Australian Government
Department of Defence
Defence Science and
Technology Organisation

Sep 2003

DSTO

Network-Centric Warfare–Its Nature and Modelling

M.P. Fewell and Mark G. Hazen

DSTO-RR-0262

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

20040225 142

Australian Government
Department of Defence
Defence Science and
Technology Organisation

Network-Centric Warfare—
Its Nature and Modelling

*M.P. Fewell and Mark G. Hazen**

Maritime Operations Division
Systems Sciences Laboratory

*permanent address: DRDC-Atlantic, Dartmouth, Canada

DSTO-RR-0262

ABSTRACT

This study examines the concept of network-centric warfare with the aims of characterising network centricity as clearly as possible and identifying metrics for 'level of net-centricity'. Properties of network-centric systems, as expounded in the literature, were critically examined to derive examples of suitable metrics. This examination suggests that, except for the provision of reachback, none of the properties is clearly diagnostic of network centricity: it is possible to conceive of systems displaying one or more of them despite not being net-centric as we understand the term. This means that metrics for these properties are not well correlated with the degree of network centricity of the system. Another list of properties was compiled, derived from characteristics of the internet and other effective networks, that is better suited to the identification of network centricity. Consideration of this led to the conclusion that access to a high-capability network is not sufficient for a system to be network-centric, it is also necessary that the network be used in an appropriate manner—a manner supporting the force as a whole, rather than being focused on the needs of a particular unit or platform. Not only must the right information be available to the right person at the right time in the right form, but also it must be put to the right use. This emphasis on motivation in the definition of network centricity parallels, though is distinct from, recent work emphasising human aspects in command and control (C^2). As with C^2, network centricity is not just about hardware. The question of defining a general metric that faithfully indicates level of network centricity is examined with the aid of a specific example, but remains open.

RELEASE LIMITATION

Approved for public release

AQ F04-05-0339

Published by

DSTO Systems Sciences Laboratory
PO Box 1500
Edinburgh South Australia 5111 Australia

Telephone: (08) 8259 5555
Fax: (08) 8259 6567

© Commonwealth of Australia 2003
AR-012-876
September 2003

APPROVED FOR PUBLIC RELEASE

THIS DOCUMENT CONTAINED BLANK PAGES THAT HAVE BEEN DELETED

Network-Centric Warfare— Its Nature and Modelling

Executive Summary

Network-centric warfare (NCW) is the central concept driving the current revolution in military affairs. For this reason, there is a need for operational analysis of net-centric systems to aid the development of appropriate doctrine and training programs, and to provide advice on the acquisition of the expensive communications and information-processing equipment likely to be required. However, immediately the problem arises that definitions of network centricity lack clarity, making them difficult to apply to specific situations. This means that it is at present difficult to recognise network centricity, or its absence, in a particular case. Hence, it is difficult to ascribe a gain in effectiveness that may be observed in a modelling or experimental study with changes in the level of net-centricity. This report explores the issue by formulating a sharper conceptualisation of the nature of network centricity than is generally found in writings of its proponents. The aim is to determine as precisely as possible what it means to be network centric, as a starting point for studies aiming to quantify the benefits, if any, of a network-centric orientation.

Characteristics of network centric warfare (NCW), as expounded in the literature, are collated in this report and elaborated sufficiently to lead to examples of metrics that may be of use for quantifying the level of those characteristics. At the highest level, these characteristics include such things as an elevated speed of command, high levels of self-synchronisation and shared situational awareness amongst the elements of a force, provision of reachback facilities, and so on—the so-called emergent properties of NCW.

The high-level characteristics of NCW are then examined in detail to determine the extent to which they can be used as indicators of network centricity: can we say that a system must be net-centric if it possesses one of them? The answer is no, except for the provision of reachback. In every other case it is possible to conceive of a non-net-centric system that shows the property in question.

Since the emergent properties of NCW do not provide a reliable route to the recognition of net-centricity, we sought another way, through the compilation of a list of properties derived from characteristics of the internet and other effective networks. This list is, we believe, better suited to the diagnosis of network centricity and, perhaps more importantly, it points to a key element in its nature, namely the manner in which the system is used. In our view, access to a high-capability network, though vital, is not sufficient for a system to be considered network-centric, it is also necessary that the network be used appropriately, namely in a manner that supports the force as a whole,

rather than its use being focused on the needs of a particular unit or platform. This concept is distilled in the following definition of NCW:

> Network-centric warfare is the conduct of military operations using networked information systems to generate a flexible and agile military force that acts under a common commander's intent, independent of the geographic or organisational disposition of the individual elements, and in which the focus of the warfighter is broadened away from individual, unit or platform concerns to give primacy to the mission and responsibilities of the team, task group or coalition.

In short, we advocate the addition of a fifth 'right' to the usual four: not only must the right information be available to the right person at the right time in the right form, but also it must be put to the right use. This emphasis on motivation in the definition of network centricity parallels, though is distinct from, recent work emphasising human aspects in command and control (C^2). As with C^2, network centricity is not just about hardware.

What does this mean for metrics? Since the emergent properties of NCW are not diagnostic of network centricity, their metrics might not correlate well with degree of net-centricity. We discuss an example from the modelling of maritime interception operations that shows explicitly and quantitatively the gain in effectiveness achievable by the 'broadening of warfighter focus' alluded to in our definition of NCW. However, the metric concerned is scenario-specific. The question of how to define a general scenario-independent metric for degree of network centricity remains open.

Authors

M.P. Fewell
Maritime Operations Division

Matthew Fewell joined DSTO in 2001, coming from an academic physics background. He has worked and published in the fields of experimental nuclear structure physics, gaseous electronics, atom–photon interactions including coherent effects, laser physics and the plasma processing of materials. His present interests include military experimentation, particularly in the maritime domain, and modelling effects of network centricity. This has led him into the area of command and control and made him an interested spectator of research into decision making.

Mark G. Hazen
Maritime Operations Division (on attachment from DRDC-Atlantic, Dartmouth, Canada)

Mark G. Hazen is a native of New Brunswick, Canada. He received the Combined Honours BSc degree in mathematics and computing science from the University of King's College, Halifax, NS, in 1985 and the MSc degree in mathematics from Carleton University, Ottawa, Ontario, Canada in 1987. Mr. Hazen joined the Operational Research and Analysis Establishment (ORAE) in Ottawa in 1986 doing tactical air operations research before moving to the Operations Research Division (ORD) of the Canadian Forces Maritime Command Headquarters in Halifax, NS. At ORD he worked in the areas of tactical decision aids, torpedo countermeasures and anti-ship missile defence. In 1991, he moved to the Defence Research Establishment Atlantic (DREA) to work in the Modelling and Systems Analysis Group and where he specialized in Maritime Air ASW operations. Mr. Hazen joined MOD for a two year exchange in June 2000, working in the Undersea Warfare Operations Group. In MOD, his research program included multistatic acoustic target strength, global optimisation techniques, the use of virtual environments, net-centric maritime warfare, and capability development and experimentation (CDE). In June 2002, Mr. Hazen returned to DRDC-Atlantic (formerly DREA) to head up the Virtual Combat Systems Group.

Contents

1. INTRODUCTION **1**
1.1 Definitions and Descriptions of Network-Centric Warfare **2**
1.2 Antecedents to Network-Centric Warfare **3**
1.3 Expectations for Studies of NCW Effectiveness **3**

2. CHARACTERISTICS OF NET-CENTRIC MILITARY SYSTEMS **4**
2.1 Top Level—Characteristics of a Network-Centric Force **5**
2.1.1 Speed of Command 5
2.1.2 Level of Agility Coupled with the Ability to Amass Effects 7
2.1.3 Degree of Self-Synchronisation 8
2.1.4 Level of Shared Situational Awareness 9
2.1.5 Ability to Conduct Effects-Based Operations 10
2.1.6 Reachback 11
2.1.7 Information Superiority 12
2.1.8 Interoperability in the Information Domain 13
Two Aspects: Information Flow and Information Usage—Coalition Interoperability
2.1.9 Comments and Summary 15
NCW and Devolution of Command Authority—Networked Forces as a System of Systems—Modelling Approaches
2.2 Command and Control **17**
2.2.1 The Place of C^2 17
2.2.2 Command Issues—the Importance of Trust 17
2.2.3 Control Issues 19
2.3 Second Level—Decision Making **19**
2.3.1 Decision Types 20
2.3.2 Decision Quality 20
2.3.3 Modelling Decision Making 21
2.4 Third Level—Information **21**
2.4.1 Information, Data, Knowledge, Belief 21
2.4.2 Characteristics of Information 22
Relevance, Clarity—Timeliness—Age, Currency—Accuracy—Consistency—Completeness—Comprehensibility—Secrecy—Authenticity—Value—Degree of Interoperability
2.5 Fourth Level—General Characteristics of Networks **25**
Availability—Concurrency—Coverage, Homogeneity—Reliability—Survivability—Security
2.6 Base Level—Physical Properties **26**

3. DISCUSSION—NETWORK CENTRICITY AND INFORMATION-BASED WARFARE **26**
3.1 The Importance of Understanding the Nature of Net Centricity **26**
3.2 What is Net Centricity? **27**
3.2.1 Emergent Properties of NCW as Indicators of Net Centricity 27
Speed of Command—Level of Force Agility and Ability to Amass Effects—

Self-Synchronisation and Shared Situational Awareness—Conduct of Effects-Based Operations—Reachback—Information Superiority—Interoperability of Information Usage—Summary and Comments

3.2.2 Network Attributes Characteristic of Net Centricity 31

Ad Hoc Geometry—Robustness—Between Peers—Common Grounding or Basis of Relationship—Dynamic Communities of Like Minded People—Open Access—Portability of Function—Anonymity—Geographical Independence—Distributed Computing—Collective Memory—Speed of Information Dispersal

3.2.3 Heuristic Characterisation of Network Centricity 32

3.2.4 Definition of Network-Centric Warfare 33

3.3 Discussion 34

3.3.1 Implications of NCW for Morale and Loyalty 34

3.3.2 Network Centricity Related to Rational Selfishness 34

3.3.3 Reachback—Linking Information-Based Warfare to Network Centricity 35

3.4 Metrics for Network Centricity 37

3.5 Summary 38

4. CONCLUSIONS 39

APPENDIX A : ON THE NAMES OF METRICS 41

APPENDIX B : DESCRIPTIONS OF DEGREES OF NETWORK CENTRICITY 42

B.1 Levels of Information Systems Interoperability (LISI) 42

B.2 Network-Centric Operations Maturity Model 42

B.3 DSTO-Communications-Division Capability Options 43

B.4 From a Study of C^2 and IO 43

APPENDIX C : ON INFORMATION 45

C.1 The Importance of Information to Warfare 45

C.2 Modelling Information 45

C.3 Information Operations 46

ACKNOWLEDGEMENT 46

REFERENCES 47

List of Tables and Figures

Table 2.1: Examples of metrics for the characteristic 'speed of command' 6
Table 2.2: Metrics for force agility and the ability to amass effects 8
Table 2.3: Examples of metrics for the 'degree of autonomy' aspect of self-synchronisation 9
Table 2.4: Examples of metrics for the level of shared situational awareness 10
Table 2.5: Generic metrics for the conduct of effects-based operations 11
Table 2.6: Examples of metrics for reachback operations 11
Table 2.7: Examples of metrics for information superiority 13
Table 2.8: Examples of metrics for the degree of interoperability 14
Table 2.9: Possible metrics for mutual trust 19

Figure 2.1: The characteristics of a network-centric military system discussed in this paper, arranged as a hierarchy 5
Figure 3.1 Queueing-theory calculation of the probability of intercepting incoming vessels in a maritime interception operation as a function of arrival rate 37

Table of Acronyms

ASW	anti submarine warfare
C^2	command and control
COMCEN	communications centre
COMSEC	communications security
CONOPS	concept of operations
COTS	commercial off the shelf
CTP	common tactical picture
EBO	effects-based operations
HUMINT	Human-sourced intelligence
IO	information operations
LAN	local-area network
LISI	levels of information-system interoperability
MAR AG-1	Maritime Systems Group, Action Group 1
MOE	measure of effectiveness
MOP	measure of performance
MORS	Military Operations Research Society
NATO	North-Atlantic Treaty Organisation
NCW	network-centric warfare
NCMW	network-centric maritime warfare
OODA	observe, orient, decide, act
ROE	rule of engagement
SME	subject-matter expert
TTCP	The Technical Cooperation Program

1. Introduction

Network-centric warfare (NCW) is the central concept driving the current revolution in military affairs. Because of the plethora of ways in which forces could be restructured to use communications networks efficiently, and in which the networks themselves could be structured, there is rapidly growing interest in modelling and experimentation as a means of sorting through the possibilities, and therefore there is corresponding interest in metrics for network centricity. The reason for this is clear: not all of the possibilities will lead to full network centricity, so it is necessary to be able to recognise net-centricity, or its absence, in a military force in order to correlate its occurrence with improvements in military effectiveness.

