Cover Page

12TH ICCRTS

ADAPTING C2 TO THE 21st CENTURY

Title: Adaptivity Led Networked Force Capability

Paper #: I-200

Tracks
1. C2 Concepts, Theory, and Policy
2. Networks and Networking;

Authors:

Mark Unewisse
Defence Science and Technology Organisation
Australian Department of Defence

Building 81L
PO BOX 1500, Edinburgh SA 5111, AUSTRALIA
Phone: +61 8 8259 4237
FAX: +61 8 8259 5055
Mark.Unewisse@dsto.defence.gov.au

Anne-Marie Grisogono
Defence Science and Technology Organisation
Australian Department of Defence

Building 81L
PO BOX 1500, Edinburgh SA 5111, AUSTRALIA
Phone: +61 8 8259 6532
FAX: +61 8 8259 5055
Anne-Marie.Grisogono@dsto.defence.gov.au

12TH ICCRTS - ADAPTING C2 TO THE 21st CENTURY

Adaptivity Led Networked Force Capability

Tracks: 1. C2 Concepts, Theory, and Policy; or 2. Networks and Networking;

Mark Unewisse and Anne-Marie Grisogono

Point of Contact: Mark Unewisse
Australian Department of Defence
Defence Science and Technology Organisation
PO BOX 1500, Edinburgh SA 5111, AUSTRALIA
+61 8 8259 4237 / +61 8 8259 5055
Mark.Unewisse@dsto.defence.gov.au

Abstract

A significant fraction of the ten-year Defence Capability Program budget of the Australian Defence Force is focused on implementing an NCW-capable combat force. But what defines being NCW-capable? How do we network the force so as to develop significantly enhanced capability in increasingly complex and uncertain broad-spectrum operations?

In this paper, we will explore the hypothesis that engendering adaptivity in all its forms is the key to enhanced capability for complex operations, and that doing so should drive the networking of force capability. We will argue that this can be achieved through application of a previously developed conceptual framework for adaptation. All four classes and five levels of the conceptual framework will be addressed in an illustrative way. These will generate consequences for the topology and dynamic properties of the networks, for force organisation and C2 processes, and for how information is sought, managed and disseminated. Some issues, opportunities and risks arising from this approach to implementing NCW will be identified and discussed.

1 Introduction

Australia, along with many other nations around the world, is migrating to a networked force capability. Over the next 10 years the Australian Defence Capability Plan (DCP) is acquiring the building blocks for an NCW-capable force. These include a large number of projects that will deliver a new generation of network capable aircraft, ships, land systems (both platforms and individual soldier systems) and the underpinning networking infrastructure including communications, command and control (C2), and battle management systems. These new systems will bring with them a range of new and enhanced capabilities across the spectrum of firepower, precision, sensing, protection, mobility and supportability. However a major challenge will be to shape and integrate these individually optimised building blocks, plus a variety of legacy capabilities, into a more effective, survivable and adaptive force capable of meeting the challenges of future complex operations [FLOC 2004].

Networking is often proposed as the solution to the problem of integration as well as delivering potentially significant enhancements to force capability. However, what dimensions of enhancement will networking actually deliver and how will these enhancements be realised? These are the issues we address here.

Previous studies [Unewisse 2005] into force networking (particularly for the Land force) have indicated that the primary benefits from NCW will be realised by designing forces to utilise the new capabilities to effectively address higher levels of operational complexity. This has become a corner stone of the Australian Army's NCW concept [Army 2006a] and is aligned with the Army's Future Land Operational Concept – Complex Warfighting [FLOC 2004]. In this approach networked forces will be developed with the ability to:

- undertake more complex operations than previously, with similar forces and with acceptable levels of success and risk;

- achieve a greater degree of success in the same operations as previously, with acceptable levels of risk; and
- achieve the same or more successful outcomes in current operations at lower levels of risk.

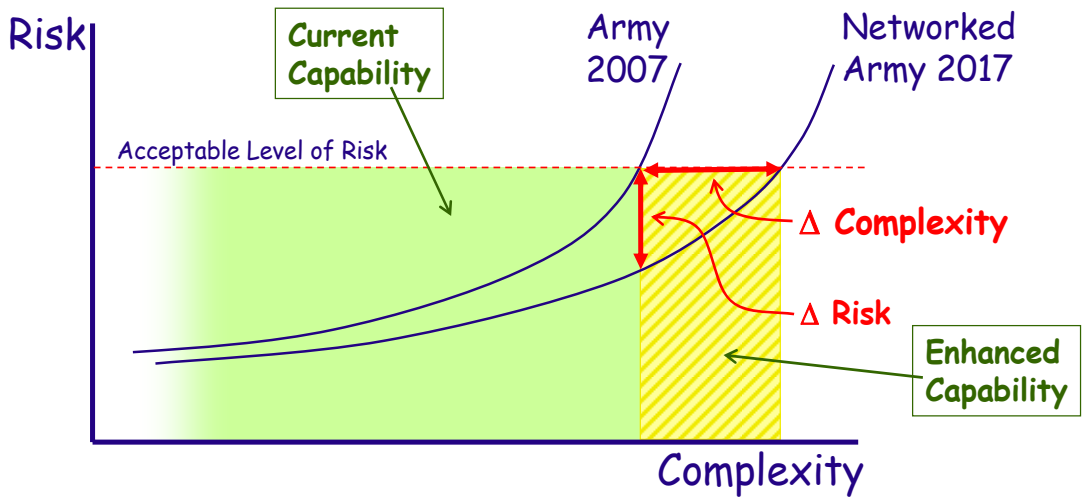

Figure 1: Illustration of the networking advantage hypothesis comparing the range of operational complexity at a given level of risk for the current force with the networked force of 2015.

This hypothesis is illustrated in figure 1, which plots illustrative curves of risk against complexity for the current force and a future NCW-capable force in 2015. Thus, the enhanced information sharing, situational awareness levels, coordination and synchronisation abilities of the networked force should increase the quality of the success that the force is able to produce, and thereby, the capacity of the force to cope with complexity. This will then provide a greater range of options to decision-makers, and enable the networked force to undertake missions and operations that would currently present too great a risk. Similarly, operations that would be currently viable could be undertaken at a lower level of risk.

In other words, coping with increased levels of complexity such as in urban operations, can be achieved in three ways: through reducing risk, through increasing the level of complexity which can be successfully dealt with, and through increasing the degree of success that can be achieved.

This is a different approach to many others described in the literature. The primary driver for NCW outcomes is no longer just increased effectiveness and speed in those missions and tasks it already does well, with potentially marginal improvements. Rather, the primary benefit from a networked force (as illustrated in figure 2) would be found in the enhanced effectiveness of the force in undertaking operations that are either currently highly challenging for our forces, or too difficult or at too high a level of risk to be considered.

This places the initial focus on more effectively undertaking missions and tasks required for complex operations, which are currently only partially or marginally feasible for the force to achieve. The next stage would develop the capacity of the networked force to undertake tasks that have significant potential to enhance its effectiveness in complex operations, but lie outside that scope of the current force capability (at least at acceptable levels of risk).

Given the need to develop force capability able to cope with higher levels for operational complexity, our thesis is as follows:

1. Enhanced adaptivity is the key to increasing the effectiveness of networked forces in both undertaking more complex operations, and in meeting the higher operational goals;
2. This enhanced adaptivity is achieved through a holistic and multi-scale approach, enabled by force-level design of an inherently adaptive networked force, which as a result, will be capable of:
    a. engendering needed adaptive characteristics while the force is being employed, and
    b. evolving to meet the dynamic challenges of the future battlespace over a longer timeframe.

The following sections will present a case for this thesis. Moreover, we will argue that the issue is not about designing a networked force on paper, and then going about an implementation plan of connecting the bits, but rather of employing a truly evolutionary process of force integration supported by iterative concept development, experimentation and evaluation, so that the capability grows in a

coherent and cost-effective way. For the bulk of the paper we will apply this thesis and utilise our previously published conceptual framework for adaptation [Grisogono 2005, 2006a, 2006b] to identify some of the key drivers, issues, opportunities and risks in developing an adaptive networked force.

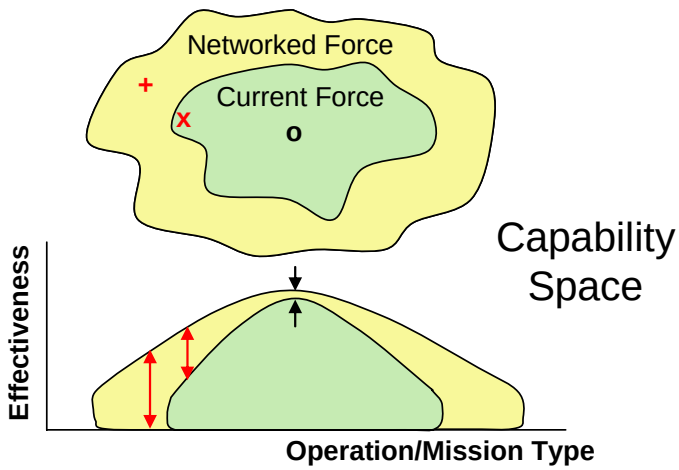

Figure 2: Schematic illustration of areas of current capability (green) and potential networked force capability (yellow), indicating that the primary enhancement will be gained for those missions at the limits of the force's current capabilities.

2 Adaptivity and Complexity

The challenge of working in complex environments is their dynamic, unpredictable and constantly changing nature, including changes brought about by other actors in the environment. Therefore the ability to adapt appropriately is absolutely fundamental to success in coping with those changes.

The essence of an adaptive response to challenges is that the system does not attempt to plan for every eventuality with a predetermined response, but has the capacity to generate new context-appropriate responses to new challenges.

