRM evolve.

Embedding feedback loops within an NCW compliance process would facilitate review, particularly in response to:

- Changes to NCW policy and guidance (e.g. updates to NCW Roadmap).
- Changes to international standards and best practice in NCW.
- Lessons-learned from experimentation. In addition to triggering a review of whether the NCW compliance process is delivering the desired NCW capability, lessons-learned from experimentation might also trigger updates to strategic and policy guidance.
- Exception handling (i.e., where an acquisition project seeks exemption from a mandated technical standard).
- Feedback from users of the NCW compliance process. A Master Question List (MQL) could also be developed to check that users are receiving appropriate support from each stage of the process and to elicit their suggestions for improvement.

Regular reviews of the compliance process should, however, be undertaken to ensure consistency with acquisition processes is being maintained.

Discussion

An NCW compliance process is about more than checking for information and communications systems connectivity. It must take into account other facets of military capability such as doctrine, structure and organization, personnel, collective and individual training and facilities. At the initial net-readiness stage, the focus may be on identifying high-priority NCW projects, implementing common standards and ensuring that project documentation demonstrates a traceable commitment to following endorsed NCW guidance. Later NCW assessment stages could test each system's ability to operate in a *netforce*.

As the flow of information is central to any future *netforce*, and the network enables the flow of information, the focus of the NCW compliance process should be on data compatibility rather than network connectivity. This has been described as an information-centric approach where:[20]

- A wider range of information will be made available more quickly to a wider range of decision-makers and
- Decision-makers will be able to access the information they need, duly processed and presented in useful ways.

Conclusions

This paper describes a three-layer Enterprise Model for NCW compliance. The distinctive feature of this compliance approach is the premise that a node (e.g. an acquisition project or system) will not exhibit net-centric behavior until it is connected as part of a *netforce*. Therefore NCW compliance should be checked in three stages structured around answering the following questions:

1. Can the node (system or capability project) be connected, interfaced and integrated as part of a *netforce*?
2. What behavior will it exhibit as part of that *netforce*?
3. Will the *netforce* support military activities as envisaged?

The NCW compliance process described here would initially focus on identifying the priority for, and checking the net-readiness of, individual acquisition projects or systems. This would involve checking that project documentation:

[20] Jacoby, *C4ISR Journal*, January/February 2006 pp. 14-15.

- Supports NCW guidance and provides a traceable path from NCW guidance to operational activities, system functions and services and then to the necessary technical standards.
- Identifies and addresses the impact of NCW compliance on all aspects of military capability from technology, through organization, doctrine and facilities to personnel and their training.
- Complies with agreed technical standards for data, information and network interoperability.

Further work is, however, required to develop NCW assessment components to:

- Identify key system linkages and information exchanges.
- Ensure a consistent NCW functional design.
- Assess each system's performance in a *netforce* environment by means of experimentation (including modeling and simulation).

Of prime importance for establishing a suitable NCW compliance process is the scoping of the operational context, identification of an appropriate functions and services model and development or adoption of an appropriate TRM.

References

[1] D.S. Alberts, J.J. Garstka & F.P. Stein, *Network Centric Warfare*, 2nd Edn, CCRP, United States, 1999, ISBN: 1 57906-019-6

[2] D.S. Alberts, *Information Age Transformation*, CCRP, United States, 2002, ISBN: 1 893723-06-2

[3] C. Boyd, W. Williams, D. Skinner. and S. Wilson, "A Comparison of Approaches to Assessing Network-Centric Warfare (NCW) Concept Implementation", *Proceedings of the Systems Engineering , Test & Evaluation Conference, SETE 2005 – A Decade of Growth and Beyond*, Brisbane, Queensland, 7 to 9 November 2005

[4] Capability Development Group, *NCW Roadmap*, Department of Defence, Canberra ACT, DPS: October/2005

[5] Director Capability Options and Plans, *Defence Capability Development Manual 2006*, Capability Systems Division, Defence Publishing Service, Department of Defence Canberra ACT, 2006

[6] Directorate of Future Warfighting, *Enabling Future Warfare: Network Centric Warfare*, ADDP-D.3.1. Canberra, Australia, March 2004, ISBN: 0 642 50184 X

[7] Dstl, "The NEC concept", *Distillation*, 3rd themed issue: Network Enabled Capability, UK MoD, 2004

[8] ISO/IEC 15288 - System Life Cycle Processes, URL: http://www.15288.com/

[9] L.E. Jacoby, "Info-centric operations: Intelligence collection, handling and analysis undergo fundamental change", *C4ISR Journal*, Vol. 5 No. 1 January/February 2006 pp. 14-15 URL: http://www.isrjournal.com/story.php?F=1229768

[10] H.E. Keus, "NETFORCE PRINCIPLES: An Elementary Foundation of NEC and NCO", *10th CCRT Symposium*, June 13-16, McLean, Virginia, US 2005

[11] G. Kingston, W. Richer and E. Kohn, ‘NCW Risk Assessment Theory’, *11th International Command and Control Research and Technology Symposium (ICCRTS)*, Australia, 2006

[12] T. McKenna, T. Moon, R. Davis & L. Warne, “Science and Technology for Australian Network-Centric Warfare: Function, Form and Fit”, *Australian Defence Force Journal*, Vol. 170 2006

[13] T.T. Moon, “Net-centric or Networked Military Operations?”, accepted for publication in *Journal of Defense and Security Analysis*, Vol. 23, Ed. 1 (scheduled for March 2007)

[14] Office of the Chief Information Officer, Defence Information Environment (DIE) Approved Technology Standards List (ATSL), Version 2.4, Australia, 19 Dec 2005

[15] W. Richer, E. Kohn and G. Kingston, “NCW Risk Assessment – Towards a Compliance Policy and Process”, *11th International Command and Control Research and Technology Symposium (ICCRTS)*, Australia, 2006

[16] UK Ministry of Defence, *Network Enabled Capability*, 01/05 C100, UK 2005

[17] US Office of the Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer, *Net-Centric Checklist*, May 12, 2004 Version 2.1.3, URL: http://www.defenselink.mil/nii/org/cio/doc/NetCentric_Checklist_v2-1-3_May12.doc

.