Before, however, one can construct metrics for network centricity, it is necessary to understand its nature. From this point of view, it is interesting to note that extant definitions of the concept are quite diffuse, making them difficult to apply to specific situations. This report explores the issue by attempting to formulate a sharper and more specific conceptualisation of the nature of network centricity than is generally found in writings of its proponents. The method of doing this began with a collation of the characteristics of network centric warfare that have been discussed in the literature. These were elaborated sufficiently to provide examples of metrics for these characteristics. Then, the highest-level NCW characteristics—the so-called emergent properties—were subjected to brainstorming to identify the points of confusion and develop a mental model of NCW that focuses as precisely as possible on what it is that characterises a net-centric orientation. The new model draws on characteristics of many different types of networks, not only those envisaged for NCW. The model was then distilled into a new one-sentence definition of network centricity. Along the way, the conclusions highlight the inadequacy of metrics derived from or referring to any one of the emergent NCW properties. The question of constructing a metric for true network centricity is canvassed (§3.4), but remains open.

The work reported herein was begun in support of a study being undertaken by the Maritime Systems Group Action Group 1 (MAR AG-1) of The Technical Cooperation Programme (TTCP). However, the results in this paper should be of use for any modelling of NCW.

This paper is organised as follows: the rest of this section outlines some background to the study. Section 2 consists of an annotated list of characteristics—of NCW, of command and control, of information and decision making, and of networks. These were obtained from a search of the literature on warfare theory and operational analysis, professional military journals, and the academic literature on the psychology of decision making. Section 2 also contains suggestions for metrics for the higher-level characteristics. The third section of the report presents a theory of net-centric command and control that aims to distil the essence of net centricity. The final section consists of a conclusion. Appendices contain related information.

1.1 Definitions and Descriptions of Network-Centric Warfare

MAR AG-1 adopted the following statement from the U.S. Naval Studies Board [1] as its working definition of network-centric maritime warfare (NCMW):

> '...military operations that exploit state-of-the-art information and networking technology to integrate widely dispersed human decision makers, situational and targeting sensors, and forces and weapons into a highly adaptive, comprehensive system to achieve unprecedented mission effectiveness.'

This could stand equally well as a description of NCW in general. Perry *et al.* write [2]:

> 'Network-centric warfare is generally thought to be *the linking of platforms into one shared-awareness network in order to obtain information superiority, get inside the opponent's decision cycle, and end conflict quickly.*' (italics original)

The U.S. Department of Defense gives its view of NCW by describing the attributes of a networked force [3(§3.2.7)]:

> 'In its fully mature form, NCW possesses the following characteristics:
>
> '*Physical Domain*:
> - 'All elements of the force are robustly networked achieving secure and seamless connectivity.
>
> '*Information Domain*:
> - 'The force has the capability to collect, share, access and protect information.
> - 'The force has the capability to collaborate in the information domain, which enables a force to improve its information position through processes of correlation, fusion, and analysis.
> - 'A force can achieve information advantage over an adversary in the information domain.
>
> '*Cognitive Domain*:
> - 'The force has the capability to develop and share high quality situational awareness.
> - 'The force has the capability to develop a shared knowledge of commanders' intent.
> - 'The force has the capability to self-synchronise its operations.
>
> 'In addition, the force must be able to conduct information operations (IO) across these domains to achieve synchronised effects in each of these domains.'

The 'four tenets of NCW' comprise a description of the purported benefits of adopting NCW. They are [3(p.i),4(pp.7,8),5(pp.8,9)]:

- 'A robustly networked force improves information sharing.
- 'Information sharing and collaboration enhance the quality of information and shared situational awareness.
- 'Shared situational awareness enables collaboration and self-synchronization, and enhances sustainability and speed of command.
- 'These, in turn, dramatically increase mission effectiveness.'

To the four tenets, Alberts [4] adds 'Thus, NCW involves both:

- 'the provision of vastly increased access to information at all echelons
- 'a redefinition of the relationships among participants in a mission and between commanders and subordinates.'

A key feature of NCW is often expressed in terms of the 'four rights': the network supplies the right information at the right time in the right form to the right person.

Numerous other descriptions of NCW are collected in Reference 6. All of these form, in a sense, the baseline from which the present work seeks to expand. The need for this arises because it is difficult to use these descriptions as definitions. They are relational in nature and therefore dependent on the initial state. The scope of NCW is so wide that it is difficult to assess a particular capability in regard to it. How do you tell when NCW capability has been achieved? For example, it is not stretching the point too far to claim that Nelson's fleet was net-centric, according the US Department of Defense's description above. It had all the capabilities listed and achieved a high degree of information advantage. Yet the impression unmistakably arises that this is not what the authors of that description really mean. A key aim of this paper is to flesh out the description of NCW sufficiently far for it to be useful as a definition.

1.2 Antecedents to Network-Centric Warfare

Its proponents claim that NCW is a wholly new way of fighting, so much so that extrapolation from past experience will not suffice to reveal fully the gain in capability that is potentially available. Rather, it is claimed, a '...campaign of experimentation is [required] to be able to understand empirically what war in this new era can be expected to look like' [7]. The 'campaign of experimentation' must consist mainly of wargaming and exercises [7], but preliminary analytical studies and low-resolution simulations are needed to seed the process of constructing a conceptual framework within which to formulate ideas on the nature of NCW and network-centric maritime warfare (NCMW) in particular. The MAR AG-1 study will contribute to this process.

Is NCW wholly new? Nagy discerns the beginnings of an NCW methodology in US Naval practices during World War II [8]. Holland points out that open-ocean anti-submarine warfare (ASW) can make fair claim to be a significant antecedent of NCW [9]: in this theatre, the integration of sensor data from multiple platforms has been standard practice since the late 1970s. The main differences between Cold-War ASW and the new concepts of NCW include scale—the number and variety of nodes in the network—and tempo, as exemplified by Cebrowski's remark that 'ASW' actually stands for 'awfully slow warfare' [9]. Nevertheless, despite its slow pace, the practice of open-ocean ASW as developed over the last two decades may provide valuable indicators toward concepts for NCW. Another source of insight into NCW might be gained from a study of team decision making: the characteristics that net-centric forces are supposed to display (§2.1 below) share many similarities with those observed in effective team-based decision making [e.g. 10,11(§§5.2,6.2)].

1.3 Expectations for Studies of NCW Effectiveness

What might be the outcome of the TTCP MAR AG-1 study, or indeed any study of NCW effectiveness? It is not obvious that increased network centricity will be found to be beneficial; even Gartska, one of the earliest advocates of NCW, recently wrote [12]: 'The source of the increased combat power associated with network-centric warfare is non-intuitive'. There is a large body of published opinion on NCW, which may be roughly characterised as follows:

- Network centricity is sure to lead to increased combat effectiveness [3,13–16].
- NCW provides opportunities for increased military effectiveness that may or may not be realised; we need to learn how to exploit it [8,17–29].

- For better or worse, NCW is inevitable; we had better get used to it [30–35].
- NCW will not work because
  - it will be too expensive to implement [36–38]
  - goals such as the provision of complete battlespace awareness cannot be achieved, even in principle [37–42]
  - future conflicts are likely to be asymmetric and unconventional, to which the capabilities provided by networking are ill matched [37]
  - its core thesis is flawed [43–45].

The above references contain opinion, albeit supported by detailed argument in many cases. On actual studies there has been much less published. Gartska [12] recently summarised the results of some experiments on NCW, declaring a wish to '...highlight evidence that demonstrates the power of network-centric warfare'. He pointed to a US Air Force study of tactical data links on F-15Cs as 'some of the most compelling evidence of the power of network-centric operations developed to date...'. The study found that aircraft fitted with the Joint Tactical Information Distribution System had a kill ratio 2.6 times higher that aircraft without. That is a 4 dB increase, rather less than the 'hemibel' (5 dB) factor advocated by Morse and Kimble as the minimum required to be sure of a real effect [46(ch.3)]. However, as Gartska notes, for maximum exploitation of the benefits of net centricity, it is critical to develop modified, or even new, tactics and procedures. By contrast to the USAF result, the US Army's Force XXI Advanced Warfighting Experiment claimed an increase in operational tempo of a factor of 6 (or 8 dB), and an increase in lethality of a factor of 10 (10 dB) as a result of networking [12]. These factors are clearly large enough to satisfy Morse and Kimbell's criterion, and so provide some grounds for optimism that the MAR AG-1 study will show an increase in military effectiveness consequent on the adoption of NCMW.

2. Characteristics of Net-Centric Military Systems

Characteristics of very many types have been ascribed to network-centric systems. These can be viewed as a hierarchy, with physical attributes of equipment at the base and characteristics higher up the hierarchy depending on those below. This is like the hierarchical structure often used for measures of performance (Appendix A), but with more levels. Figure 2.1 shows the full list of characteristics. We concentrate on those towards the top of the hierarchy, since these are more likely to be useful in providing metrics for network centricity.

At the top level in the hierarchy lies a set of characteristics that have been seen as 'emerging' from increased networking capability; they are properties that a network-centric force is supposed to display. These are reviewed in §2.1, followed by a discussion of concepts of command and control (C^2). This sets the framework for evaluating the effects of network centricity (§3). Concepts introduced here appear to scale from broad to narrow applications and from high to low levels.

The next level of the hierarchy is decision making, a large topic that is the subject of a companion paper [47]. The main points of this study are summarised in §2.3. Below decision making in the hierarchy lies information; a discussion of some theories on the nature of information is included in addition to the properties of information. Below this again lie the general characteristics of networks *per se* (§2.5).

Top level—force-level characteristics:
- speed of command
- self-synchronisation
- effects-based operations
- information superiority
- force agility and massing of effects
- shared situational awareness
- reachback
- interoperability

Second level—characteristics of decisions:
- speed
- soundness

Third level—characteristics of information:
- relevance, clarity
- accuracy
- comprehensibility
- value
- timeliness
- consistency
- secrecy
- degree of interoperability
- age, currency
- completeness
- authenticity

Fourth level—general characteristics of networks:
- availability
- reliability
- concurrency
- survivability
- coverage, homogeneity
- security

Base level—physical properties
- bandwidth, network topology, server speed etc.

Figure 2.1: The characteristics of a network-centric military system discussed in this paper, arranged as a hierarchy: characteristics depend only on those at the same level or lower in the hierarchy.

2.1 Top Level—Characteristics of a Network-Centric Force

At the highest level in the hierarchy of characteristics lie emergent properties of net-centred systems, properties that a network-centric force is supposed to display [3,16, 48]. The characteristics discussed are those listed at the top of Figure 2.1.

2.1.1 Speed of Command

Speed of command may be defined as the time required to complete one full cycle of Boyd's observe–orient–decide–act (OODA) loop. That is, it includes the time required to detect objects and activities of interest—the 'observe' part of the cycle—and the time taken in implementing decisions—the 'act' part of the cycle. This definition has the advantage of capturing any shortening of 'observe' time by advanced sensor networks and of the 'act' part of the loop by direct sensor-to-shooter communication. (Note that this is not the same as decision speed. The distinction between these two is elaborated in §2.3.2.)

Some authors have argued that the OODA loop is insufficiently sophisticated to provide a useful representation of organisational decision-making at the highest level [16(p.133)]. However, Smith [26] successfully uses the OODA loop in a high-level analysis of the Battle of Midway, and also in other strategic-level examples illustrating the importance of increased speed of command. Moon *et al.* [49] give a more abstract discussion of the OODA loop, on the basis of which they make useful comments about NCW, an example of which is described in the next paragraph. Official Department of Defense reports to the U.S. Congress use the OODA loop to illustrate concepts of NCW [3(p.3-18),50(p.C-1)]. Polk [51] critically examines the application of the OODA loop in the land domain, concluding that '...Boyd Theory [i.e. the OODA loop] as a major contributor to the modern maneuver warfare movement has even more to offer the Army at the turn of the century than ever before.' Moffat [52] and Essens [53] use the OODA

loop, or close variants, as a basis for analyses of command processes. These examples show that the OODA loop, as a fundamental concept, is a useful tool for discussing operational tempo, whether in NCW or otherwise.

Moon *et al.* [49] analyse a simple attrition-warfare scenario showing that, to obtain a significant increase in overall effectiveness, one's own speed of command needs to be about twice as fast as that of the enemy. On the other hand [54],

> '... speed of command is, in itself, *not* necessarily an unmitigated good. Rather, the quality and timeliness of decisions are what is really important. Thus, the OODA Loop premise that "acting inside an opponent's decision cycle will bring success" will not work if the decisions lack quality. Bad decisions—no matter how quickly made—are still bad decisions.' (emphasis original)

That is, it is not enough to 'get inside an enemy's OODA loop'; what one does once inside is also important [32] (See also §2.5 of Ref. 47). The situation is in fact more complicated than the above quotation suggests: decisions are not simply 'good' or 'bad'; rather there is a range in quality. In a given set of circumstances, a marginally sub-optimal decision made and put into effect quickly might produce a better outcome than the best decision made slowly. Also, a very high speed of command, compared with that of the adversary, may enable the effect of a bad decision to be countered by a subsequent decision before the adversary has had time to exploit the mistake.

These considerations indicate that speed of command—the time taken for a full cycle of the OODA loop—is a useful measure of system performance, but should be used with a measure of the effectiveness of the outcome. Some suggestions on how to implement this, from the point of view of both command speed and effectiveness of outcome are given in Table 2.1. The first entry in Table 2.1 is an example of a well characterised and familiar task. The second entry is a generalisation of the first to any situation in which one is reacting to adversary action. Here, 'preplanned' means that the response is selected from a range of possibilities determined ahead of time. The third entry in Table 2.1 shows a general metric for proactive actions by own forces. The concept of outcome effectiveness is closely related to, but generalises, decision soundness (§2.3.2 below).

Table 2.1: Examples of metrics for the characteristic 'speed of command'.