This is essential in the face of complexity because the number and diversity of potential future challenges quickly poses an intractable problem in which planning for all eventualities becomes impossible on any reasonable scale of time, system size, or energy. One must therefore strike a balance between developing particular capabilities which have proved their worth in the past (which amounts to planning on tomorrow being somewhat like yesterday) and investing in the capability to adapt to the unexpected (which amounts to betting on tomorrow springing some surprises). The more complex the environment becomes, the more important is the ability to adapt, and the less reliant we should be on the continued relevance of what worked yesterday – in essence the challenge that underlies any defense transformation.

The defining characteristic of adaptation is that the system 'learns from experience' – by which we mean that information drawn from past successes and failures is somehow incorporated into the system so as to tend to increase its probability of future success. Of course, success is never guaranteed – however inability to adapt in the face of significant change is a surefire recipe for failure.

There are many forms that adaptation can take and when it works well, it results in new capabilities, new strategies and new behaviors that improve the system's success. Nevertheless there are still many ways it can fail. It is very important therefore to understand adaptation, to really explore how it works, how it fails, and how and where we may harness it.

This is the thrust of the conceptual framework for adaptation, more fully described in [Grisogono 2005] , which we will draw on extensively in this paper, and which we briefly outline below. We also acknowledge earlier work (Bar-Yam 2006, Braha 2006) which laid pioneering groundwork for some of these approaches.

2.1 Conceptual Framework for Adaptation

The framework is based on the most basic concept of a (complex) adaptive system as having the capacity to sense and act conditionally on its environment as a result of what is sensed, and a generic model of adaptation, which comprises the four essential components of:

1. an internalised concept of ‘fitness’ or relative success and failure,
2. a source of variation in some parts of the system,
3. a means of testing the variations produced for their impact on fitness, and
4. a selection process which preferentially retains variations which enhance success and discards those which lead to failure.

Continuous cycling through 2,3 and 4 results in the encoding of information into the system, in a way that tends to increase the relative success of the system.

Examining the various ways in which such a generic model can be instantiated has led us to a number of classifications for specific examples of adaptive mechanisms:

- whether it operates on individual systems (as in individual learning) or on populations (as in evolution of species),
- what parts of the system are subject to adaptation – leading to five nested levels of adaptivity, which we describe as:

  Level 1. Action-in-the-world – tuning existing sensing, processing and action capabilities;

  Level 2. Learning – expanding or modifying existing capabilities to improve success at Level 1;

  Level 3. Learning-to-learn – improving how Level 2 is done, to increase effectiveness of learning;

  Level 4. Defining-Success – improving the alignment of the internalised success and failure criteria in the selection process with ‘real’ success, and

  Level 5. Co-Adaptation – with two parallel and interwoven threads:

  - for those systems within our own control – tuning the allocation of roles and resources to them in a System-of-Systems context, and
  - for systems we interact with but do not control, choosing our options with a better appreciation of their consequences through anticipating their likely adaptive responses to our actions.
- what kind of change or stress is the adaptive mechanism targetting – leading to four classes of adaptivity which we describe as:

  Responsiveness – ability to recognise and deal effectively with immediate threats and opportunities as they arise,

  Agility – ability to recognise when changes in the context or in system capability require a change of strategy, and to implement it easily,

  Flexibility – ability to recognise and deal effectively with new challenges, i.e. to be reconfigured in different ways to do different things, under different sets of conditions, and

  Resilience – ability to recognise and deal effectively with harmful changes to the system itself i.e. to recover from or adjust to misfortune/damage, and to degrade gracefully under attack or as a result of partial failure.

  The outcomes and characteristics of these classes from the perspectives of an enemy, the owner of the force, a partner, and an operator within the force, are summarised in a table in Appendix A;

and finally,

- the scale at which it operates.

These classifications offer a rich matrix of templates for possible adaptive mechanisms which we can use to either recognise, analyse and tune existing mechanisms, or to identify and exploit opportunities for engendering new ones.

To complement these classifications, and to assist in creating effective interventions to improve the success of existing adaptive mechanisms, or in the even more difficult task of engendering new ones, the framework also addresses how to assess and tune:

- the integrity and ‘health’ of adaptive mechanisms (i.e. what Level 3 should target),
- their temporal dynamics in relation to relevant processes in the environment (in the context of a multi-scale analysis), and
- whatever other factors will influence their degree of success or failure.

2.2 Scales of Application

Judicious use of networking and integration certainly has the potential to enhance the effectiveness and adaptivity of individual force elements and small teams. While force elements at these scales are

generally already inherently highly adaptive, more effective information sharing can enhance their responsiveness and their ability to align their actions with other force elements. However, we argue that the largest payoff for implementation of NCW is through engendering adaptivity of military forces at the higher scales of application, where modern western forces rarely display the level of adaptivity that they claim to need.

Guided by the classes and levels of adaptivity identified in our conceptual framework for adaptation, we will propose the necessary sharing, and appropriate management, of information, together with changes in processes, structures and operational concepts at these higher scales, required to engender adaptive mechanisms to enable coherent adaptive actions generating synergistic effects, across all relevant scales of the operation. This will be the main focus of this paper.

3 Designing for Adaptive Networked Force

In the main the design of networked forces has tended to focus on the design of component networked systems and on information systems standards that will enable a base level of systems interoperability. However, a networked force is more than just a collection of locally optimised parts that will somehow automatically integrate to deliver an effective force. It is a force-level system-of-systems operating in dynamic and stressful environments. As such it requires active design and the associated trade-off decisions in order to effectively integrate and function as a coherent system [Unewisse 2006].

3.1 Force-level Design and Capability Development

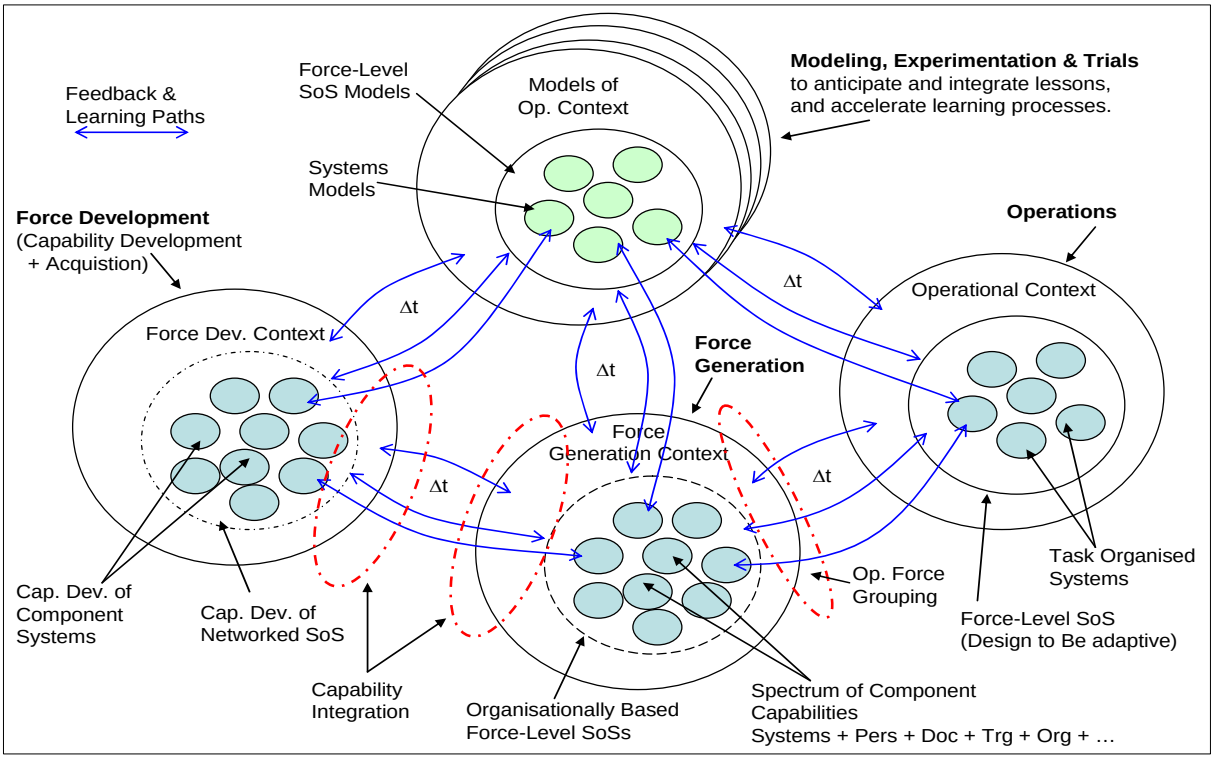

Figure 3: Simplified schematic of the capability development and implementation process showing the stages from systems acquisition by projects to actual force level operational capability. It also highlights the potential of modelling and simulation to accelerate the learning processes to enable a more adaptive capability development process.

A schematic of Australia's capability development and implementation process is illustrated in figure 3. Although simplified, it still provides some insights to key stages of networked force design and development and some of the key learning and adaptation processes involved. Each of the 4 identified elements in figure 3 is described as a number of associated components that form (or at least potentially form) a higher level system-of-systems. Surrounding each is a context within which they view and interact with the world. There are also feedback loops between the 4 elements of the model,

each associated with a range of time constants that reflect lags in adaptation and learning. The 4 primary elements are:

1. Force Development: The force development component incorporates the entire capability development and acquisition process. It fuses together two separate stages of the Australian acquisition process, namely capability development - identification and definition of major systems requirements, and material acquisition – acquisition of actual systems against the requirements.

   The core components of force development are the individual projects that deliver the systems that will form building blocks of the future force. In general projects deliver systems as locally optimised stovepipes. Consideration of the integration of the systems into components of a larger system-of-systems is often limited to mandating of a variety of technical interoperability standards. Design of these systems as parts of a larger force-level capability is still emerging at this stage Unewisse 2006].

   The capability development context is driven by predictions of future warfighting environments, high-level concepts, and a historical tendency to linearly build on the major systems that have traditionally been in place. The context is also strongly driven by the need to address financial considerations. As a result, the overall force development process can exhibit a tendency towards risk aversion, particularly outside the individual project stovepipes.