Metric	Description
OODA-loop cycle time	
Time to prosecute adversary platform	Clock starts when adversary platform enters region monitored by own sensors (ground-truth time) and stops when engagement* is completed. (Clock is reset if platform leaves monitored region before it is engaged.)
Time taken to undertake a contingent action (whether preplanned or not)	Clock starts when trigger for contingent action occurs (ground-truth time) and stops when action is complete.
Time to undertake self-initiated action	Clock starts with commencement of planning and stops at conclusion of the action.
Outcome effectiveness	
Probability of Red mission kill	Probability that adversary platform is prevented from executing its intended task.
Correlation of actual to planned outcome	Probability of action having the planned result, or fraction of planned goals achieved.

* 'Engagement' must be defined for each application in a manner that matches the way in which the metric is to be used. See text for discussion.

Despite the clearly defined nature of the task 'prosecute adversary platform' (first example in Table 2.1), the definition of the metric requires interpretation depending on the particular scenario and the manner in which the metric is to be used. The issue here revolves around the definition of 'engagement'. For example:

- Consider the prosecution of a submarine. The release of a torpedo would usually be followed by observation in an attempt to determine whether a hit occurred. Should this be considered as a second OODA loop, starting at the completion of the run out of the torpedo? To do so would follow the conventional OODA paradigm, and may be useful in some circumstances. However, a difficulty arises if one intends to compute an average loop time; for the second loop benefits from all the tracking information gathered during the first, and so will almost certainly be shorter. To ensure that only like quantities are being averaged, 'engagement' should be taken as the whole prosecution, including observation following the first fire and any subsequent ordnance release, until the prosecuting platform terminates the engagement.
- To generalise the above point: if loop cycle times are to be averaged then the definition of the cycle should ensure not only that only like quantities are averaged, but also that the quantities being averaged are independent of each other.
- In the case of aircraft or fast inshore attack craft, usually there will be more than one adversary platform. One could use different OODA loops for each, with several clocks running, in effect. Alternatively, it may be preferable to consider the prosecution of the formation of adversary platforms as a whole. For example, if own forces can react quickly enough to destroy each successive platform as soon as it enters the area of operations, then one has denied the adversary's attempt to amass effects. It may be easier to recognise this outcome if the whole attack is treated as one engagement, rather than dealing with each adversary platform separately.

2.1.2 Level of Agility Coupled with the Ability to Amass Effects

It is said that increased network centricity should increase the ability of a force to achieve a massed effect at a critical point in the battlespace, and then to reorganise quickly to amass effects elsewhere as the situation develops. The concept is that military units will be able to be well dispersed, yet able to bring the massed forces to bear where and when required [55]. Clearly the ability to conduct these types of operations requires knowing the when and where, which implies a high speed of command or high situational awareness, or both.

Massing of effect does not necessarily require physical aggregation; it is the massing of firepower, communications jamming capability, sensor coverage, etc. that is important. For example, the continuing development of precision guidance munitions is steadily eroding the long-standing link between range and accuracy, so allowing the massing of firepower from widely dispersed platforms. Remotely deployable sensors are likely to provide in the future a similar capability as regards sensor coverage.

Closely coupled with the ability to amass effects is an increased level of agility. Here agility is not necessarily a capability to move a weapons platform, instead it is the ability to reconfigure resources quickly—to move from one force organisation to another, as battalions in the Napoleonic conflicts moved from square to line and back again as required. In the context of modern warfare, force agility includes the ability to alter the nature of the engagement quickly, as for example shifting from ordnance delivery to counter measures such as jamming, and the ability to sustain several types of engagement simultaneously as required.

Table 2.2 lists examples of metrics for agility and massing of effects.

Table 2.2: Metrics for force agility and the ability to amass effects.

Metric	Description
Massing of effect	Quantity and accuracy of firepower, jamming capability, sensor coverage, etc. delivered to a critical location in the battlespace.
Force redirection	Time required to redirect already amassed effects to another location—will probably depend on the distance between locations, particularly if the new location lies beyond current own-force control radius [56,57].
Force flexibility	Time required to change the nature of the effect being amassed.
Parallelism	Number of simultaneous effects amassed or targets affected.

2.1.3 Degree of Self-Synchronisation

The issue here is not just synchronisation—a prerequisite of the ability to amass effects—but *self*-synchronisation. In our view, this concept does not require every unit commander to draw identical conclusions from the available information, so as to ensure robot-like lock-step action. Rather, it means that the theatre commander's promulgated common intent, in concert with knowledge of other unit commanders' likely reactions to the situation at hand, allows unit commanders to synchronise their units' individual efforts so that they are mutually supportive in the accomplishment of the overall goal, without the need for detailed centralised control.

Whether self-synchronisation is important or not hinges on the structure of the networked force and the manner in which net-centric operations are conducted. It is widely held that a 'swarming' style of combat is desirable [17,58–62] and would be enabled by a high level of net centricity. Pure swarming requires a high level of self-synchronisation, since the force is structured as a collection of many small semi-autonomous units. Each unit commander decides independently, with no more than broad guidance of the theatre commander's intentions, how the unit shall deploy. Clearly, each unit commander in such a force would require access to accurate and up-to-date information on the state of the battlespace. However, such an information system also permits a high degree of centralisation—exactly the opposite C^2 structure from that usually envisaged as arising from increased net centricity. For, if each unit has access via the network to sufficient information to enable self-synchronisation and swarming, then the same detailed information is available in real time to the highest level of command. As FitzSimonds writes [63]:

> 'The result is likely to be a highly centralised planning *and* execution process like that evident in HUNTER WARRIOR [the US Marine Corps's 1996 "advanced warfighting experiment"], where individual field troops were essentially reduced to passive battlefield sensors directly supporting a single ordnance-allocation authority. Recent war games have surfaced the possibility that relative ordnance scarcity [occasioned perhaps by the cost of modern precision-guided ordnance] may oblige future theater commanders to withhold authority from local commanding officers even to expend their own weapons in unit self-defence—surely one of the most jealously guarded prerogatives of "command".'

Further [63], '...future knowledge-empowered commanders are likely to find it ethically unacceptable to absolve themselves of accountability for lower-level actions of which they have full knowledge and control, and for which they are ultimately responsible.' Thus, the consequence of increased net centricity could be an *increase* in the centralisation of command [43,63,64]. The tendency to centralisation was manifest in Operation Enduring Freedom [29] and below the divisional level in the first Gulf War [51,

65]. This is completely inconsistent with a swarming style of combat, but if effects can nevertheless be amassed, then a greater overall combat effectiveness could result.

On the other hand, it is widely assumed that a reduction in command centralisation is an effective way to achieve a significant increase in the speed of command [16(p. 215ff.),17,19,60,66(p.4-2),67(p.8-1),68]. So, *self*-synchronisation may be seen as desirable for this reason. A metric for it must distinguish it from agility and the ability to amass effect under centralised command; in effect, the 'synchronisation' aspect has been addressed already under 'ability to mass effects'. Hence, metrics suggested here (Table 2.3) as a pointer to the level of self-synchronisation concentrate on the extent to which commanders at the unit level have autonomy and are willing use it.

2.1.4 Level of Shared Situational Awareness

Shared situational awareness may not be needed if the force is operating under highly centralised command, but it is crucial for swarming [58–60]. It does not mean that every unit need know everything that there is to know about the battlespace; '...in fact, flooding the network with information will guarantee that shared awareness does not occur' [60]. Rather, '...all involved [should] have the capability to share and access needed information' [69(p.12)]. The goal is to ensure that all unit commanders agree on the essentials of what is happening at any point in time and on the desirable way forward, and continue to agree as the battle progresses. Thus, a metric for this characteristic should not be the amount of information available, nor its accuracy, completeness etc. Rather, it should reflect the commanders' decision-making processes—the degree of commonality of the conclusions to which they are led by the information available to them, and the actions that they plan in consequence. Some suggestions on suitable metrics are given in Table 2.4. Note that what is being measured is the level of agreement between various commanders in a force, not whether the common picture agrees with ground truth. Where the accuracy of the common tactical picture (CTP) is an issue, it should be the subject of a separate metric.

All the metrics presented in this report may be time-dependent, but this aspect is perhaps most pronounced in the metrics of Table 2.4; it is to be expected that values of these could change markedly during the course of a battle. There is also the difficult question of exactly how to obtain numbers that represent commonality of or differences in understanding. This remains to be resolved.

If it were possible to achieve fully shared situational awareness among unit commanders who clearly understand and fully accept the theatre commander's intent, then concerns about increased net centricity leading to extreme centralisation of command

Table 2.3: Examples of metrics for the 'degree of autonomy' aspect of self-synchronisation.

Metric	Description
Degree of autonomy of unit-level commanders (qualitative)	Extent to which unit-level commanders have explicit authority to manœuvre, commit fire etc.*
Degree of autonomy of unit-level commanders (quantitative)	Percentage of orders from the theatre-level commander that do *not* attempt to prescribe the detail of unit-level operations.
Extent to which unit-level commanders exercise autonomy	Percentage of actions/operations/initiatives that actually originate from unit level as opposed to theatre level.

* Rules of engagement (ROEs) often place significant constraints on unit-level commanders. In some situations, a particular ROE may either enhance or degrade the effect of an increase in network capability. The degree to which this is permitted to influence the conclusions of a study must be judged on a case-by-case basis, bearing in mind the aims of the study.

*Table 2.4: Examples of metrics for the level of shared situational awareness.**

Metric	Description
Commonality of (or complementarity† between, as the case may be) CTPs	Differences among commanders in their comprehension of the tactical situation.
Commonality of purpose	Differences between unit-commanders' understanding of the theatre-commander's intent.
Commonality of expectations	Extent to which one unit commander is surprised by the actions or omissions of another.
Commonality of action	Differences in the battleplans of different unit commanders, in so far as these affect each other.

* In all cases, the smaller the value, the better.
† Commonality is not required between unit commanders operating in disconnected parts of the battlespace. In these cases, complementarity between CTPs is the appropriate concept.

authority should be obviated. For if a theatre-level commander knows that a unit commander is about to embark on an unwise course of action then, when situational awareness is fully shared, the unit commander also knows that his or her plans are unwise. This is like the Nelsonian 'band of brothers' concept of the relationship between various levels of command: all commanders are confident in their knowledge not only of the plans of their fellows, but also of how each will respond to emerging contingencies [70(p.21)]. To work in the modern context, the band of brothers would have to encompass many more officers than Nelson had to deal with, and over a wider range of rank. If this can be done, and making the assumption that unit commanders would strive to avoid unwise actions, it should then be rare for a theatre-level commander to need to intervene in unit-level operations.

2.1.5 Ability to Conduct Effects-Based Operations

Smith [26] describes 'effects-based operations' (EBO) as outcome-oriented activities aimed at enemy behaviour, so that the objectives are psychological rather than physical: '... they are focused on the enemy's decision-making process and ability to take action in some coherent manner'. In short, this is the age-old goal of attacking the adversary's will to fight. 'Put simply, EBO seek to defeat an adversary's strategy and resolve instead of merely attriting his armed forces' [71(p.22)]. Planning must focus on effects rather than means. For example, targets should be selected for psychological and strategic impact rather than solely on the basis of the level of attrition likely to be achieved. It has been noted that modelling EBO is difficult because it logically requires a model of the opposing leaders' psyches [72].

The concept is that EBO would be facilitated by the improved understanding of the battlespace, faster command cycles and precision targeting that are expected to result from NCW. EBO imply using these to identify and target enemy C^2 networks, with the aim of cutting the connections between their sensors, shooters and command hierarchy. In addition, elements of information operations (IO) are likely to be involved, to target the actual commanders and not just physical C^2 systems. Here again, the increased knowledge of the battlespace and of the enemy expected to be available through networked information sources and reachback to cultural experts should facilitate these operations. However, access to current HUMINT (human-sourced intelligence) is the critical element for EBO, and it is the extent to which a network can facilitate the use of HUMINT that will determine whether the network has a positive benefit as regards EBO.

Table 2.5: Generic metrics for the conduct of effects-based operations.

Metric	Description
Degradation of enemy resolve	Reduction in duration of adversary resistance from that expected without own effects-based focus
Degradation of enemy operations	Reduction in adversary's MOE from that expected without own effects-based focus.

Table 2.5 shows two generic metrics for EBO. These are intended to focus on the extent to which an operation is effects-based, rather than the quality, speed, etc. of the military outcome. That is, the metrics in Table 2.5 can be correlated with other measures of military effectiveness to determine the degree to which EBO have been useful in the given circumstance. Because of the general nature of the concept of effects-based operations, these metrics must be adapted to each specific case.

2.1.6 Reachback

Reachback is the ability to access resources that are not locally available. In many senses, the ability of infantry to call in an airstrike or artillery barrage embodies the essence of the concept. However, in the NCW literature, the concept goes well beyond requests for ordnance delivered to a target. Britten [73], for example, advocates leaving at home the majority of the personnel and equipment required to plan large-scale air operations. The U.S. Navy posits the linking of sonar operators with third-line and fourth-line sonar analysts, giving the operator on the scene reachback to subject-matter experts (SMEs) in real-time.

Most of the few articles in the literature on reachback are currently focused on the provision of access to SMEs, usually by having them on call in some way. Perhaps the archetypical example of reachback to a central repository of information was provided by the operation to rescue the Apollo 13 mission [74]. Neal [74] envisages such a repository as operating like a call centre, but goes further to the point that the SMEs would be pre-generating the information required, would have sufficient awareness of the situation in the battlespace to know who needs the information, and would be proactive in pushing it out to them.

Many successful examples of networked reachback can be found in the area of medical support, such as the increasing use of telemedicine in many countries. Equivalently, units on deployment have used digital cameras to send pictures of damaged equipment back to base for assessment, and for repair instructions to be faxed to the deployed units—simple but effective instances of reachback.

Table 2.6 shows examples of metrics for the effectiveness of reachback. The 'utilisation' metric is not independent of the other three: slow response, low quality or a

Table 2.6: Examples of metrics for reachback operations.

Metric	Description
Speed of response	Time from a request for resources until they are delivered.
Resource quality	Comparison between a locally available resource and that delivered by reachback.
Breadth of available resources	Extent to which reachback extends the range of available useful resources beyond that available locally.
Utilisation	Fraction of resource needs not available locally and available by reachback that are actually filled by reachback.

narrow range of available resources may be expected to lead to low utilisation. However, utilisation would also be affected by the level of networking available; it is this aspect that is intended to be captured with this metric.

2.1.7 Information Superiority

Information superiority is seen as one of the benefits of NCW. It is also an aspect of the second description of NCW given in §1.1 above (information domain, third dot point). The U.S. Department of Defense gives the following definition of information superiority [3(§3.2.1)]:

> 'Information superiority is a state of imbalance in one's favor in the information domain. Information superiority has also been described in terms of what is needed to achieve it; e.g., the ability to get the right information to the right people, at the right times, in the right forms, while denying the adversary the ability to do the same.'

This definition does not mean that the side with the most information automatically has information superiority. First, it does not matter how much information is available if it is not put to effective use; secondly one must take into account the information needs of the two sides: '...in asymmetric areas of capabilities, future adversaries with limited information requirements may have an informational advantage' [75 (p.16)]. Alberts *et al.* make the same point [16(p.55)]:

> '...we will face adversaries whose information-related needs will be asymmetrical to ours. What will matter is which force does a better job satisfying their respective information needs, not which side has better information-related capabilities. Thus the advantage is determined by comparing each side's information capabilities relative to their needs.'

As a crude and extreme example of this point, consider a conflict in which one side has precision guided munitions carrying conventional warheads and the other side is equipped with, and is prepared to use, missiles with nuclear warheads. The force with nuclear capability needs a much lower level of detail in its targeting information than the other, and so may achieve information superiority—an imbalance in its favour—with a lower level of information capability than the non-nuclear side possesses.

Is information superiority achievable? One enthusiast claimed over five years ago that the U.S. already has it [76], but others are much more cautious. For example, as regards the conflict in Somalia [40]:

> 'Clearly, the Somalis had information superiority. They knew what tactics we would employ; where our forces were stationed; what routes we would use to reinforce the Rangers; and how we would react to a helicopter shot down. They even knew the importance of immediate international media coverage; they had a plan to get media to the scene to record the event and then to get those pictures on the air.'

This is a striking example of the effect of asymmetry; technology alone is insufficient to guarantee information superiority. The Kosovo conflict provided another cautionary example [77]: 'Information superiority allowed NATO analysts to know almost everything about the battlefield, but NATO analysts didn't always understand everything they thought they knew'. This was in part due to a deliberate and low-tech campaign of disinformation conducted by Serbia. That campaign achieved a remarkable level of

success considering the asymmetry in capability. Because of these and similar examples, the balance of opinion seems to be that information superiority, though achievable, has yet to be achieved by western militaries [e.g. 78].

On the question of technology, there is an interesting polarisation of opinion concerning cost. Many sceptics of NCW claim that the technology envisaged as necessary to achieve information superiority is unaffordable [e.g. 36,38], while others point to the increasing reliance on commercial products and the astonishing reduction in the cost of commercial electronic equipment—a trend that shows no sign of nearing its end—to argue that cost will be no impediment, even for a non-state adversary [13,30,32]. However, this decrease in unit cost is offset by integration costs and the requirement to update equipment far more frequently than in the past. Also, commercial-off-the-shelf (COTS) equipment is sometimes not able to withstand the rigours of combat.

Table 2.7 lists some examples of metrics for information superiority. The last item refers specifically to adversary information *requirements*; denial of inessential information is excluded from consideration. Only this and the first metric address the issue of capability relative to needs, the other two are absolute measures and so are subject to the caveats expressed above. That is, the degree of information superiority is not affected by inaccuracy in or incorrect interpretation of unimportant information.

As with the metrics for the level of shared situational awareness (Table 2.4), there is a significant quantification issue for the metrics in Table 2.7. Here, the issue is how to quantify 'amount of information'. For data, one may count bits, but information is distinct from data, as discussed in §2.4.1 below. In specific situations, a natural definition of quantity of information may be possible. For example, in a platform-defence scenario, number of threat tracks may be used. However, such a simple definition may be problematic because it takes no account of track accuracy or completeness. That is, some tracks may contain significantly more information than others. How much of a problem this is depends on the use to which the metrics are being put.

2.1.8 Interoperability in the Information Domain

Two Aspects: Information Flow and Information Usage

NATO defines interoperability as 'The ability of...forces...to train, exercise and operate effectively together in the execution of assigned missions and tasks' [79].

Interoperability is usually viewed as primarily an issue of equipment and the interchangeability of consumables and spare parts, and only secondarily as the commonality of information-exchange protocols. However, in this paper, we put aside the equipment side of interoperability and concern ourselves with information interoperability, which we see as having two aspects. At the level of technology lies the question

Table 2.7: Examples of metrics for information superiority.

Metric	Description
Relative superiority	Ratio of information requirements, normalised to information needs, obtained by own force to that obtained by an opposing force (at some point in time, or as a function of time).
Accuracy	Percentage of information obtained that is actually true.
Comprehension	Percentage of information obtained that is correctly interpreted.
Denial effectiveness	Fraction of adversary information requirements that are denied by own deception, jamming, covertness etc.

of the degree to which platforms are able to exchange information. Security issues, which may be very significant in coalition operations, also affect information flow. Beyond this are cultural, linguistic, doctrinal and terminological issues that determine the degree to which information that is exchanged is comprehended and effectively used [80].

The information-flow aspect of interoperability is not a consequence of NCW but the reverse: it must be at a high level between many, perhaps most, of a force's platforms for the attainment of network-centric warfare. In view of this, information-flow interoperability belongs further down in the hierarchy of characteristics (§2.4.2 below). Interoperability is included here partly because it is a widely discussed characteristic of NCW, but more importantly because of the information-usage aspect. The majority of papers in the maritime-interoperability literature is concerned with the first, but the second aspect of interoperability is just as important. In essence, all the information flow in the world will not produce an interoperable force unless there is a congruence of language, culture, and above all mission. One of the biggest issues for any force, whether it be international, joint or even within the same service, is ensuring that units understand each other [81].

Although ease of information flow is a prerequisite for networking rather than a product of it, the case of information usage could be different. It is conceivable that an increase in the level of networking may help to raise the level of accessibility of meaning in the information passed, simply by providing the opportunity for greater familiarity and exchange of information between units. Insofar as this happens, information-usage interoperability can be viewed as an emergent property of network centricity; this issue is important for some of the discussions of C^2 in §2.2.

Some metrics for interoperability are listed in Table 2.8; the first two concern information flow, the last information usage.

Coalition Interoperability

Interoperability can be an issue even in single-nation joint-force operations, but it is a crucial aspect of the coalition operations that are commonplace in modern warfare. Usually cultural, political and military-doctrinal aspects are rather more significant in coalition than single-nation operations [66(ch.4),80,82,83] and security concerns may be a serious impediment to the flow of information between coalition partners [84]. In the long span of history leading up to World War II, coalition armies were by and large ineffective except in those cases where the coalition could quickly muster overwhelming force or came from a common cultural background. The well known constraints on the success of coalitions still obtain, but attention to the cultural aspects of interoperability has allowed coalition forces to achieve considerable success in the last half century [85].

Table 2.8: Examples of metrics for the degree of interoperability.

Metric	Description
Commonality of information availability	Percentage of unit commanders who can obtain published information, or the average fraction of the produced information that is available to unit commanders.
Ability to share information	Percentage of units that can feed usable information from their organic sensors to other units, or fraction of organic sensors that can generate sharable information.
Commonality of interpretation	Degree to which all units make the same assumptions about the nature of the information (e.g. shape of error bounds—rectangular, elliptical etc.—probability levels, measurement units, values of constants, etc.)

One of the most significant constraints on the success of coalition forces concerns the principle of unity of command; political considerations often prevent the appointment of a single commander with unfettered authority over the whole force. Other command structures, involving parallel command to a greater or lesser extent, have existed and may again exist [66,80]. Even if a unified command is established, the degree of subordination of units in a coalition force can be lower than that in a single-nation force; units of nationality different from that of the commanding officer might of their own accord choose to leave the battlespace, perhaps in response to their own nation's policy on the level of peril to which a platform may be exposed. Also, national leaders may choose to remove some or all of their units from the coalition at any stage.

There can indeed be an issue with lack of inter-service trust in a joint force, but trust may well be a dominant issue in a coalition force. With current security practices, there are almost certainly categories of information that one nation would not be prepared to share with one or more coalition partner. This compromises shared situational awareness and makes it difficult to establish a Nelsonian 'band of brothers' across the whole coalition. To the extent that swarming is regarded as desirable, the coalition may well have to adopt a hybrid mode of operation, with units from some nations engaging in swarming while those from other nations are subject to more centralised direction.

From the point of view of the overall measure of effectiveness (MOE), the requirement to operate in a coalition would therefore be expected to be at best neutral, but with a tendency toward reducing the MOE—that is, opposite to the expected effect of adopting network centricity. However, this may be outweighed by political or strategic benefits stemming from the formation of the coalition, or by the benefits obtained from an increase in the size of the force.

2.1.9 Comments and Summary

NCW and Devolution of Command Authority

As noted in §2.1.3, it is widely observed that a powerful network would enable a swarming style of combat, in which command structures are flattened and authority is devolved to quite low echelons. Many authors go further, positing that a devolution of command authority is a desirable consequence of, or even would necessarily result from, the adoption of a net-centric orientation [e.g. 16(p.218),19,55,67]. The latter is far from clear to us, because an increase in network capability could just as easily facilitate a concentration of authority in the hands of a central command, as noted in §2.1.3. That is, the issue of orientation—net-centric versus platform-centric—is entirely separate from the issue of the desirable degree of command centralisation. A highly capable network enables both greater devolution and greater concentration of command authority, compared with current practice. Which produces the greater military effectiveness is very likely context dependent and remains to be determined.

Networked Forces as a System of Systems

It is becoming common to observe that a networked force should be structured as a system of systems, rather than as one large complex system [e.g. 86,87]. What meaning is there in such a statement? There is no consensus on what the term 'system of systems' means, or even whether it is valid to conceive of the concept in terms of properties of the system in question [88]. However, one may discern in some authors [88–90] the distinctions detailed in the following paragraphs. On the balance of probabilities, it seems to us that these distinctions are what is intended by those who remark that a networked force should be organised as a system of systems.

In a system of systems, each component is itself a system, which means that it has the capability to act autonomously; its inputs and outputs are well defined and, most importantly, it has its own purpose or reason for being that can guide its independent actions. This individual purpose might be subsumed into a higher purpose when the system acts as part of a system of systems, but it can re-emerge if the system of systems should become dysfunctional for any reason. In contrast, the alternative structure of a networked force as a large complex system implies that the component parts need not be capable of independent action; if the overall system becomes degraded, then most or all parts of it may possibly become dysfunctional also, or purposeless if still functional. The advantage of the system-of-systems structure in terms of robustness is plain.

A second advantage to having components that are themselves systems lies in the facilitation of reconfigurability. As contingencies emerge, components can be reorganised quickly and with confidence if they have clearly defined inputs, outputs and purposes. In contrast, components that are not themselves systems may have complicated and ill-understood interdependencies that, if not correctly accounted for, may compromise the functioning of the reorganised system. As an example to help fix ideas, a complex system can be likened to the sort of ill structured computer program in which poor initial design is exacerbated by indiscriminate modification to the point that it is difficult to comprehend the operation of the program in detail or to verify its correctness. On the other hand, a well structured program has many of the attributes listed above of a system of systems. In this case, reconfigurability is likened to ease of maintenance.

Concerning the organisation of the components of the system, this is almost always hierarchical in a large complex system, but need not be so in a system of systems. The mutual independence of the components of a system of systems facilitates the forming of interrelationships that are as diverse and numerous as needed to maximise the performance of the overall system. Also, a system of systems has flexible interrelationships: linkages can comparatively readily be altered to improve performance or to adjust to changed situations.

Examples help to solidify concepts, but only if one accepts the view that a system may be validly classified as either a system of systems or a large complex system on the basis of its intrinsic properties. This view is denied by many systems theorists, but statements about the structure networked forces are meaningless without it. On this basis, then, the following examples are presented (other examples are discussed by Maier [90]):

- As noted above, a well structured computer program has many features of a system of systems. It has a hierarchical organisation. An unstructured program is also hierarchical, but is more like a large complex system.
- A modern naval frigate has many hierarchically-organised components that are ostensibly systems, but whether it should be considered as a system of systems depends on the extent to which the components have had their capability to act autonomously degraded by the process of integration. That is, although it is generally the intention that frigates and other modern military platforms should be systems of systems, many designs fall short of this goal in practice.
- A school of fish that manœuvres to avoid a predator is acting like a system of systems, but without a hierarchical organisation.
- The internet is a system of systems without an overall hierarchical organisation.