   Effective learning interactions with the other model elements could improve functioning of the capability development context, and will be needed to establish a force-level view of force development. If these feedback paths are not effectively implemented the context can, particularly in times of relative peace, become increasingly removed from the lessons and realities of the operational world. This can be manifested as efforts to become increasingly "efficient" at the expense of overall force flexibility and effectiveness. A further difficulty is the relatively long timescales of traditional force development processes, often struggling to keep pace with the in flow of lessons and feedback from the other model elements.

2. Force Generation: Once the warfighting systems and platforms have been acquired, they need to be transformed into viable warfighting capabilities with suitable trained personnel, organisation, doctrine and TTPs, collective training, and so on. This process generates elements of warfighting capability that are in turn able to be delivered to the operational world.

   In general the system-of-systems level within this element is based on standard military organisational structures focused on the raising, maintaining and training of the forces. The force generation context tends to be driven by a combination of doctrine and the incorporation of lessons learned from operations. These and other feedback links are essential to ensure that the force generation processes deliver warfighting capabilities that match the operational needs. Higher operational tempos tend to have the dual impact of stressing the force generation processes and providing greater learning and feedback opportunities. However, the learning and feedback links also need to extend back to the force development element.

3. Operations: The warfighting capabilities provided by the force generation element are then task organised to meet the requirements of the operation. These task organised teams are the building blocks of the force-level capabilities that will undertake the challenges of the operational context. The nature, scope and scale of the teams will vary across operations, and must adapt to deal with the dynamic challenges the force may face.

   Through the feedback and learning paths (shown in Figure 3) across the development process. and connecting the contexts, SoS levels and component capabilities of each of stage, lessons learned in the operational context will influence the force generation context and more indirectly the capability development context. Similarly, lessons on the force level SoS and the component networked capabilities will be shared across the development process. Unfortunately there is usually a significant delay in capturing and applying the lessons from on stage to another. In particular, there has been a historic tendency for a significant delay between the realities and lessons learned in the operational context to filter back to the force development let alone the capability development stages.

4. Modelling, Trials and Experimentation: A modelling, trials and experimentation (MTE) capability is an essential component of the overall adaptivity of the capability development and implementation process. It provides an ability to test and explore options in order to assess their potential impact on success or failure, as required in step 3 (Section 2.1).

   MTE capability provides the operational context with rapid turn around insights to accelerate the understanding of the operational context and support the insertion of new concepts, tactics and systems to address operational requirements.

The services provided to the force generation and capability development stages tend to be more orientated into the future and harness the ability of a range of modelling, simulation and trials approaches to anticipate future requirements and challenges for the operational force. In periods of low operational tempo this capability can play a central role in ensuring that future force capabilities are not focused on winning the last war. In periods of high operational tempo, the capability provides a complement to the lessons from the field, and assists in ensuring that the forces are able to address a broad range of military operations. The system level components of the MTE element are models of the individual systems and force elements. These are then grouped into system-of-systems models describing force level capabilities under investigation. Unlike the other elements in figure 3, the MTE element has multiple distinct contexts. These contexts vary with the problems, scale and timeframes being investigated, ranging from relatively realistic simulations of current battlespaces in support of operations, to multiple future models of possible operational contexts to explore options and impacts in support of the force development and force generation stages.

3.2 Approaches to Networking

There are a variety of approaches that might be taken to the design of a networked force. In a highly stable battlespace context, with known adversaries, environments and tactics a classic top-down system engineering approach to the implementation of a networked force might be effective. In such a context most of the design degrees of freedom would be concentrated in the systems acquisition stage. The drivers for adaptation would tend to primarily come from advances in technology, with relatively minor changes to force generation to adapt the doctrine, TTPs and training to take advantage of the new technologies. Adaptivity within the operational force would be limited to low level tactical applications and immediate responses to the battlespace. This design approach is often a legacy of Cold War attitudes and has frequently influenced approaches to force networking.

A different approach is needed to address the challenges of an increasingly diverse and complex battlespace (as is now faced in most theatres of conflict). In this approach we need to design for far higher levels of adaptivity in both the force generation and operational contexts. This will result in a significant increase in the degrees of freedom provided in both these contexts, with a consequent increase in the potential for adaptation. Operational commanders will have greater options at their disposal to adapt to and learn from the battlespace. Similarly, force developers will have greater freedom to responsively adapt force doctrine, TTPs, training, etc. to maintain success with a co-adapting operational context.

However, a balance is needed between an increase in operational adaptivity and force effectiveness. Appropriate design decisions need to be made at each the 3 capability development stages so that commanders are provided with greater degrees of freedom, without burdening them with large force integration and design problems while trying to conduct operations. Thus, we need to design for the maximum level of force adaptivity at each stage of the capability development process that is still consistent with high levels of force effectiveness.

Networking capabilities can support both increased scope for adaptivity and the maintenance of high levels of effectiveness. This will require appropriate design of the networked force to harness the potential of networked systems to enable higher-scale adaptive mechanisms by linking their essential elements, and to support decision-makers everywhere by better sharing, management and exploitation of information (including lessons learned), facilitating their distributed collaboration, and connecting them to essential reach back services.

The end of the cold-war and the ever accelerating pace of technological innovation are forcing nations around the world to move from individually stovepiped acquisition projects to integrated force development programs (such as US Army Future Combat System program) or major subsets of force capability (such as the UK Future Rapid Effects System program). These require development of processes, procedures, systems and culture to enable ongoing evolution of their components, force-level systems-of-systems and contexts for force development and generation. Thus, the approaches to networked force creation must be adaptive by nature to remain both responsive and relevant in their ability to deliver future networked force capability.

The following sections will primarily focus on the operational context and addresses some aspects of the force generation and force development contexts, drawing primarily on insights from our work undertaken in support of networking Australia's Land force capability.

3.3 Current Force Adaptivity

Adaptivity is not new to military forces. Millenia of military operations have evolved current military forces with a range of adaptive mechanisms and processes, including:

- Hierarchical command structures providing the ability for forces to simultaneously operate at, and adapt across, multiple physical and temporal scales, so that while lower level forces respond to immediate combat pressures, senior commanders can be shaping the longer term battle;
- The mission command concept facilitating local initiative and adaptation within the context of an agreed framework of command intent and the forces allocated to the commander;
- Training as both the mechanism to forge personnel into responsive and robust teams, and one of the key vehicles to test and explore new ideas within the context of existing doctrine;
- Capture of 'Lessons learned' as the primary mechanism for insights from the operational context to be disseminated across the force and to influence both the force generation and capability development stages;
- Modular forces enabling commanders to rapidly combine elements to generate forces for various missions and to dynamically adapt force groupings to adjust as required to the battlespace;
- Redundancy in both organisation and equipment enhancing force resilience to enemy actions and environmental factors, as well as providing increased capacity to cope with unforseen events;
- Specialisation enabling concentration of skills which can then be integrated to form elements of task organized teams; and
- Multi-roling in the design of systems and in training engendering increased robustness of forces that must cope with losses due to the impact of an enemy or the environment.

We acknowledge that in designing more adaptive networked forces it is important to build on these mechanisms and processes.

4 Adaptivity Insights within the Operational Context

The increasing levels of operational complexity faced by future networked forces places a significant premium on force adaptivity. Although the scope of available options and timeframes varies significantly, this need for greater adaptivity applies from the lowest tactical levels to the strategic domain.

A number of opportunities for force adaptivity can be found in the operational context. The component capabilities need to be task organised into integrated joint and combined arms teams to meet the mission requirements. These task organised teams will constitute force level systems-of-systems (ranging in scale from combat teams through to task forces) that will need to adapt to the challenges of the operational context.

Understanding and influencing this context (both directly though combat or via more subtle mean) will also offer opportunities for force adaptivity. This adaptivity will be manifested in the way forces undertake and implement: planning; orchestration; decision making; coordination of manoeuvre; synchronisation of fires; information capture, filtering, processing and dissemination; teaming; training; and a range of administration and support functions. It will also include how operational forces deal with lessons learned within the operation.

4.1 Responsiveness – recognise and deal effectively with immediate threats and opportunities

For obvious reasons, military forces have evolved to be highly responsive to operational challenges. Further improvements to responsiveness can come from better sensing and discrimination of threats and opportunities, better choices of response, and a better range of responses from which to choose. In the context of improving responsiveness, the principal benefit of networking is to facilitate drawing on the most appropriate response from a wider palette than a non-networked force could access.

While timeliness is only one of the qualities that pertains to these factors, it seems that much of the NCW literature has focused on the potential of the new networking technologies to enhance the speed of force responsiveness. Consideration must also be given to the actual military benefit of making things faster. Some functions and actions, such as the responsive application of fires, will potentially be greatly enhanced through an increase in tempo. However, simply speeding up processes may provide very limited impact on war fighting effectiveness if the processes being accelerated are already providing timely responses, if tempo is limited by other factors, or if associated processes are not suitably co-adapted. In fact speed is not an end in itself – the timescale of response must be matched to the timescale of the situation being responded to. In some cases it may even be better to slow down.

4.1.1 Implications for networked force design

Consideration of how to enhance force responsiveness through all five levels of adaptation leads us to a number of insights concerning not just force networking, i.e. what connections are needed, but also what other changes are required for integration into a responsive and effective force.