Modelling Approaches
This section (§2.1) surveys those properties supposedly resulting from the adoption of a net-centric orientation. In modelling NCW, a very high-level model could take some or all of the characteristics as inputs to a calculation of an MOE. However, the current level of understanding of these concepts in the military setting is so rudimentary that it would be more valuable to treat them as secondary outputs to be calculated from quantities lower down in the hierarchy (§§2.3–2.5). This would provide the possibility of learning about NCW as well as about the scenario modelled. To set the scene for the discussion of the lower-level quantities, the next section discusses issues of command and control.

2.2 Command and Control

2.2.1 The Place of C^2

The movement of information and the making of decisions is usually associated with the concept of command and control (C^2). Definitions and discussion of these terms sometimes confound the two and place more emphasis on control. The definitions given by the U.S. Naval Doctrine Command [66(¶301)] are:

> 'Command is the authority vested in an individual for the direction, coordination, and control of military forces. Through this vested authority the commander impresses his will and intentions on his subordinates. ...',
>
> 'Control is the authority exercised by a commander over part of the activities of subordinate organizations, or other organizations not normally under his command, which encompasses the responsibility for implementing orders or directives. ...'

These definitions highlight the two aspects: the authority to do things (command) and the exercise of that authority (control). A C^2 system is meant to assist in both. The importance of command as distinct from control is a recurring theme in the review of Bryant *et. al.* [11], and the two aspects are also highlighted by Pigeau and McCann [91–95] who, however, criticise the above definitions as circular. In addition, they identify 'command and control' as a concept distinct from both 'command' and 'control', an insight shared by other authors [e.g. 96–98]. Pigeau and McCann's definitions are:

> 'Command: the creative expression of human will necessary to accomplish the mission.'
>
> 'Control: those structures and processes devised by command to enable it [i.e. command] and to manage risk.'
>
> 'Command and control: the establishment of common intent to achieve coordinated action.'

As well as emphasising the two aspects of command and control, these definitions are motivated by a desire to '...reassert what may seem obvious: only humans command' [92]—which is achieved by inserting the proposition explicitly into the definition of command—and to emphasise the parts played by will and intent.

2.2.2 Command Issues—the Importance of Trust

The concept of command incorporates a complex set of relationships between people (and possibly machines), where there is an acceptance on the part of one person that

directives coming from another person should or must be carried out. Part of this acceptance may come from recognition that the directing person has a legitimate claim to authority derived from delegation from someone else whose authority has already been accepted. But history is replete with examples of troops who have not accepted what appears to be duly delegated authority. Thus, there is a second aspect to command that may be described as *trust* in the commander's capability to issue 'correct' directives. If subordinates trust their commander, they may even accept directives likely to result in harm to themselves. Subordinates' trust is a multi-faceted entity, possibly depending upon a common acceptance of the goal to be achieved, or upon the knowledge that doing other than accepting the directive will result in a worse result for the subordinates' goals. As an extreme example of the second case, if troops are told to advance or be shot, advancing at least offers the chance of survival.

Relying on fear of retribution for not following directives is generally acknowledged to be more susceptible to failure than relying on a shared view of what is best for a unit. In practice there is probably a mix of the two aspects in most command relationships. A major function of the maintenance of command, then, is maintaining the trust relationship. Britten [73] states in his work on reachback that a commander must lead people and this requires staying in touch with the people being led; it requires being seen to have an understanding of the troops' situation. This seems to be widely understood as necessary for successful leadership and command.

The command relationship of acceptance and trust works in the opposite direction as well, in that commanders must establish their own trust in and acceptance of the capabilities of subordinates. On both sides, the relationship may be improved by expressions of trust from one side to the other. What else builds trust? On both sides, familiarity could work either way, either increasing or diminishing the level of trust. The force of the commander's personality might engender trust in his troops, and trust in both directions can be earned through a history of loyalty [99]. The Dutch Army recognises mutual trust as essential for the successful application of their formal doctrine [100]. The four pillars of mutual trust are held by them to be: competence, openness and honesty, concern, and reliability.

In terms of force effectiveness, it is important that the trust relationship is based on realistic assessments of capabilities; that is, that acceptance of command authority does not let bad decisions go unchallenged and, on the other side, that a commander's level of trust in subordinates' abilities is based on a realistic assessment of the level of those abilities.

These ideas of commonality of purpose and trust may have important implications for whether a force tends towards distributed self-synchronisation or centralised control. There are also direct implications in terms of morale on the subordinates' side and on the appropriate use of information and task assignment on the commander's side to the maintenance of effective command relationships. If net-centric concepts lead to improved understanding by commanders of their subordinates and vice versa, then improvements in force effectiveness might be expected. It is also likely that a high level of such understanding is essential to the undertaking of effects-based operations. Measures of effectiveness for this might include measuring levels of trust in commander's plans, the match between a commander's understanding of unit capability and reality, overall morale etc., although morale has the disadvantage of poor discrimination: it is affected by many factors other than trust in the commander.

Table 2.9 lists some examples of metrics for mutual trust.

*Table 2.9: Possible metrics for mutual trust.**

Metric	Description
Trust from above	Level of trust of higher commanders in subordinate commanders' and troops' professionalism.
Trust from below	Level of trust of subordinate commanders and troops in higher commanders' decision-making ability and willingness to give support as required.
Trust at the same level	Level of trust of commanders in the ability and professionalism of other commanders at the same rank echelon.
Perception of commanders' perceptions	Degree to which troops believe that their commanders have a realistic appreciation of their capabilities in the given situation.

* In each metric, 'level of trust' may be read as referring to any of the 'four pillars': competence, openness and honesty, concern, and reliability [100].

2.2.3 Control Issues

The concept of control seems easier to approach from a technical point of view than that of command since, in simple terms, it is often seen mostly as consisting of processes of communications and decision making. These issues are discussed in detail in §§2.3–2.6. Outside of strict decision making on responses to opposition actions, control includes a measure of the application of retribution or reward to own forces, the fear of which is occasionally used to reinforce the command authority previously discussed. Bryant *et. al.* [11] report, however, that improved organisational effectiveness occurs when there is less retribution and more problem solving: an organisational structure that encourages the admission of mistakes leads to greater initiative and possibly to less control being required. In any case, control involves the monitoring of subordinate actions to ensure that they fall within the limits of delegated authority, and applying corrective measures when required, whether these involve problem solving or retribution. It requires making sure subordinates receive and understand both instructions and the authority to implement them, and the ability to dynamically change both as required.

A major issue in control is the level of detail in the control that is required for a given unit. There can be a tendency in inexperienced commanders to micromanage subordinates; while this may be an important part of developing the trust relationship required for the commander, it can also lead to the commander missing bigger-picture issues. Kahan *et al.* [101] state that, in general, commanders should not try to deal with detail at more than two levels below their command echelon. To do so is to risk degrading their command performance. Bryant *et. al.* also document numerous references to a two-echelon knowledge or information aggregation limit. They also report the concern by commanders to limit the amount of fine-tuning of plans, especially in time-constrained situations, since subordinates need the time to work up their own plans.

2.3 Second Level—Decision Making

Decision making is a large topic that is the subject of a companion paper [47]. Here, we summarise some of the conclusions and recommendations of that paper. The aim both there and here is to lay the ground work for going beyond modelling in which decision makers are assumed to have all the information that they need when they need it, that the information is fully accurate, that decisions are made instantly and with the ultimate in rationality, and that actions required by the decisions are executed

immediately and flawlessly. These assumptions seem too restrictive for a study of the processes involved NCW; this and the companion paper are aimed at formulating methods for relaxing one or more of them.

An important aspect of decision making is knowledge building—the process by which a decision maker uses information to obtain knowledge. Both how this occurs in practice and how it should ideally occur appear to be open questions in the literature. This paper does not enter into this debate, but assumes that appropriate methodologies are employed to obtain information and built it into actionable knowledge.

2.3.1 Decision Types

Decisions can be classified either according to the parts of the OODA loop (§2.1.1) involved in a given decision, or on a cognitive basis [47]. The cognitively based scheme results in the categories of 'analytical' and 'recognition-primed' decisions. Analytical decision making is the style long propounded in military doctrine: options are generated and evaluated, and the best option is selected for execution. This process is a heavy consumer of cognitive resources, that is, working memory and attention. It can also be slow. On the other hand, a recognition-primed decision involves the decision maker recognising a familiar situation and recalling an appropriate response, judged on the basis of direct experience, training or study. This type of decision making is rapid and requires few cognitive resources unless the option that sprang to mind has to be adapted to meet the needs of the situation at hand. It clearly relies on expertise: recognition-primed decisions can be made only by those with a store of experience on which to draw. Nevertheless, recognition-primed decision making is common in military operational contexts; it is estimated that over 90% of tactical-level decisions are recognition-primed [102,103].

2.3.2 Decision Quality

It is argued in the companion paper [47] that, notwithstanding the myriad of factors affecting decision making and the performance of decision makers, it is sufficient for the purposes of modelling NCW to quantify decision quality with just two characteristics: decision speed and decision soundness.

'Decision speed' should be regarded as the time taken execute the 'orient' and 'decide' steps of the OODA loop (§2.1.1). This definition avoids diluting the metric with the possibly protracted 'observe' and 'act' steps that are common to all types of decision making [47], while allowing for the shortening of the process when the decision is recognition-primed. As mentioned above, it is entirely possible that the result of the decision is to seek more information, that is, to dispense with the 'act' part of the current OODA loop and to start a new OODA loop. This is a fully legitimate conclusion of a decision-making process; it results in the clock being stopped, yielding a decision time, and being reset in preparation for restarting when new information has been observed.

'Soundness' is the degree to which the decision taken is the best possible. As discussed in Ref. 47, this can be interpreted in two ways: either the best possible decision under the circumstances prevailing at the time, or the best possible in an absolute sense. The first is appropriate when the focus is on the competence of the decision maker, the second when one is more interested in how improvements to the decision maker's support system and infrastructure can improve decision quality. In addition, 'best' requires interpretation in the context of the specific case at hand. For example, in some situations, the level of risk may be more important than in others; sometimes

robustness against flaws in execution may be important in deciding between options, and so on.

2.3.3 Modelling Decision Making

Because of the emphasis on command and control and because network centricity is mainly about information generation and flow, modelling the decision-making process is likely to be an important aspect of any study of NCW. However, the state of fundamental understanding in this area is such that a detailed representation is not feasible at present. This points to a probabilistic approach, so avoiding having to specify too much detail. It means that speed and soundness would each be specified by a mean, a standard deviation and an adopted probability distribution. Section 5 of the companion paper [47] attempts to develop a general framework for such modelling.

As noted in Ref. 47, there is both experimental evidence and theoretical support for the use of the inverse Gaussian distribution to describe decision speed, and data are available on values of mean decision times and their variances for the two types of decision, analytical and recognition-primed. In a model, a given percentage of decisions could be presumed to be analytical, depending on training and experience of the modelled decision maker, with a random variable used to determine the character of each particular decision.

Unlike decision speed, there is no empirical data known to us on which to base a probabilistic model of decision soundness. Also, the concept behind the probabilistic approach, in which a soundness value is selected at random at each modelled decision point, may be too coarse for many applications. Rather, it may be desirable to model the process of option generation and selection in more detail. Aside from the complexity of such an approach, difficulties in quantifying decision soundness are likely to arise in identifying the 'best possible' decision. The best possible course of action, in the absolute sense, is usually unknown to the decision maker at the time that the decision must be made. A possible approach, based on the construct of extant commander's intent, is developed in Ref. 47. Where the situation is too complicated for this to be feasible, a parametric study on mean decision soundness and its variance may be required. Comparison of a range of parameter values would simulate the effects of varying the decision-maker's competence and experience, and the effects of stress, cognitive biases etc.

2.4 Third Level—Information

Information is placed below decision making in the hierarchy of characteristics because it is the raw material required by decision makers. In a simulation-type model, one can envisage that, for example, decision time will depend on the characteristics ascribed to the information flow.

2.4.1 Information, Data, Knowledge, Belief

The distinction between data, information and knowledge is made by Seymour *et al.* [104] (also [105–107]), who define 'knowledge' as the final product of a sequence of transformations starting with data derived from the environment. An additional step, inserting belief between information and knowledge leads to the following [104]:

- 'Data' is the product of sensor systems, possibly following some automatic low-level processing such as threshold discrimination, Fourier transformation etc.

- 'Information' results from further processing of data to render it suitable for presentation to a human decision maker.
- 'Belief' is obtained by human processing of information.
- Belief becomes 'knowledge' after a certain level of confirmation derived from the processing of subsequent pieces of information. That is, knowledge consists of beliefs that correspond to the truth with a high degree of probability.

Burke [108] advocates including 'feeling', 'will' and 'thought' as categories above knowledge that lead to 'understanding', which is held to be an emergent property of a 'Thought System.' With the possible exception of will, which may have a place in defining 'command' [93], the usefulness of these higher categories to the analysis of NCW is not clear to the present authors.

A different view of the relationship between information and knowledge is presented by Griffin and Reid [45]. They regard knowledge development as a process of conceiving theories about the situation at hand and then seeking information to test the theories. The 'knowledge' of the situation consists precisely in the set of theories, together with the history of how each has fared under test. In this view, information does not lead to knowledge, rather knowledge arises from a process of creative conception by the commander. The function of information is then to test the conceptions.

From the point of view of modelling at a high level, it is recommended that the transformation of data into information not be represented in studies of NCW. This is equivalent to the assumption that this transformation is sufficiently rapid not to be the limiting step. It also can be rationalised by reference to the definitions of 'data' and 'information' given above. In terms of these, it is unlikely that the transformation of data to information will be much affected by the adoption of NCW. For example, an ASW combat system turns sonar data into tracks, which are information. With NCW, there may be many more data, but they will still be turned into tracks. On the other hand, the transformation of information to belief and belief to knowledge are part of the decision-making processes discussed in the previous section, which are expected to be strongly influenced by the degree of net-centricity of the force.

2.4.2 Characteristics of Information

This section lists many general attributes of information. The importance of a given attribute depends on the manner in which the network is implemented. For example, relevance and clarity may have less importance when unit-level commanders 'pull' information from the net, compared with the situation where the network 'pushes' information onto commanders.

Many of the properties listed below have two aspects, one that is intrinsic to the piece of information and a second that depends on the context: the use to which the information is being put, or the relationship of the piece of information in question to other pieces. In a model, it is envisaged that the context would be supplied as an input. Intrinsic properties might also be specified as inputs, but could equally well be derived as outputs from the model, depending on the level of detail modelled.

Relevance, Clarity

Relevance is the extent to which an item of information is required by the recipient. Each individual piece of information has an intrinsic relevance in a given scenario, but this may be altered, in either direction, by subsequent pieces of information. That is, several pieces of information may together have a relevance different from that of any one of them alone.

Relevance is an inherently binary quantity—a piece of information is either relevant or irrelevant—but uncertainty leads to the desirability of interpreting relevance as a continuous variable. For example, consider a piece of information that is relevant in situation A and irrelevant in situation B, but the commander does not yet know which situation pertains. If the two situations are equally likely, then it makes sense to say that the piece of information has a relevance of 0.5; if situation A has probability 0.1, then the relevance of the information is 0.1. That is, relevance can be taken as a probability-weighted mean.

Clarity is a contextual property intended to reflect degree of clutter: the extent to which a relevant item of information is obscured by a plethora of irrelevant items.

Timeliness

Timeliness is *not* the same as network bandwidth. A metric for timeliness must reflect the difference between the time at which an item of information is required and the time at which it is available—time of availability is an intrinsic property; time at which the piece of information is required is a contextual property. Timeliness is undefined for a piece of information with zero relevance.

Age, Currency

Age, an intrinsic property, is the time since the item of information was created or last updated. Currency is the contextual property that relates age to the time when the piece of information becomes so outdated that it can no longer reliably be used.

Accuracy

When an item of information is created, it has an intrinsic accuracy determined by the properties of its source. Contextual accuracy is a function of this and the perceptions of the recipient: the level of uncertainty in the recipient's mind over the degree to which the item of information corresponds to ground truth. By taking into account a recipient's beliefs, we include the effects of circumstances that cause the recipient to suspect that the accuracy of an item of information is more or less than its intrinsic accuracy. This could be important to decision making.

Consistency

Consistency is the extent to which a new item of information agrees with previous items, or with the local common tactical picture (CTP). This is clearly a contextual property. Lack of consistency could be a reason for a commander to downgrade the contextual accuracy of an item of information. This raises the complicated question of the processes by which misconceptions in a local CTP can be corrected by additional information.

Completeness

Completeness means the extent to which all the required parts of an item of information are present. Completeness is an intrinsic property acquired by information when it is created; it degrades as the information passes along unreliable communications channels or is held in storage locations that are less than 100% reliable (§2.5).

Comprehensibility

Comprehensibility is the ease with which the recipient can fuse the item of information into the local CTP. It is intended as an intrinsic property, despite its definition by way of a context. Low comprehensibility may mean that the information does not make sense to the recipient or that the form of the information is such that the recipient cannot easily integrate it into the CTP.

Secrecy

Intrinsic secrecy is a function of the source of information and the security of the communication channel (§2.5); it is degraded by transmission through a channel that is not 100% secure. The contextual aspect to secrecy concerns the extent to which the recipient suspects that the adversary may have intercepted the information.

Authenticity

Authenticity is the extent to which the recipient of information can verify that it has come from the purported source unaltered, as opposed to having been subjected to adversary information operations. This is an extreme aspect of secrecy; its degradation requires not only that adversaries can access the network, but also that they can alter information in a manner that is difficult to detect.

Intrinsic authenticity may be conveyed by trusted signatures, where they exist. As before, contextual authenticity refers to doubts that may be raised in the mind of a recipient. Degraded contextual authenticity does not require the adversary to have been successful in altering an item of information; it is enough for own commanders to suspect that it may have happened. Sowing doubt over authenticity is a powerful tactic for countering an opponent's network centricity ([75], Appendix C.3).

Value

Information value is usually defined as the extent to which possession of an item of information enables the recipient to perform more effectively [109]. With this definition, value is a higher-level metric than the others in this section—more of a measure of system performance than a measure of performance, in the terminology of Appendix A—since it depends on most, perhaps all, of the other properties of information. That is, value is not expected to be wholly independent of the other properties. It is a contextual property.

The definition has been interpreted as implying that a particular piece of information is of little value to a force if the force would probably win regardless of the availability of the information, or would probably lose even if it receives the information [109]. This interpretation depends on the MOE chosen. For example, perhaps possession of the item of information could lead to a win or loss with fewer casualties than would have been the case without it.

The concept that knowledge of a particular situation consists of the set of theories that have been created in explanation of it [45] leads to a different definition for the value of a piece of information: it is the utility that the piece of information has in testing the various theories. This emphasises an aspect of the contextual dependence of 'value'—information that can test a certain theory is of value to a commander only if the commander has conceived of the theory in question. The concept of 'value' given in the previous paragraphs is also context-dependent, but the context there is more physical than cognitive.

Degree of Interoperability

Degree of interoperability also appears higher in the hierarchy (§2.1.8, p. 13), where the distinction between information-flow interoperability and information-usage interoperability is discussed. The second is the high-level property; here we refer to the first.

As regards information flow, degree of interoperability means the efficiency with which a unit commander can obtain information from, or provide information to, the network. The first two entries in Table 2.8 (p. 14) list some metrics for this. It is a contextual property in that it depends not only on the characteristics of the piece of

information, but also on the nature of the recipient. The degree of interoperability required for a significant gain in MOE is a suitable question for any study of NCW to address.

Degree of information-flow interoperability could be interpreted as a property either of information or of the network. In view of the importance attached to interoperability in the NCW literature, it seems preferable to place it at as high a level as reasonable, so the metrics in Table 2.8 have been constructed to emphasise the information-exchange aspect of interoperability rather than the networking aspect.

2.5 Fourth Level—General Characteristics of Networks

Technical network characteristics are regarded as likely inputs for a study of NCW. That is, it is envisaged that as many of these quantities as required would be represented by variables that are varied from one run of the model to the next. For example, Davis *et al.* give rationales, in the context of modelling a military C^2 system, for utility functions for a wide range of network and information characteristics [110].

The following definitions are constructed with a modern communications network in mind. As described below in §3.2.2, there are many other types of networks of military relevance and utility for elucidating general characteristics of network-centric systems. However, attempting to generalise the definitions below to cover all types of networks of interest would unnecessarily complicate statements that are intended to be mainly illustrative. In most cases, the nature of the generalisation required for a given network type is plain.

Availability
Availability is the fraction of instances that a communications channel is accessible on the first attempt. Alternatively, it could be taken as the mean number of attempts required to obtain access to the channel.

Concurrency
By concurrency is meant the level of conflict resolution in the network; for example, the robustness of the procedures for dealing with a situation where two nodes in the network try simultaneously to update a piece of information.

Coverage, Homogeneity
Coverage refers to the percentage of the force that can access the network; homogeneity measures the extent to which different commanders have the same level of access. Both are intended to reflect the consequences of hardware variability across platforms. Coverage may also have a geographical aspect.

Reliability
Reliability has two aspects: the amount of distortion or corruption that the channel introduces into information passing along it, and the extent that information is protected from loss while not in transmission. Here, distortion or loss is viewed as being caused by hardware inadequacies, as opposed to enemy attack, which is the subject of the next two characteristics.

Survivability
Survivability is the degree to which the network can withstand physical attack and still function with given levels of availability and reliability or, alternatively, the level of degradation in availability and reliability that a given level of enemy attack causes.

Security
Security is the degree of difficulty experienced by the adversary in gaining access to the network, either to copy information or to alter it covertly. These are likely to be two different things; presumably it is easier to secure a network against data alteration than against data copying. Note that 'copying' means more than electronic copying; it may include activities as low-tech as an adversary making written notes or committing material to memory.

2.6 Base Level—Physical Properties

Quantities such as bandwidth, network topology, server speed, screen layout etc. are foundational in the sense that all higher quantities depend upon them. They are important in assessing specific implementations of a system, but it is expected that the relationships between these quantities and the higher-level properties are very complex and hence difficult to determine verifiably. For this reason, we recommend that studies of NCW avoid dealing with physical properties, taking instead network properties and perhaps some information or decision-making properties as inputs.

3. Discussion—Network Centricity and Information-Based Warfare

The previous section contains a review of concepts and issues from the literature on net-centric warfare, command and control, and decision-making. In this section, these concepts and issues are examined to further the understanding of what it means to be net-centric and explore some consequences of network centricity.

For the purposes of this section, we take a 'network' to be a system of resource nodes plus the constrained capabilities for moving resource elements between specific nodes. Early in §3.2, the scope of the discussion is restricted to high-capability modern communications networks. From there, we broaden our considerations to encompass a wide range of other network types, such as road networks and social networks. For any of these, a particular network may or may not be complete in the graph-theoretic sense, namely that resources can move directly between any pair of nodes. Similarly, node links may or may not be reciprocal; for example a node may be able to move resources directly to another node but not receive directly from that node. However, it is assumed here that the network is connected; that is, that there is at least one route from a given node to any other node.

3.1 The Importance of Understanding the Nature of Net Centricity

In assembling the review of §2, we found ourselves frequently asking the question in regard to a concept or behaviour pattern: 'is this net-centric?' Section 3.2 presents our approach to this question, but first it is appropriate to reiterate why the question matters; why, that is, one would invest effort in seeking to understand and define network centricity.

The recent very great advances in information network-based technology, of which the rise of the internet is perhaps the most visible, can reasonably be expected to

be of significant potential benefit to the military. They could lead to capabilities that are scarcely possible in the absence of networking, or possible only at great cost, resulting in greater flexibility, allowing a force to be able to deal with a wider threat spectrum, and higher efficiency of operations, so that more can be accomplished by a force of given size. The question is, how should military forces be structured to maximise these benefits? Proponents of NCW answer: 'by becoming net-centric'. That is, it is desirable to do more than just put a high-capability network in place. It is entirely plausible that the provision of high-capability communications networks to a military of traditional structure and concepts of operations would lead to improvements, but much greater improvements are available, it is claimed, if the military restructures and adapts its concepts of operations to become network centric.

To test this point of view, it is necessary to know what is meant by net centricity, and to be able to recognise it, or its absence, in any given instance of military organisation or behaviour. For it is only with this capability that it becomes possible to quantify the extent to which military operations may benefit from NCW and to identify paths toward network centricity. The last point is very important: a fundamental issue for military decision makers is to choose, within the constraints of available resources, among the many ways in which forces could be restructured to use communications networks efficaciously, and in which the networks themselves could be structured.

From the point of view of paths toward network centricity, it is useful to regard net centricity not as a binary property, either present or not, but rather as a continuum ranging from platform centricity—complete absence of any net-centric orientation—to full network centricity. That is, it makes sense to conceive of partial network centricity. This point is elaborated in §3.2.3, but first we consider how to identify network centricity in any given situation.

3.2 What is Net Centricity?

Is such-and-such network centric? The obvious approach to answering such a question is to look for the characteristics of network centricity (§2.1) but, for reasons detailed in the next section, we are unconvinced that these properties have diagnostic force; it is possible to conceive of non-network-centric systems that display the characteristics, at least when taken one by one and when 'network' is taken to mean a high-capability communications network. Having reached this point, we were led, via consideration of several examples, to formulate a concept of network centricity that is, we believe, more diagnostically useful than previous conceptions. Like all attempts so far at defining network centricity, ours is derived from a list of properties that, in our view, characterise a net-centric system. This section presents this view of net centricity, beginning with the difficulties that motivated its development.

3.2.1 Emergent Properties of NCW as Indicators of Net Centricity

Section 2.1 details the supposed emergent properties of NCW. In much of the literature, it appears to be assumed that the occurrence of one or more of these emergent behaviours is direct evidence of net centricity. It is, however, not clear to us that there is an immediate or direct relationship between the advanced use of network technology and many of these properties. Nor is it clear that there is anything revolutionary about these concepts or, if revolutionary, what the nature of the revolution is.

The basis upon which the properties of §2.1 are used to define net centricity is the claim that they are emergent properties of increased networking. A well known

example of an emergent property is intelligence, arising from the accumulation of neurons. Somehow, the combination of many simple objects and processes—neurons and their connections—combines into a complex system from which intelligence emerges. How this happens is unknown, although the importance of complexity *per se* is generally recognised. It is not required that an emergent property to be beneficial or desirable, but all properties so far identified as emerging from network centricity in warfare can be beneficial. In most of the literature on NCMW, it is assumed that the benefits of network centricity will vastly outweigh any negative impacts.