Level 1: Action: - *tuning existing sensing, processing and action capabilities*

- Mission command is essential to ensuring that the opportunities for adaptive action are available throughout the networked force. Networking can support mission command through allowing direct command intervention by exception when necessary – the danger to be avoided is the inhibition of adaptive action through too-frequent micromanagement .
- Within the mission command context and Effects Based Approaches to Operations, networking can support choosing of mission objectives to take into account the broad range of effects that actions may generate and how these may contribute to, or impact upon higher level operational intents.
- Networking supports vertical alignment of effects by allowing higher commanders to monitor effects generated and adapt higher level strategies and tactics to either build on or moderate these effects.
- Decision support tools within the networked force need to be able to be shaped to the needs of commanders as they adapt to the changing requirements of the operation. Where possible this should occur automatically, but still guided by the commanders requirements.
- Networked battle management systems and processes enable decision-makers to draw on relevant information for adaptive action, and to choose actions from the full spectrum provided by the force.
- Networking enables rapid, comprehensive collection and dissemination of blue situation awareness to support commanders in effective adaptive actions, while minimising the risk of fratricide.
- Networking can accelerate the provision of joint and coalition fires by rapidly passing the targeting, blue force and other collateral, and battle damage information between the sensors, controllers and effectors in the battlespace.
- Networked intelligence systems tools and processes permit quality and speed of intelligence generation and its appropriate dissemination within the tactical force, utilising automated tools, meta-data, filters, fusion engines, decision support tools and reach-back services as appropriate, in the context of suitably-modified information management processes and policies.
- As network capacity will often be a limiting factor, the networking systems must be dynamically managed, through both information management and adaptive network management to ensure maintenance of force responsiveness under high network loads. [Shoubridge 2007].

Level 2: Learning: - *expanding or modifying existing capabilities to improve success at Level 1*

Level 2 encompassess improvements to all of the above systems and processes that support Level 1, and includes training and capability development. In the operational context considered here we focus on aspects that can be implemented in theatre, or are intended to directly support operations, and make the following observations:

- Networking should facilitate the timely provision of relevant feedback to support individual learning by all decisionmakers from their own and and others' actions, and
- should support their adaptation of teams, approaches, and tactics as a result.
- Networking can support distributed in-theatre training and mission rehearsal to increase the proficiency of the forces for adaptive action once execution begins.
- Networking can support rapid technology insertion programs in-theatre to target identified deficiencies in forces' abilities to sense, decide and act responsively, and to enable dialogue and collaboration between operators and capability developers for faster and more effective outcomes.
- Networking enables dynamic teaming and therefore amplifies the need to take a team and team-of-teams perspective within the operational context, and to improve the ability to team. This in turn will require collection of appropriate team performance metrics to assess their effectiveness and support their learning.
- Further development of networked battle management systems and processes to improve quality of decision making, should focus on automation of functions where appropriate, so as to free decision-makers to concentrate on higher-level issues and decisions.
- Networking and information technologies can support collection and analysis of lessons from operations, eg through distributed After Action Reviews, to both identify first order insights, and to extract trends that can help anticipate enemy actions and thereby, assist effective adaptation of current forces, tactics and approaches.

- Development of networked information management processes to dynamically provide decision-makers with appropriate information in the operational context [Coombs 2005, Hayes-Roth 2006].
- Networking enables reachback support services to augment intelligence and analysis of lessons learned, to improve decisionmakers' responsiveness and understanding of the operational context.
- Improving how information and uncertainty are handled can reduce risk of unwarranted confidence in displayed information.
- Since networking supports a wide range of approaches to coordination, synchronisation and delivery of fires (see force generation section below), commanders will need to learn when the different modes are appropriate within the operational context.

Level 3: Learning-to-learn: - *improving how Level 2 is done, to increase effectiveness of learning*

Networking can support efforts to change and improve the way learning is undertaken within the operational context. When the ability to learn is improved, one expects to see better outcomes from the learning, here in the form of more rapid and effective enhancement of networked force responsiveness. However Level 3 is generally under-recognised and under-exploited. The following illustrative suggestions for Level 3 implementations will require support from networking as well as from information technologies and other aspects:

- Reviews of training effectiveness leading to improvements in how training is conducted;
- Reviews of effectiveness of how lessons learned are captured, analysed, managed and disseminated leading to better use of those lessons to enhance force responsiveness;
- Reviews of effectiveness of technology insertion programs to improve their impact on force responsiveness; and
- Reviews of the effectiveness of linkages between learning in the various contexts (operational, force development and force generation - see figure 3) to improve overall force learning ability.

Level 4: Defining Success: - *improving the alignment of the internalised success and failure criteria in the selection process with 'real' success*

This level aims to reduce the frequency of situations in which "we won the battle, but lost the war". Such unfortunate outcomes spring from the difficulty of choosing appropriate mission objectives (which become the internalised success criteria for the mission), to effectively contribute to achieving the longer-term strategic objectives (which we here identify with 'real' success). This difficulty stems from the complexity of the operational context, and the opaqueness of its causal and influence networks [Grisogono 2007], and requires both adaptivity and an Effects Based Approach [Smith 2006].

Because of the different timescales over which mission objectives and strategic objectives materialise, it is only possible to implement Level 4 adaptation with hindsight, or through historical analyses of similar operations. Nevertheless, it is important for future success to put such processes in place.

As one example, care will need to be taken not to confuse measures of force effectiveness with efficiency measures. Networking capabilities will be able to collect large amounts of information, particularly on costs and overheads. Unless solidly embedded within metrics to assess mission effectiveness these can be misused (particularly in peace time) to significantly constrain force options and adaptivity available to commanders.

Level 5: Co-Adaptation: - *tuning allocations of roles and resources to our systems in overall force context, and choosing actions in awareness of likely adaptive responses by others.*

Operating at Level 5 requires local action to be informed by more global or wider views of what is happening, both within one's own forces, and in the entire context. Historically this capability has been available to limited extents only at higher commands. Networking offers the exciting possibility of co-adaptive responsiveness throughout the force, by better information to support local decisions (already discussed above), and by expanding the scope of decisions that can be supported because of an improved ability to identify and solve problem or conflicts those decisions might create.

4.2 Resilience – recognise and deal effectively with harmful changes to the system, recover from misfortune or damage, and degrade gracefully under attack or as a result of partial failure

Military forces must be resilient if they are to function effectively in hostile battlespace environments.

Future complex warfighting operations will tend to increase the risks faced by military forces. Operations will range across nation states, ethnic conflicts, counter insurgency, and nation building, often complicated by the need to integrate with a variety of joint, coalition, interagency, UN and non-government organisations. Forces must be designed to be inherently robust and be able to adapt rapidly to remain effective despite damage to key elements of the force. This has traditionally been

achieved through a combination of protected systems (e.g. armour), equipment and force redundancy, cross training of personnel, and a capacity to regroup to adjust to force losses.

While networking offers potential to greatly enhance force resilience, it can also be the source of dramatically increased force vulnerabilities. Thus, it is vital to identify these strengths and weaknesses and design the networked capabilities so as to build on the former while managing the latter.

The operational context will set the resilience requirements that the force generation and capability development stages will need to provide. During operations, resilience depends on how effectively the networked force can adapt its capabilities to deal with battlespace stresses.

4.2.1 Implications for networked force design

Consideration of the advantages and risks of networking, and their implications for force resilience lead us to a number of insights concerning force networking and integration. Most of the points below reside in Level 1 or Level 2, and as was the case for Responsiveness in the preceding section, there are many unexploited opportunities for increased resilience through more comprehensive expoitation of all five levels of our framework. This discussion would have benefitted from being couched in those terms, but that will have to wait for a future occasion. For the present, the insights presented here are grouped in terms of potential benefits and vulnerabilities of networking.

- The emergence of adaptive and / or ad hoc networks creates the potential for operational forces to more flexibly connect to each other and to cope with any localised impacts of either enemy action or the environment. Thus, networks can be more resilient to degradation and forces can be dynamically task organised to cope with the impact of the battlespace. Of course this only will work if the technological potential is coupled with appropriate doctrine, TTPs, training and culture to enable the warfighters to realise and apply this potential.
- The ongoing development and implementation of adaptive information management and policies is critical if the capability to exchange data is to be converted in the effective exchange of knowledge. The information management processes and policies (generally in coordination with network management) will need to be designed to manage the dynamic variation in user demand including the prioritisation, aggregation, fusion and filtering of information. This will ensure that highest priority information get to where it is needed and the available capacity is most effectively utilised. Similarly, information management must cope with variations in communications capacity.
- Processes and procedures need to be developed to deal with uncertainty in the information and the perpetual fog of war. Therefore networked forces and their supporting tools and processes need to take the degree of uncertainty into account in the information being used. An approach based on management of diversity, where primary interpretations of information are supplemented by alternate interpretations, can position planners and warfighters to be better attuned to risks to the force, and to rapidly invoke resilient responses, should their initial interpretations prove in error.
- Networking permits distributed forces, enabling them to concentrate their effects while reducing their vulnerability to attack through reduced footprints to enemy sensors.
- Networked forces (particularly in Land operations) need to be able to function autonomously, both to cope with the impact of enemy action or the environment and to enable them to function should they choose to break or minimise their links with the rest of the networked force (e.g. signature minimisation by special forces). Mission command is a key tool in achieving this. However, it must be coupled with processes, procedures and suitable tools to enable all key data to be held across the distributed force. If this information is pre-positioned, it has the dual advantage of increasing the robustness of the force and minimising the need for dynamic information exchange. The network force must also be able to reintegrate the force elements that have been and ensure that appropriate data replication occurs on rejoining the network.

In addition consideration must be given to designing the networked force to guard against the potential risks and vulnerabilities of networking with the potential to degrade force resilience, such as:

- Increased reliance on networking means that network failures can have devastating consequences, especially if they fail catastrophically. For networked forces to function effectively in challenging operational contexts, networked capabilities need to be able to degrade and integrate gracefully. This requirement will be discussed further in section 5.
- Networks are vulnerable to enemy attacks, random failures and environmental degradation. As networked capabilities will be increasingly critical to the functioning of the future force, they need to be both robust and adaptive to ensure that the required quality of service is maintained.
- Networking creates the potential to move to a centralised decision-making model, which may appeal to some commanders by offering the opportunity of applying their greater experience to

apply direct control low level tactical missions. However, most complex operations (particularly in the Land context) are characterised by a large number of parallel tasks and missions all of which need rapid highly parallel decision-making. This can not be provided by a central commander no matter how advanced their networks may seem. To centralise this decision-making would be akin to replacing the parallel decision-making of a free enterprise economy with a command economy on the basis that we now have better information systems. For some high impact missions, central control has its place, but it should be considered as a 'by exception' approach.

- The rationale for networking forces includes trading-off reduced conventional protection (armour, concentration, etc) for a compensating network-derived information advantage. However the risk is that disaggregated networked forces have increased vulnerability to targeted enemy action, particularly in complex Land operations. Resilience therefore requires operational commanders to adapt their strategies to reduce these risks, for example through designing networked systems to support rapid teaming of force elements and/or effects to respond to any such localised attacks.
- A lack of interoperability is a major risk area for the implementation of networked forces. This spans the domains of physical, technical, semantic and process interoperability. Most interoperability issues are best addressed at the force development and force generation stages to ensure maximum potential for force interoperability. However, legacy systems and multiple competing standards often result in operational commanders being given force elements with less than ideal interoperability. These operational commanders will then need to put in place processes and procedures to enable their forces to work around these limitations. The impacts of mixes of networked, partially networked and non-networked (legacy) systems is as yet not well understood and is an area of current research in DSTO [Pratt 2007]. These difficulties are of course greatly compounded with the impact of joint, multinational and interagency operations.
- Poor information management processes, procedures and systems may result in a range of critical problems, including information overload, inability to extract signal from noise, 'one size fits no one' standards of information such as inappropriately aggregated blue situation awareness data being provided at levels of resolution that do not support decisionmakers' needs.
- An assumption of 'information superiority' can be very dangerous if planners assume that they know more than the enemy about what is usually the enemy's backyard because they have a 'sensor grid' and information networks. This can reduce the active management of uncertainty, limiting the provision for unforeseen circumstances. This can in turn lead to highly fragile plans and a general reduction in force resilience.
- Highly networked forces will generate large electromagnetic signatures, increasing the visibility of the force and providing avenues for attack. Management of these signatures will need to be actively undertaken as a part of the operational context. High electromagnetic signatures of a networked force will also impact on civilian systems. In all out warfare this may not be an issue, however, in operations other than war it will be necessary to control the impact on civilian systems as these will generally also need to function in order to meet operational aims.

4.3 Agility – recognise when a change of strategy is required, and implement it easily

The most critical metric of agility is that the networked force maintains a high level of effectiveness no matter what unexpected hostile or circumstantial changes occur. From the perspective of an adversary, the force's agility means that he is unable to capture and maintain the initiative, or to come up with options that cannot be countered – an agile force slips out of his grip like water (see Appendix A).

The ability of networked forces to switch rapidly from one focus or mode of operation to another as the context requires, is critical in dealing with complex operations. This concept was first described by the US Marine Corps as the Three Block War [USMC 1998][*], but has more recently been considerably developed in the Australian Army's Adaptive Campaigning concept paper [Army 2006b] and is extensively discussed in a companion paper [Grisogono 2007].

In its earlier form, it was a key element of the characterisation approach developed to assess the NCW readiness of Australian Land NCW capability [Unewisse 2004], covering the need to be able to move sequentially from one mode of operation (e.g. humanitarian relief) to another (e.g. close combat operations) in a short period of time. The Adaptive Campaigning formulation of the concept might well be dubbed the 'Three Block War on Steroids', and encompasses the ability to operate concurrently in five different modes (now called Lines Of Operation in Adaptive Campaigning), with different balances of effort across them in different regions of the operational environment, and with both the balances in,

[*] "Three Block War." – USMC description of the need for forces to undertake a wide range of operational functions either concurrently or within a few hours/days, ranging from humanitarian relief through to lethal conflict within three city blocks.

and the boundaries of, the regions changing over time. As a result, the agility challenge is now to balance and manage the flow of limited resources across Lines Of Operation in space and time, and adjust local courses of action accordingly in order to achieve the 'best' overall success outcomes.

Various approaches to enhancing force agility are possible:

- Historically, agility has been based on centralisation of decisionmaking power, with other force elements subordinate to them. This facilitates agile changes to strategy, or course of action as required by the dynamics of the situation, provided adequate means exist to know when a change is called for, and to communicate the change required to deployed forces that are already executing the current course of action. These conditions are not easily met, particularly in the absence of pervasive networking, mission command and a reactive force posture. As a result, central commanders sometimes judged it less risky to persevere with a strategy that was clearly no longer the best choice, than to attempt to change it.
- A decentralised approach on the other hand, might achieve force agility through drawing on highly parallel and distributed local knowledge to test for the continuing validity of critical assumptions and conditions, and might then develop appreciation of the needs and options for change through collaborative interactions between the key decisionmakers, who are then also responsible for facilitating implementation. Such an approach might ultimately be expected to be far more robust and effective in creating and maintaining force agility under a wide range of stressful contingencies, but would require an extensive adaptive implementation process to allow the needed competencies, structures .and processes to evolve.
- Intermediate C2 modes such as mission command utilise the capabilities of networked forces to combine high-level shaping and orchestration of the force with distributed decision making to deliver the tactical effects. Agility could then be fostered through appropriate interactions between the shaping and the execution levels, but would also need to evolve in an iterative implementation.
- For complex operations in a joint / land context, a primarily or largely decentralised approach based on mission command is likely to permit adequate force agility.
- If centralised control is necessary, for example in the delivery of key services that may be in short supply or for highly sensitive missions, some agility may still be possible provided the conditions described above can be met.

4.3.1 Implications for networked force design

Level 1: Action: - *tuning existing sensing, processing and action capabilities*

Level 2: Learning: - *expanding or modifying existing capabilities to improve success at Level 1*

Level 5: Co-Adaptation: - *tuning allocations of roles and resources to our systems in overall force context, and choosing actions in awareness of likely adaptive responses by others.*

We group these three levels together here since detailed analyses for each level have not yet been performed, and because each of the points below can be treated at all three levels by considering how its existing disposition contributes to Agility at the Action level, how it can be modified to improve its contribution (Level 2), and how Agility can be increased by taking a force-level perspective (Level 5).

- Agility begins with the ability to know when a change is needed – which requires
  - monitoring of a sufficient set of indicators to be able to detect when any of the critical conditions and assumptions underpinning the current strategies and courses of action start to fail,
  - which in turn requires the ability to know what the critical conditions and assumptions are, and how their validity may be monitored.
- Subsequently, agility also requires the ability to make this information available in a timely way to the decisionmakers who have the capacity to assess the situation, to develop alternate strategies, and the authority to make the changes needed.
- Finally, agility requires that strategies or courses of action can be changed smoothly without exposing the force to undue risk
- Networking therefore has the potential to enhance force agility through its capacity to support:
  - collaborative development of the set of assumptions and conditions, and their indicators that should be monitored,
  - dynamic tasking of collection assets to monitor the currently relevant indicators,
  - the rapid compilation of assessments of those indicators from distributed sources.

- the timely alerting of those responsible for current strategies, courses of action, and decisions on any significant changes, and
- the coordination of changes in tasking and resourcing of distributed force elements in order to effect the required changes.

- These key agility-related tasks also depend on suitable doctrine, TTPs, training, and organisational structures being in place, but the role of networking in enabling agility is fundamental, ranging from. Rapid exchange of information, distributed situation awareness, coordination of manoeuvre, synchronisation of effects, to the provision of key services such as logistics.
- Networked forces are capable of many C2 approaches. To deal with the challenges of future complex operations forces must be able to rapidly adapt their mode of operation across the full spectrum of C2 approaches. Force agility therefore requires the abilities to choose and apply the most appropriate C2 approach given the current properties of the force and of the operational context, to change the C2 approach when the situation demands it, and to manage risk across the spatio-temporal boundaries of different C2 approaches. This in turn requires monitoring of the key internal and external properties needed for determining the most appropriate C2 approach.
- Networking also creates the potential for experimentation to support agility in operations through reach-back processes. This may be utilised to accelerate learning processes in the field to test options, processes and approaches for the operational force. Experimentation can increase the agility of the force to adapt to challenges not envisaged when the operational force was first constituted. It can be applied to both the component elements of the operational force (see figure 3) and to the force level (e.g. supporting the development of combined arms tactics, or new approaches for tactical surveillance and reconnaissance that can better support agility). It can also be used to explore more options for understanding and shaping the operational context. If correctly applied, experimentation offers the potential to transfer risk away form the warfighters while accelerating their ability to adapt to operational challenges.
- Re-evaluation and refinement of key assumptions on the enemy, environment and own forces is a key factor in enabling force agility, since these assumptions underpin decisions on how networking systems will be utilised and how to set their control parameters so as to enhance force agility.
- Agility requires the ability to rapidly regroup force elements to facilitate changes to courses of action within and across Lines Of Operation as appropriate, eg shifting from decentralized support and reconstruction efforts to a warfighting mode with mutually supporting, concentrated effects.
- Enhanced sharing of appropriate information and distributed command and control systems must be developed to foster the potential for agile forming and re-forming of teams as required, especially in the type of complex contexts described by Adaptive Campaigning [Army 2006b].
- Agility requires the ability for networked systems, processes and procedures to shift rapidly to support different modes of operation and C2 and concurrent C2 processes.
- Developing the capacity to learn when different modes are appropriate and identifying the queues and triggers for changing these modes. Some of these triggers may be obvious, such as a unit coming under attack. However, others may be triggered by less clear indicators and intelligence based on shifts in the trends of enemy actions and/or the operational context. Once identified, these triggers may result in changes to both shaping actions on the operational context (e.g. support to the local communities) and shifts in the warfighting modes to deal with emerging threats.

Level 3: Learning-to-learn: - *improving how Level 2 is done, to increase effectiveness of learning*

Level 4: Defining Success: - *improving the alignment of the internalised success and failure criteria in the selection process with 'real' success*

The analysis of how Levels 3 and 4 can be exploited to enhance Agility has not yet been performed either, but we assert that these levels will be key to enabling the requisite agility to emerge from Levels 1,2 and 5. In particular, Level 4 will be vital for supporting Level 3 improvement to how we learn to be agile, because it is precisely over the longer time scale that Level 4 addresses, that the failure to be agile becomes most apparent. We will return to complete these analyses in a future paper.