Just as intelligence is supposed to emerge from a sufficiently complex arrangement of neurons, it is argued that, from networking technology and the correct (i.e. network-centric) conditions, the properties of §2.1 arise. The reverse is then widely assumed: the presence of these properties is an indication that the system must be net-centric. In this section, each of the properties of §2.1 is examined in turn to see how far this assumption is valid.

Speed of Command

Putting to one side the question of whether an increase in the speed of command promotes military effectiveness, here we address the question of whether a net-centric focus can produce a higher speed of command than is possible by any other means. It is not relevant to note that a network might actually slow the speed of command (due to, for example, information overload); that is the equivalent of noting that a complex system need not be intelligent. The correct question is: can one achieve a speed of command higher than is conceivable without a net-centric orientation? The answer might be yes, but that then raises the question of degree. Many systems patently without a high-speed communications network have nevertheless displayed remarkably high speeds of command. A well known example is the Mongol invasions of the thirteenth century.[†] So, how fast must the speed of command be to provide evidence of network centricity? There is no clear answer to this question, and hence it is difficult to use elevated speed of command to label a system unambiguously as net-centric.

Level of Force Agility and Ability to Amass Effects

Level of agility pertains to the ability of a force to react to new circumstances and revise its organisation to handle them. A prime example is the army battalions of the mid 1800s that could quickly change formation in order to handle the diverse threats of artillery and cavalry (line-a-breast and square respectively). Perhaps the prototypical example of force agility was displayed by the Mongol warriors. As regards massed effect, in Napoleonic times weight and quickness of fire were needed to offset a lack of accuracy of aim. In World War II, the carrier battle group was a potent example of both agility—its manœuvrability and the reconfigurability of its aircraft—and massed effect. These examples of force agility and the ability to amass effects were entirely adequate

[†] '...such was [their] speed and ardour..., that in less than six years, they had measured a line of ninety degrees of longitude...' [111,p.77]. During the campaign for the conquest of Hungary, the Mongols at one stage famously travelled 180 miles in 3 days to outmanœuvre Polish and German reinforcements and rout the Hungarian forces [112]. The result was catastrophic: 'The whole country north of the Danube was lost in a day and depopulated in a summer' [111,p.78]. During the conquest of Persia two decades earlier, the Mongol forces frequently took towns by surprise because they travelled faster than the news of their coming, a feat that no modern force of similar size (Gibbon estimated ~700000 warriors) could expect to equal. Here, too, devastation was extreme. Writing in the late 1700s, Gibbon commented that 'five centuries have not been sufficient to repair the ravages of four years' [111,p.64]. None of this would have been possible without an efficient C^2 system that was very fast for the age.

for the needs of the time, and all were achieved without a network in the modern sense. Hence, although force agility is probably enhanced by net centricity, it cannot be used as a defining property of a net-centric system.

Self-Synchronisation and Shared Situational Awareness

NCW orthodoxy says that increased networking would produce increased joint situational awareness and, when this is coupled to a common sense of purpose and a high level of interoperability, units will naturally self-synchronise their resources so that the requirement for a central command hierarchy would be reduced. This would in turn enable swarming tactics with smaller platforms. As with speed of command, we set aside the question of whether swarming is an effective style of combat, and also the point that the existence of a network could just as easily promote a centralisation of command (§2.1.3). The question here is: is self-synchronisation inconceivable without a network-centric focus?

A cursory glance at historical examples of swarming given by its proponents [59 (p.28)] suggests that the answer is 'no'—the Athenian Navy at Salamis, the Mongols, the British Navy defeating the Spanish Armada, American Minutemen against British regulars are all examples from before the rise of modern communication networks. However, these examples refer to swarming, not self-synchronisation. They show that the ability to conduct swarming does not require net centricity, but say nothing about high levels of self-synchronisation. It seems that, however much swarming requires trust and shared intent, only infrequent episodes of synchronisation are needed.

In fact, it *is* possible to conceive of a force without a network but nevertheless self-synchronised and with a high degree of shared situational awareness. It could look like the following: each unit in the field has its own sensors sufficient to inform it of conditions in its portion of the battlespace. The common intent is already promulgated. Unit commanders have previously trained together sufficiently extensively to be confident that they know how their colleagues will respond to the situation as it unfolds. This scenario encompasses the elements required for self-synchronisation and shared situational awareness, without the necessity for any communication between unit commanders. It is not claimed that this is the best or most efficient manner to achieve self-synchronisation—using a network may well be better—but the fact that it is conceivable shows that self-synchronisation and a high level of shared situational awareness are not sufficient to characterise a system as network-centric.

The scenario outlined in the previous paragraph may seem rather forced, but it is not so far from reality in coalition operations when security considerations constrain the passage of information between national forces. Then it might be the case that each nation is forced to rely more or less on its own sensors. However, given a clearly understood common intent, effective liaison staffs and a sufficient background of personal contact between officers of the various nations, the whole force may be able to self-synchronise even in the absence of comprehensive sharing of information between the various national groupings.

Conduct of Effects-Based Operations

'Effects-based operations' means the concentration of operations on the adversary's will to fight. This is an age-old goal [113(book 3)], one that was conceivable and indeed pursued as practical doctrine long before the rise of modern communications. So it is clearly not one that requires an electronic network in the current sense of the term.

The key to EBO is an understanding of the opponent, their objectives, concept of operations etc. This type of information is fundamentally based upon HUMINT, not

extended sensor nets; however, the application of this information is likely to require precision sensor information and the collation of disparate data, which may be more available using network resources.

Reachback

One might argue that reachback could be carried out by telephone or, even more extremely, by signal fires. However, the level of resources accessible by these means is very limited, so that the activity scarcely qualifies as reachback in the modern sense. The situation here is different from that concerning speed of command, for which one has the problem of deciding how fast is fast enough to qualify as network centric. With reachback, the differences are of kind rather than of degree; if the outcome of reachback requires graphics, video, large text documents etc, then a modern network must be involved. Hence, the provision of high-level reachback services indicates the existence of a high-capability network. Whether net centricity then automatically follows remains to be determined. (This is considered in §3.2.3.)

Information Superiority

As with effects-based operations, so with information superiority: the goal of knowing the adversary while achieving covertness oneself is age-old (Appendix C.1). Hence, the same argument applies—if it could be conceived of and pursued as practical policy so long ago, then it is achievable in the absence of a modern communications network and so is not an indicator of network centricity. However, as with self-synchronisation, the availability of a high-capability network is probably the only really practical way of achieving information superiority, at least where large forces or multi-mission operations are involved.

Interoperability of Information Usage

The term 'information-usage interoperability' is used here to encompass all those aspects of interoperability that determined the extent to which information received is understood and can be put to effective use (§2.1.8). Once again, although the presence of a network might facilitate information-usage interoperability, it is not necessary. Other media for promoting effective information usage are eminently conceivable and probably more effective, such as liaison staff, extensive personal contacts between staffs of different nations and services, and appropriate training.

Summary and Comments

The arguments of this section can be summarised as follows: network centricity cannot exist without a high-capability network yet, except for the provision of a significant reachback capability, examples can be found of systems without networks that display each of the posited emergent properties of net-centric systems. Hence, apart from reachback, these properties cannot be used as indicators of network centricity. The fact that provision of reachback might be an indicator of network centricity is hardly very strong—a system could be network centric without having a reachback facility available.

Most of the examples cited in this section, and on which its conclusion is based, are taken from history; some of them occurred many centuries ago. How relevant are they to modern warfare? The distinguishing features of modern warfare include a very high tempo of battle, operations over great distances and a high level of complexity of operations, in terms both of the number and variety of combatants. There are limits to the extent to which any of these can be increased, limits that may well depend on the level of network capability possessed by a force. Nevertheless, the fact that a net-

centric force may be able to reach a higher level in one or more of these capabilities is a matter of degree rather than kind; it does not help much with the task of identifying or defining network centricity in a system. There is a clear need for the identification of genuinely defining characteristics of network centricity; §§3.2.2–3.2.4 attempt this.

We reiterate that we do not argue that networks will not facilitate warfighting capabilities or enhance the emergent characteristics of NCW, but rather that the characteristics are of themselves not definitive of net centricity.

Many commonly held naval attitudes to NCW boil down to something like: 'if we have a computer network and are using it, then we are doing NCMW'. Is this reasonable? It mirrors developmental reality, but does not imply a revolution or radical change in operations. What is required for a revolution in military affairs is the development of radically effective new warfare concepts that are enabled by computer networks. The study of emergent properties is a methodology for developing these. Clearly, network centricity need not have any emergent properties, but its claim to be considered revolutionary is weakened without at least one. However, even if NCW is not revolutionary, it might still be useful. This is a question for analysis to arbitrate; and, in the end, being useful is more important than being revolutionary.

3.2.2 Network Attributes Characteristic of Net Centricity

Since the properties of §2.1 appear to be inadequate for defining network centricity, we explored instead characteristics of a wide range of existing networks. In particular, examples of the successful usage of the internet and social networks (e.g., alumni associations, 'old boys' clubs etc.) were examined to suggest and test proposed network characteristics. In this section, networks are characterised through a list of capabilities. The list, though perhaps not complete, is based primarily upon the authors' observations of the civilian and military internet as it has developed over the past twenty years, and on our personal experience with various social networks such as academic, military, scientific, religious, sporting and family networks.

- *Ad hoc geometry.* Effective networks do not in general have a regular geometrical structure, such as hierarchical, hub-and-spoke, etc. Rather, connections between nodes grow out of a myriad of local concerns, so that the pattern of linkages appears random when the network is viewed at an appropriate scale.
- *Robustness.* Because of the geometry, there are large numbers of communication paths between most pairs of network nodes. Where this is the case, bottlenecks are rare and the system is not so vulnerable to the failure of an individual node.
- *Between peers.* Each node in the internet is the equal of all other nodes. It is true that social nets often have a hierarchy, but this usually produces bottlenecks and points of failure, so reducing the efficiency of the network.
- *Common grounding or basis of relationship.* Nodes have cultural or other points of commonality that facilitate the usage of the network.
- *Dynamic communities of like minded people.* Internet users organise themselves into interest groups and sub-networks often without formal membership requirements. These groups have a dynamic membership depending upon the availability and interest of the members. Similarly, social groups form when there is a common basis of interest or issue to address, and then evolve or dissolve when the issue is no longer of importance.
- *Open access.* Appropriately authorised users can access the network through any node; they are not restricted to a single or 'home' node.
- *Portability of function.* Functions are not tied to particular nodes, but can be carried

out at any node. For example, in a net-centric system, a sonar operator would not need to be located on the platform carrying the sonar system.

- *Anonymity*. With the internet, users and providers of information need know little about one another. Often, providers of information do not know *a priori* who will access their information. Also, providers usually do not know who is advertising the location of their information.
- *Geographical independence*. Physical location of nodes is unimportant. The network imposes a new distance metric based upon communication lag times or numbers of nodes traversed in a communication. For example, by this metric DRDC-Atlantic is closer to nodes in Ottawa than university nodes in Halifax because the Canadian military network links to the civilian network through Ottawa.
- *Distributed computing*. The network allows partial computations to be conducted in parallel utilising resources at physically separated locations.
- *Collective memory*. Each node has access to data stored in a wide variety of locations, giving a robust memory. Virtual bulletin boards and lists of links provide assistance in locating particular items of data; the dispersed and *ad hoc* nature of these also enhances robustness.
- *Speed of information dispersal*. Information is spread with exponential rapidity, using the principle 'I tell three people, each of them tells three people, and so on'. On the one hand, the impact of this is attenuated by the possibility of errors accumulating with each re-transmission; on the other hand, a given piece of information may arrive from more than one source or by more than one route, giving rise to possibilities for trapping transmission errors.

A consequence of several of these capabilities is that resources might not be available on demand as required, but the likelihood of unavailability diminishes as the size of the network grows.

The totality of the network is usually beyond the capability of a single person to control or know. Thus, whether it be the 'old boys' network, sales networking or the internet, the manner of usage is not so much that of a user knowing exactly where to find something, than one of publishing a request for a resource and waiting for another user, often unknown, to fill it. Similarly, data is often offered on the net, not because it has been requested, but because it is available and may be of use to someone else.

This list of network characteristics refers not so much to the nature of the technology as to its use. The characteristics are nevertheless facilitated by the technology. The main difference between modern electronic 'internet's and social networks is the breadth of their scope and speed of their response. Past social networks can respond as fast with information or have as wide a breadth, but without an electronic network are incapable of both together.

3.2.3 Heuristic Characterisation of Network Centricity

The characteristics listed in the last section can be used to distinguish net-centric from other systems, thereby providing an implicit definition of network centricity. The essence of the characteristics in the previous section concerns how the network is used rather than the underlying technology. By implication, therefore, the key characteristic of a net-centric system is one of attitude of the users, a breaking out and broadening of focus away from individual, unit or platform concerns—the 'platform-centric' attitude—to acknowledge the wider mission and responsibilities of the team, task group or coalition. This point of view—focusing not on the properties of the network but

rather on the use to which it is put—may be a sharper way of defining network centricity and recognising it in a system.