4.3.2 Example of Networked Force Agility

An example that illustrates some of the issues relating to networked force agility is the potential impact of NCW on the application of joint and coalition fires. Analysis of the Australian Army offensive support C2 systems identified a number of potential C2 models that would be possible for a future networked force [Sands 2004]. Some of these models represented alternative approaches to the C2 of Land offensive fires. However, others represented different modes of operation that a networked force might

choose to apply, either sequentially or in parallel as dictated by the operational requirements. Three of these models are schematically illustrated in figure 4.

The first is a simplified representation of the current artillery model based on a Headquarters (HQ) containing a Joint Offensive Support Coordination Centre (JOSCC), a gun line based on towed artillery, and a forward observer. This is an entirely voice-based model and provides maximum agility within the limitations of the current technologies. The second is a networked and decentralised model of C2 built around combat teams with forward controllers (FC), trained in application of joint fires, assimilation of sensor feeds and contact reports from combat team elements and coordination with tasked effectors (artillery, close air support, maritime, …) to deliver required effects. The combat team members in the sensor role would provide the information to the FC and during terminal phases of the engagement provide target information directly to the relevant effectors. The role of the HQ would be to provide the underpinning intent and then to shape and orchestrate the combat teams and effectors to enable them to form temporary teams to deliver the required fires effects. This model allows for shifts in the balance of control between the sensor, FC, effector, and HQ decision-makers to tune this model to the needs of the operational context thereby providing a significantly enhanced level of force agility. The third model is networked but highly centralised. All sensor feeds are integrated in the one HQ and then assigned to effectors to deliver the required effects, and is potentially efficient if centralised decision making can provide globally optimised outcomes for application of limited offensive fires assets. It also lends itself to the automation of key processes thereby making it a logical tool to address the problem of dealing with time sensitive targets. However, this model tends to lose some the advantages of highly parallel decision-making as well as diluting the details of local situational awareness.

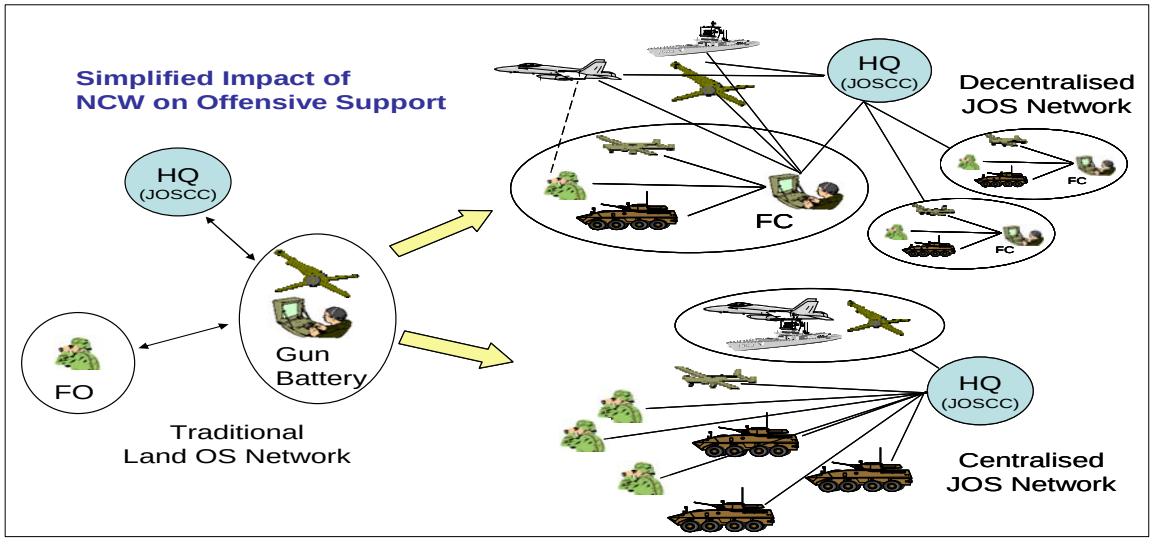

Figure 4: Schematic illustration of alternative offensive fires models showing the traditional fires model based on a HQ, gun line and forward observer (FO) and 2 networked force models for joint offensive support (JOS). One based on a highly distributed C2 structure with forward controllers (FC) and the other a highly centralised model.

Each model of networked C2 has its strengths and weaknesses and is best suited to particular contexts. A hybrid approach is therefore proposed such that networked systems and processes are designed to enable each model to be used (including concurrently) as required by the operational context. Thus, fires support to local combat teams, normally delivered by the distributed model using organic and some externally orchestrated effectors, is combined with centralised access to higher level effectors for time sensitive targets. This design aids agility in multi-national operations, where one nation could maintain maximum internal agility, while still being able to call on the higher force's fires capabilities for larger scale effects and for rapid responses to time sensitive targets. Once appropriate TTPs and triggers for moving between the modes have been developed, such a hybrid model should provide a higher level of force agility than either of the separate networked fires models

4.3.3 What About Swarming?

Swarming, and some of its conceptual variants, are sometimes perceived as a way of facilitating enhanced force adaptivity. It is argued that large numbers of force components operating under a shared intent and utilising modern networking systems to share information, will be able to rapidly self-synchronise to adapt to varying battlespace requirements, and that these largely independent force elements will be more responsive to dynamic changes than a traditional military force, as more effective

force-level behaviours emerge from the cumulative, self-synchronised actions of the comment force elements. These arguments are loosely based on aspects of emergence in complex systems, and to a degree, on current drives in business practices to flatten organisational structures.

Such an 'informed swarm' approach may well produce some enhancement to the immediate responsiveness of a force. The force will, if composed of sufficient numbers, be relatively robust as it will readjust rapidly to the elimination or degradation of any particular swarming component. However, by flattening the command structures, the force is being optimised for efficiency within a narrow band of force behaviours, resulting in limited force agility.

Moreover, the gains delivered by the 'informed swarm' approach will tend to be at the expense of the ability of the force to adapt effectively at higher levels of scale. In particular, the ability of the force or even major subsets of the force to demonstrate high levels of agility let alone flexibility will tend to suffer from significant inertia as they will not be able to respond as an integrated whole. Thus, adaptation of the higher order force behaviours will be severely limited. Overall force effectiveness will also tend to suffer, as the force will be composed of a large number of local optimisations for each of the individual force components, rather than an attempt to maximise the overall force effectiveness. The force will also tend to operate on relatively short conceptual timeframes that match the timeframes of component elements. The smaller the swarming elements the more immediate will be their conceptual horizon. As such the ability of the overall force to anticipate and plan for future threats and option will be severely constrained.

4.4 Flexibility – recognise and deal effectively with new challenges, ability to be reconfigured in different ways to do different things, under different sets of conditions

Given a requirement for a new operation, Flexibility requires the abilities to:

- Develop appropriate measures of success for the operation and strategies for achieving them;
- Develop the means to execute the strategies by drawing on the force and non-military elements that are available and forming effective teams and relationships between them;
- Bring the teams up to an operational level of capability in a timely way;
- Continue to monitor the effectiveness and appropriateness of the ends (measures of success), ways (strategies) and means (teams and their tasks) during the operation and modify as required.

Obviously networking can support the exercising of flexibility in operations in many ways, and all five levels of adaptation will be important to achieve flexibility, but a detailed analysis is yet to be completed. We make some illustrative observations here:

- Flexibility may call for significant innovation and improvisation to deal with operational tasks that have not been encountered before, or for which the expected capability elements are not available.
- In combined, coalition and interagency operations, full flexibility requires the ability to deal with cultural differences, and to make good use of the valuable diversity that is represented, eg information systems and processes must adjust how information is exchanged eg by changing the balance of explicit and implicit information depending on the similarity of background of the force elements,. Data dictionaries and agreed lexicons for information exchange will be needed.
- An important contributing characteristic is that the structure and capability of the force can be reconfigured in different ways to do different things, under different sets of conditions, and the need to do this can be recognised and implemented rapidly Such abilities are to some extent determined in the force development and force generation stages, which will be canvassed further in Section 5.

5 Adaptivity Insights within the Force Generation and Development Contexts

Force development and force generation are responsible for the creation of operational capabilities.

Since there can be no adequate single description of the needed future force-level capability, it is not enough to create systems with potential to be networked and then connect them in the expectation that they will spontaneously form into effective warfighting capabilities. Nor will detailed top down systems engineering suffice, as if the intended force could be exactly defined and the parameters engineered to deliver the desired outcomes.

The generation of a networked force is more accurately described by the concept of complex systems engineering [Bar-Yam 2006, Braha 2006, Norman 2004], where large numbers of capability elements are developed interdependently, and adaptively integrated into a coherent whole.

These processes must create the conditions for adaptivity within the force produced, but the generation processes themselves must also be adaptive, since conditions, requirements and possibilities will keep

evolving throughout the long gestation periods of capability. So, we must consider the adaptivity properties of both the forces generated by these processes, and of the processes themselves.

If undertaken well this should facilitate the realisation of the potential of NCW. If ignored or undertaken poorly, there may be a dangerous transfer of risk: from force development to force generation, and ultimately from force generation to force employment, i.e. to the warfighters.

As in Section 4, we simply seek here to identify some illustrative insights for development and implementation of networked force capability, by considering adaptivity across all classes and levels.

5.1 Responsiveness – recognise and deal effectively with immediate threats and opportunities

We will focus here on the responsiveness *of* force development and generation processes, and defer consideration of how they could better enable responsiveness *in* the force produced, to a future paper

So the threats and opportunities that need to be responded to here, arise from rapid changes in what is technically possible, in the nature of the operational threats that future forces will have to contend with, and in the strategic, economic and political climates within which force capability is developed. The accelerating pace and scope of these changes is stressing traditional and cumbersome force development approaches and driving the need to increase their responsiveness.

However the concepts for how this can be achieved are much less mature than their counterparts in the operational context. Full exploitation of all five levels of adaptation will be vital for developing the needed responsiveness in force development and force generation processes, just as in the operational case. We present here some initial illustrative thoughts, which can be considered at each of the five levels, to foreshadow the analytical work that remains to be done to flesh these out more thoroughly.

5.1.1 Implications for responsiveness <u>in</u> generation of networked forces

Level 1: Action: - *tuning existing sensing, processing and action capabilities*

- Seek and use lessons from real-world operations and from experimentation to <u>identify changes to requirements</u> for force generation, <u>and to best practice</u> for how doctrine, TTPs, organisational structures and training of forces can be developed for networked forces.
- Actively <u>monitor critical indicators</u> in the technical, strategic, tactical, economic and political domains and <u>make prompt adjustments</u> to current networked force development and generation processes and priorities, to take advantage of opportunities and mitigate threats that arise.

Level 2: Learning: - *expanding or modifying existing capabilities to improve success at Level 1*

- Improve ability to leverage information in lessons from real-world operations and experimentation by <u>resisting the negative attitude that they represent 'scope creep'</u> in the acquisition process.
- <u>Improve ability to detect and respond</u> to threats and opportunities in the domains above

Level 3: Learning-to-learn: - *improving how Level 2 is done, to increase effectiveness of learning*

- <u>Monitor success</u> of Level 2 in improving Level 1 outcomes, and <u>identify and implement ways</u> in which Level 2 can be made more effective.

Level 4: Defining Success: - *improving the alignment of the internalised success and failure criteria in the selection process with 'real' success*

- <u>Broaden force generation success metrics</u> for new networked systems to include impacts on team effectiveness, integration of legacy systems, force adaptivity and full spectrum effects.

Level 5: Co-Adaptation: - *tuning allocations of roles and resources to our systems in overall force*

- In responding to threats and opportunities, <u>address both specific projects and force-level design</u> to identify SoS trade-off decisions on capabilities and between component systems.

5.2 Resilience – recognise and deal effectively with harmful changes to the system, recover from misfortune or damage, and degrade gracefully under attack or as a result of partial failure

Resilience *of* the force development and force generation processes refers to the ability to remain focused on and deliver the most important capability outcomes despite adverse changes, eg in what is possible (technology failures) or in resources (loss of key personnel or funding cutbacks).

Similarly, we consider ways in which these processes can foster resilience *in* the resulting networked force. For lack of space, we focus on the latter here, and defer the former to future work. Again, we select a few illustrative insights and acknowledge the need to exploit all the levels of adaptation.

5.2.1 Implications for generation of resilient networked forces

There are many ways to engender resilience in distributed systems, and some of these depend on decisions made in the force development and force generation processes.

Static robust design features that contribute to resilience include redundancy and physical protection in systems providing the most critical functions, and distributed designs with no single points of failure. Object-oriented system architectures minimise interactions between components to reduce systemic consequences of individual component failure, but at a cost of potentially reduced overall system synergy. It is obvious how force development and generation could prioritise such features in networked force design to deliver greater inherent force resilience if the additional costs warranted the benefits, and how one could employ Levels 2, 3 and 4 to improve success in doing so.

But a more interesting aspect of resilience arises from the *dynamic* aspects of the force, and here there are contributions from the force development and generation stages, but also from the organisation and processes of the operational force. This approach treats resilience as the outcome of particular adaptive processes that dynamically create the ability to carry on with essential functions by rapid compensating actions, when damage or failure do occur in spite of the static robust design aspects.

The force development and generation aspects of enabling this dynamic resilience stem from the capability requirements implied by the following tasks for Resilience at Levels 1 and 5:

- Monitor key operational and contextual factors to determine what the core functions are, and their essential levels of capability at any time;
- monitor indicators of 'health' and enemy intent in order to know when individual elements are damaged, or preferably, are about to be;
- provide the above information rapidly to decision nodes that can:

  at ***Level 1: Action: -*** *tuning existing sensing, processing and action capabilities*

  - cause the core functions to be maintained <u>within the same system</u> by one or more of:
    - shifting of essential tasks from damaged to undamaged elements, exploiting redundancy within system;
    - redistribution of tasks within system, exploiting multiroled or multifunctioned elements;
    - repair of damage, which requires the capacity to detect damage, assess and repair it, exploiting capacity for frontline repair and rapid mobilisation of logistic chains;

  and / or at ***Level 5: Co-Adaptation: -*** *tuning allocations of roles and resources to systems in SoS*

  - cause the core functions to be maintained <u>by other systems at the same level</u> as the damaged one, by redistributing tasks so that essential ones are done *vice* non-essential. This requires:
    - redundancy of functionality so that other elements are able to pick up tasks;
    - contingency plans (know how to action quickly) for loss of particular types of elements;
    - capacity for rapid reconfiguration (generation of options, assessment, choice, implementation), load-shifting, selection and implementation of contingency plans; and/or
  - cause the core functions to be maintained by making co-adaptive changes <u>at other levels</u>, eg:
    - redistribute roles and responsibilities of systems across the SoS, and/or
    - compensate for the damage by changing the resources available to the system; and
  - execute the above quickly enough in the context of operations.

Levels 2, 3 and 4 can then be invoked in order to accelerate learning how to do these things better

Implications that can be derived from the above to facilitate force-level resilience include:

- Balance is needed between the costs, risks and benefits of resilience versus effectiveness eg flexible multifunctional force elements versus highly-trained specialised elements.
- The need for rapidly task reorganisation will drive networked forces to increase modularity and ability to dynamically form diverse teams, placing greater premiums on force interoperability.
- Interoperability is a key design driver for resilience in networked force implementation:
  - individual systems must be able to interoperate with each other (still often an aspirational goal);
  - force-level interoperability is traditionally achieved through technical and systems interoperability in the force development stage, and formal process interoperability through development of appropriate TTPs and training in the force generation stage;
  - networked forces will also need integration of many informal social processes and procedures;

- close collaboration between the two stages will be required to ensure resultant systems meet future force interoperability requirements.

- Definition of technical standards is necessary but not sufficient for interoperability to support force resilience. It also requires suitable force architectures, doctrine, TTPs and training to be developed.
- The networks themselves must be resilient. Network integrity and reliability against both hostile action and technical failures is vital. NCW's potential to enhance the delivery of fires and other lethal force effects, makes the networks and associated information systems into safety-critical systems. Accreditation of these systems in all possible configurations to safety-critical standard may be impractical, but it is important that reliability be designed into the whole of the networked capability, not just its individual elements.
- Similarly, designing systems, processes and procedures for graceful degradation and integration is essential if networked forces are to be resilient to the impacts of enemy and the environment.

5.3 Agility – recognise when change of strategy is required, and implement it easily

As in the preceding two subsections, we can consider both agility *of* the force generation and development processes, and how those processes can deliver force outcomes which are predisposed to permit or foster agility *in* their employment.

In this case we will briefly consider the former. This is very complementary to our discussion of responsiveness in force development and generation in Section 5.1. A similar analysis obtains, but the range and scope of what needs to be monitored, and the types of actions that can be taken, must be enlarged to encompass indicators of the validity of critical assumptions and conditions underpinning the current strategy and course of action (as in Section 4.3.1 except that here the strategy relates to force development rather than force employment and the course of action refers to capability projects rather than missions), and major changes to these such as cancelling or redefining projects, or adopting quite different capability strategies (eg bespoke development versus off-the-shelf, staff processes versus field experimentation, etc). Similarly, the ways in which the higher levels (2 – 5) of adaptation are invoked will be the same, albeit with a different focus. We again offer some illustrative observations:

5.3.1 Implications for networked force design

- Assumptions about requirements for force capabilities and networking need to be constanly re-evaluated in the light of lessons learned both operationally and through experimentation.
- As for any operation, regular reassessment of the underpinning strategic assumptions is needed to ensure that the overall intent and mission of capability development are aligned the strategic goals.
- A major stumbling block for agility of networked force development is the long timescale for capability development relative to the rapid evolution in both networking technologies and lessons from operations.
- One strategy is taking a holistic view of the capability being generated (eg the US FCS program), and addressing inter-system issues as elements within the overall process. This allows greater flexibility to foster required systems interoperability and undertake design trade-offs, and permits delaying decisions on individual components to later stages of development, enabling more agility in the process by lengthening the window in which lessons can be incorporated.
- Another strategy focuses on modelling, experimentation and trials to enable a wide range of potential future options to be explored. These can be used to test capability options, force level behaviours, and assess risks across a wide range of potential operational contexts, thus enabling a greater range of issues to be incorporated into the development process.These techniques can, if used effectively, provide significant enhancement to the agility of the force generation stage.
- Education initiatives can also support enhanced agility of force development and generation, in particular to achieving the required cultural changes. Education needs to be designed to help capability developers to extend their ability to apply adaptive approaches to complex force development and generation processes, beyond the degrees of adaptivity already in their culture.

5.4 Flexibility – recognise and deal effectively with new challenges, ability to be reconfigured in different ways to do different things, under different sets of conditions

Early concepts of NCW grew out of a desire to generate an integrated maritime battlegroup in the context of force-on-force conflict in the cold war era. This resulted in a vision for NCW that was aimed at optimising forces to meet a narrow and well defined threat. More recent warfighting experiences have shifted the focus of warfighting to counter-insurgency and similar complex warfighting scenarios,

with increased awareness that force flexibility, the ability to effectively operate across a broad range of warfighting types, is an essential characteristic of military forces and a major driver for future force design..

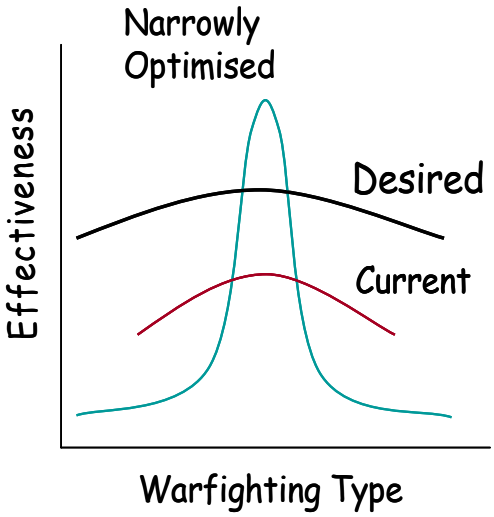

Figure 5: Schematic illustration showing the a comparison between the flexibility of current forces to address a rang of warfighting types and how this might change in a networked force to either be a highly efficient but narrowly optimise solution, or be a less efficient by more broadly flexible approach. It is argued that the more broadly flexible approach should be the goal.

Figure 5 schematically illustrates the need to migrate from the current force capability to one which can address a broader range of operational types at a highly level of effectiveness. If forces are too narrowly optimised for a particular type of operation there is a great danger that when suddenly faced with a challenge outside this narrow range that the force will find itself unable to adapt. On the other hand, approaches to networked force implementation that would result in highly effective but inflexible military capability are equally dangerous. In the latter case an opponent would simply have to move outside the narrow band of optimal force effectiveness to rapidly render the force ineffective.

Once again, we can here only barely touch on the ramifications of flexibility in both how the force development and generation processes operate, and how they can better create the conditions that permit and foster flexibility in the forces they create.

5.4.1 Implications for networked force design

Networking technologies are capable of supporting a wide range of warfighting types. In designing future networked forces decisions must be made about the spectrum of operations that the force will be designed to address. Like all exercises in design, the implementation of a networked force will require trade-offs in the way the physical network, doctrine and TTPs, training and command and control are implemented. If flexibility is a major design driver this will result in consideration being given as to how to address force responsiveness, resilience and agility across a wide range of contexts. However, it must be remembered that for any particular operation the flexible force will be less effective than one specialised for that type of operation. This trade-off can not be continued indefinitely. The force will need to be bounded in its potential scope of operations or the effectiveness of the force will become too dissipated. Thus the degree of force flexibility must become one of the cornerstone design characteristics in implementing a future networked force.

6 Conclusions

In addressing the problem of migrating to a future network capable force, we have argued that the primary benefit of networking is to enable the force to be more effective in achieving those tasks that are currently difficult, and in enabling the force to undertake more complex operations with similar forces and with an acceptable level of risk. Our thesis has been that a major factor in achieving this enhanced ability to address complex operation will be derived from an increase in both the adaptivity of the force and in the supporting force development and generation processes.

Using a simplified model of the overall process of force implementation, we have utilised the conceptual framework for adaptation to identify some insights, issues and approaches that will facilitate the design and implementation of networked force capability. Most of these insights relate to how a focus on adaptivity can assist in enhancing operational capability. However, some attention has also been given to the implications of adaptivity for the force development and force generation stages.

A key theme of the paper is the need to approach the migration to a networked capable force from a force-level perspective. Most efforts in NCW implementation focus on enabling the technical interoperability of the components of the network. Taking an adaptivity based approach, it is possible to identify a wide range of force-level issues and insights that are generally masked by the details of the networking technologies. By focusing on adaptivity, it is the view of the authors that a more balanced whole-of-force can be achieved in the design and implementation of networked capability.

References

Army 2006a *Networking the Army Campaign Plan*, Army Headquarters, 2006.

Army 2006b *Adaptive Campaigning – the Land Force Response to Complex Warfighting* Future Land Warfare Directorate, Australian Army, Dec 2006

Bar-Yam 2006 *Engineering Complex Systems: Multiscale Analysis and Evolutionary Engineering,* in Complex Engineered Systems: Science Meets Technology, D. Braha, A. Minai, Y. Bar-Yam (Eds.), Springer, 2006 and earlier references contained therein.

Braha 2006 *Complex Engineered Systems: A New Paradigm*, in Complex Engineered Systems: Science Meets Technology, D. Braha, A. Minai, Y. Bar-Yam (Eds.), Springer, 2006 and earlier references contained therein.

Coombs 2005 Coombs, G., Unewisse, M.H. and Sands, D. *Concepts for Managing Information on the Land Tactical Battle Management System Network*, Land Warfare Conference '05, Brisbane, 2005

FLOC 2004 Australian Department of Defence, *Future Land Operational Concept: Complex Warfighting,* Future Land Warfare, Army Headquarters, Edition 1, May 2004.

Grisogono 2005 Grisogono, A.M. *Co-Adaptation,* invited paper 6039-1 Complex Systems Conference, SPIE Symposium on Microelectronics, MEMS and Nanotechnology, Brisbane December 2005

Grisogono 2006a Grisogono, A.M. *The Implications of Complex Adaptive Systems Theory for C2*, CCRTS 2006 – State of the Art State of the Practice, San Diego, 2006.

Grisogono 2006b Grisogono, A.M. *Success and failure of Adaptation,* Interjournal, 2006(1901).

Grisogono 2007 Grisogono, A.M. and Ryan A *Operationalising Adaptive Campaigning*, ICCRTS 2007 – Adapting C2 to the 21st Century, Newport, 2007.

Hayes-Roth 2006 Hayes-Roth F. *Two Theories of Process Design for Information Superiority: Smart Pull vs. Smart Push* CCRTS 2006 – State of the Art State of the Practice, San Diego, 2006.

Norman 2004 Norman, D.O. and Kuras, M.L *Engineering Complex Systems*, Mitre Corp, 2004.

Pratt 2007 Pratt, J. and Tregenza, M. *Experiment Perseus Vision – Dynamic Teaming in a Networked Battlegroup with Mixed Levels of Networked Capability*, work in progress, DSTO, 2007.

Sands 2004 Sands, D.G. Tomecko, N. Wheeler, S. Ryan, A. Kempt, N. and Judd, G.*Alternative Force Structures for Offensive Support and Their Impact on Command and Control in a Networked Environment*, Proceeding of the Land Warfare Conference 2004.

Shoubridge 2007 Shoubridge, P. *Network Services and Their Management*, informal discussion paper, DSTO, 2007.

Smith 2006 Smith EA Jr and Grisogono AM, *Towards a Synthesis of Complex Adaptive Systems Theory and Effects Based Approaches to Operations: Warfighters to Coalitions: A Case Study of Multi-level Adaptation in Effects-Based Operations* 11th ICCRTS, Cambridge UK, 2006

Unewisse 2004 Unewisse, M.H. JP 5000: *A Review of the Progress Towards an NCW-Capable Land Force*, In Proceeding of the Land Warfare Conference 2004.

Unewisse 2005 Unewisse, M.H., Pratt, J.M., Tregenza M.J., Sands D., Krause D., Kirby B., Perry, A. and Wilson, S.A. *A Review of the Progress Towards an NCW-Capable Land Force*, DSTO Report, DSTO-TR-1779, 2005.

Unewisse 2006 M.H. Unewisse, S. Wison, A. Perry and C. Boyd, *An Australian Approach to Assessing Force-Level Network-Centric Warfare (NCW) Readiness*, 11th ICCRTS, Cambridge UK, 2006.

USMC 1998 Commander USMC, *Sustaining the Transformation*, WHITE LETTER NO. 3-98, 1998.

Appendix A: Classes of Adaptivity and their Characteristics

Class / Charac-teristics	Responsiveness	Resilience	Agility	Flexibility
OUTCOME	The ability to react in a timely manner to change in the environment – i.e. in the context of a set of strategies that are already being executed, and a change occurring that creates a new threat or opportunity, responsiveness is the capacity to recognise and deal with the new threat or opportunity as effectively as if there were ample time to plan and prepare for it.	The ability to recover from or adjust to misfortune or damage, and the ability to degrade gracefully under attack or as a result of partial failure – i.e. the core functions of the force continue to achieve essential levels of capability when individual elements are disabled one or more at a time; there is quick recovery from damage with minimal interruption or loss of capability	The ability to recognise when to shift from one strategy to another and to do so easily. – i.e. producing a rapid change of tack to more effective behaviours when significant external and/or internal changes arise requiring significant and different responses.	The ability to create and maintain effectiveness across a wide range of tasks, situations, and conditions. – i.e. structure and capability of the force can be reconfigured in different ways to do different things, under different sets of conditions, and the need to do this can be recognised and implemented rapidly
Enemy Perspective	The force is 'context-aware', it discovers enemy vulnerabilities and pursues them, finds and uses resources, recognises enemy intent and foils enemy attempts to surprise and deceive it.	The force is unbreakable, disproportionate effort is require to inflict minimal damage.	The force slips out of your fingers like water.Enemy is unable to come up with options that cannot be countered. Can't maintain initiative.	The force morphs effortlessly from one form to another always maintaining a high level of potency and effectively checkmating any hostile intent or CoA. It is difficult for the enemy to pit its strength against our weakness because the force seems to 'sense' any attempt to do that and fluidly shifts its strength to the perceived weakness.
Owner Perspective	The force displays context - awareness and intelligent autonomy even in a hostile environment	The force provides a high degree of assurance of being able to continue to deliver its essential role even in a hostile environment.	High confidence the force can deal with an unpredictable, hostile, changing environment. It can apply itself to any task given. It can forge new partnerships and relationships.	The force is a flexible and powerful tool of government power, offering a sufficient range of options in any situation, able to generate customised force packages rapidly for emerging situations,...
Partner Perspective	The force is an intelligent partner, can find valuable new resources, provide valuable information about dangers, provide protection, etc...	The force can be counted on to continue playing its essential roles in a hostile environment. Roles of lesser overall value may be shed – may impact on partner	High confidence in the ability of force to adapt in a timely manner to changes in environment and adversary.	The force is resourceful and can take on many different roles in a coalition operation; it has a 'can do' posture; it is able to effectively negotiate distribution of roles, resources, and responsibilities with its partners.
Operator Perspective	I am able to recognise and deal apprropriately with unexpected events and I can count on my team mates to do the same.	I am able to rely on essential functions continuing to operate and I have the means to continue delivering my own critical roles.	I am able to respond and change in a timely manner to significant changes in adversary/environment and have expectation that this happens in a coherent way across the force.	I am able to rapidly create tailored teams of force elements to deal with any emerging situation