In more detail, we advocate that a definition of network centricity should include the following aspects:

1. The nodes of the system are widely dispersed geographically, yet are able to access one another with high speed.
2. There is an element of altruism in the manner in which each node uses the network —users keep the benefit of others on the net in mind when determining their style of net usage.
3. Each user has a relationship with, or sense of responsibility to, the community of other network users as a whole. This implies a degree of commitment to the community.
4. Users have some level of trust that requests posted to the net by others are not frivolous, selfish or narrowly acquisitive.
5. Users have a reasonable level of trust that their own requests posted to the net will not be ignored.

To explore this further, if one considers 'net-centric' and 'platform-centric' as representing extremes, then there are two different types of intermediate case:

- 'Network-enabled platform-centric orientation' can be said to apply when the focus remains with the platform while use is made of the network to exchange information efficiently. The idea of a reachback centre (§3.3.3 below) is an example. Others independently make a similar distinction between network centricity and platform-enabled network centricity [78,114].
- The term 'task-group-centric orientation' refers to a situation with a high level of unity amongst units in a task group, with integrated sharing of all resources and task focus, but much less integration with entities outside of the task group. Effectively, a force with this orientation comprises several separate net-centric entities—the task groups—with only a low level of connectivity between them.

In terms of the five aspects of net centricity above, a platform-centric network might include the first, but would not include the second or third, and the levels of trust referred to in points 4 and 5 would be rather low compared with the net-centric case. That is, the difference between a network-enabled application and a net-centric system depends on the relationship between nodes. In a network-enabled application, the network is used primarily to benefit the user's unit and does not require any relationship between nodes. Thus, IP-addressable sensors, where a user can access the data from a sensor independent of the sensor's owner, is a network-enabled application. To become net-centric, there must be a relationship between the user and the owner, so that the owner is willing not only to share the resource, but further to consider the concerns of other users when deciding to change the state of the resource, even to the point of releasing some level of control to possibly unknown users. In return, the owner must gain some benefit from the user's activity, which need be no more than furtherance of a common goal or purpose.

3.2.4 Definition of Network-Centric Warfare

As concerns the definition of network centricity, the key feature emerging from the analysis of the previous section is the manner in which the user uses the network. The previous section contains the details, but it can be convenient to have these distilled into a single sentence. In the context specifically of NCW, such a sentence might read:

> Network-centric warfare is the conduct of military operations using networked information systems to generate a flexible and agile military force that acts under a common commander's intent, independent of the geographic or organisational disposition of the individual elements, and in which the focus of the warfighter is broadened away from individual, unit or platform concerns to give primacy to the mission and responsibilities of the team, task group or coalition.

Our approach to the definition of network centric warfare can be encapsulated by the addition of a fifth 'right' to the usual four (§1.1): not only will the right information be available to the right person at the right time in the right form, but also it will be put to the right use.

3.3 Discussion

3.3.1 Implications of NCW for Morale and Loyalty

The motivation for moving to network centricity in warfare lies in the benefits that it may bring. It is credible to expect that a properly set up network-centric force will be able to use resources more efficiently than is currently possible. This includes more efficient provision of logistics, access to reachback, faster and more effective decision making, and so on. The result ought to be a force multiplier; a network-centric force should be able to do more than a platform-centric force with the same resources. Beyond this however, we note that many of the social networks mentioned in §3.2.2 provide more than information and access to resources. They also provide 'moral' support. This socialisation aspect to networking could be expected to strengthen morale and contribute positively to unity of purpose, especially of a coalition force.

On the other hand, any move away from platform centricity encounters the issue of loyalty. Loyalty to a ship, regiment etc. is a powerful unifying force in the military. There are real benefits to be obtained from developing such *esprit de corps*, not the least being the promotion of unit cohesiveness—one of the most important factors motivating the warfighter under fire [115]. However, extremes of unit loyalty that are founded on or in some way promote negative attitudes to the rest of the force are detrimental to the force as a whole and particularly to the development of a net-centric orientation. Yet it may be that this is saying no more than that there is a natural limit to the size of the group in which an intense loyalty can be engendered. If so, then perhaps the greater interconnectivity provided by networking can push back this limit, so giving common intent and in-group relatedness a chance to become force-wide. If, on the other hand, this cannot be achieved, then net-centric operations may lead to high levels of stress derived from unresolved conflicts of loyalty. It is not clear where the balance lies in this complex issue; this may be another question for analysis to address.

3.3.2 Network Centricity Related to Rational Selfishness

'Rational selfishness' is a term coined by the populist philosopher Ayn Rand [e.g. 116, 117] to describe her version of a concept that dates back at least to ancient Greece. Rand applies it to a range of social dichotomies such as capitalism versus socialism and individualism versus the collectivist orientation of many eastern cultures. The relevance here lies in the correspondence of these dichotomies with that of platform centricity versus network centricity. Exploration of these parallels provides a different perspective on the nature of network centricity.

A platform-centric orientation can be regarded as selfish in focus: the interests of the platform are paramount. In this sense, it corresponds to the capitalist and individualist sides of the social dichotomies. In contrast, a network-centric orientation implies acting with the interests of the whole group primarily in mind. This is not so dissimilar from the golden rule of Judeo-Christianity or the social mores of many eastern cultures, such as in Japan, where one is supposed to moderate one's actions by continuously accommodating other people's wishes, desires and sensitivities.

Rational selfishness links these seemingly opposed ideologies; one cannot, it is claimed, obtain the best for oneself if others in the society are not also doing well. That is, the outcome desired by naive selfishness is impossible to achieve in isolation, and can in a community only be achieved when others are also in a position to achieve their own selfish outcomes. In more specific terms, any action of mine that damages the interests of others must eventually but inevitably also be harmful to me, and so is an action that I would avoid if my selfishness were rational.

The application of this notion to a military force is clear: it is rare for a platform to fight in isolation; the interests of any one platform are inextricably linked with the interests of its fellows in the task group. Hence, unthinking platform-centric actions will in fact be detrimental to the interests, viewed in the large, of the platform. With this perspective, we see that platform centricity, rightly conceived, ought to be little different in its effect from net centricity. The difference in focus is not as great as it appears.

What are we to make of this point of view? Is it just philosophical smoke and mirrors that hides all the hard bits in the words 'rightly conceived'? The history of philosophy attests to the difficulty of getting people to have right conceptions, or even to agree on what they might be, let alone to act on them. The conclusions of rational selfishness rely on trust and clarity of thought, neither of which are universal in any community. As applied to NCMW, we must take into account the reality that not every commander will be a team player, that rivalry exists and that clear-sighted prediction of the consequences of one's actions is difficult. That is, the damage that one's behaviour causes to others often is a result of misunderstanding rather than malice.

True network centricity will be achievable only with a rather higher level of trust than has been typical in joint or coalition forces. Taking the internet as a paradigm, one can envisage situations in which a platform may seek a resource without knowing in advance where it will come from. This would not be tolerated unless the platform commander were prepared to trust that access to the resource would be denied only if it truly were needed elsewhere, and not because of another's waste or hoarding. On the other side, those offering the resource must be prepared to trust that a request from a platform commander, of whom they might have no knowledge, stems from genuine need.

3.3.3 Reachback—Linking Information-Based Warfare to Network Centricity

Using the definition of net centricity in §3.2.4, it is clear that, for currently configured C^2 processes and force organisations, there may be many useful applications of networking that are not net centric, but merely network enabled. Indeed, there may be scenarios in which there is more to be gained from network-enabled processes than from something that is fully network centric.

For example, Neal [118] envisages the establishment of a 'reachback centre' to handle all requests for information. In our view, this is not a network-centric concept,

but rather is network-enabled platform-centric thinking. Neal's reachback centre is available 24 hours a day, has access to whatever resources field commanders may require and also has such a high level of situational awareness that, whenever it answers a question, it knows who else in the battlespace would benefit from the information and dispatches it accordingly. There is no doubt that, if such a reachback centre could be staffed continuously with the right mix of expertise, could avoid overload at times of high demand and could be protected from attack, either physical or electronic, then making subject matter experts available on such a basis would add a capability that would be difficult to provide individually to all potential users. The reachback application of Britten [73] is similar and provides major advantages in terms of supportability, speed of deployment and maintainability. There is little question that these are beneficial ideas, despite being 'merely' network-enabled.

However, it is much more in the spirit of net centricity to envisage reachback as working in a distributed fashion, like an internet newsgroup. When commanders need something, they post a query or request and a response comes from whomever may be willing to contribute one. Whether this is better or worse from the point of view of military effectiveness depends on practicalities. For the distributed net-centric reachback system, a major worry is that there is no guarantee of an answer or of when the answer will arrive. However, the experience of the internet suggests that, when a network becomes large enough, the likelihood of such an adverse outcome is negligible.

An example of such a newsgroup-like application might be the formation of a support group that is available to augment a commander's staff dynamically and voluntarily. To follow the newsgroup analogy, a commander facing a potential situation might post a query to the newsgroup asking for solutions. The response would depend who was monitoring the newsgroup at the time, their interests and available resources. In an associated analogy, a moderated newsgroup might be able to debate a number of solutions to a problem and provide the commander with an expanded assessment of a planned operation. Because of security concerns and to engender trust in the competence of the replies, the 'reachback group' should be more structured than an ordinary internet newsgroup. For example, membership would have to be vetted. In times of likely high demand, there may need to be a roster set up to ensure that people with the right mix of skills are logged on and monitoring the newsgroup. Membership of such a reachback group need not be limited to current serving officers. This may be a very good way of drawing on the skills and experience of recently retired staff, or even particularly highly trusted analysts.

The concept of reachback can be expanded to apply to all resources, not just information. For example, a unit could call up anti-tank fire when needed, rather than carrying anti-tank capability themselves. Taking the full net-centric viewpoint, the call for anti-tank fire should be non-directed, just like a call for information; the unit does not care where the anti-tank round comes from, so long as it is timely and well targeted. If information operations were well advanced, it might even be possible to delude an adversary unit into delivering the anti-tank round!

Following on from these ideas of net centricity, a network-enabled platform-centric force might be set up so that any platform can access data from any other platforms' sensors. A net-centric force might instead be organised across warfare areas instead of platforms, with a dynamic linking of warfare-area subject-matter experts who evaluate data from sensors that do not belong to their particular platform and which was processed on a third platform.

3.4 Metrics for Network Centricity

As the reasoning in this Section makes clear, none of the metrics given in Tables 2.1–2.9 is adequate as an indicator of level of network centricity, however much they may be useful as measures of the various characteristics of net-centric systems. This is because these characteristics are not definitive: §3.2.1 gives examples of non-net-centric systems that display each of them. The key characteristic of network centricity, in our view, is the broadening of warfighter focus that is emphasised in our definition of NCW (§3.2.4, p. 33), so that the information received via the network is put to the right use. The task of constructing a metric for network centricity then comes down to the difficult problem of capturing 'broadening of focus' quantitatively. We do not have a suggestion sufficiently mature for presentation here. However, further research on this question may be assisted by a concrete example. The following paragraphs present such an example, taken from recent modelling by TTCP MAR Action Group 1 [119].

The scenario analysed is a maritime interception operation, in which a force of N interceptors patrols a control line and seeks to intercept any vessel wishing to cross the line. TTCP MAR AG-1 applied queueing theory to this scenario. As well as the number of interceptors, the model requires as inputs:

- the mean number of incoming vessels per day
- the mean time required for an interceptor to service in incoming vessel
- the mean time for an incoming vessel to evade the interception (that is, to 'renege' in queueing-theory terms).

The overall measure of effectiveness (MOE) is the probability that an incoming vessel is intercepted. Figure 3.1 shows results as a function for arrival rate for 4 interceptors with a mean service time of 4.0 h and a mean evasion time of 1.0 h.

The three lines in Figure 3.1 show the effect of different concepts of operations (CONOPS). In the platform-centric CONOPS, the control line is divided into sectors of

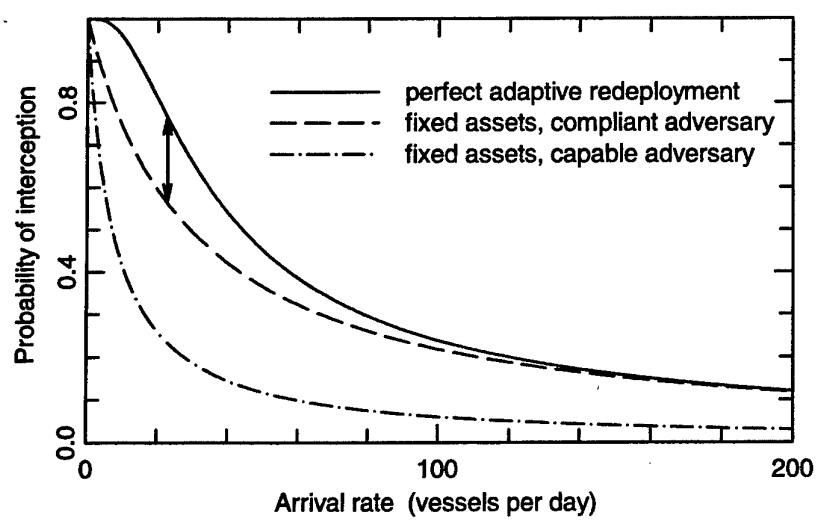

Figure 3.1: Queueing-theory calculation of the probability of intercepting incoming vessels in a maritime interception operation as a function of arrival rate (after Fig. 5 of Ref. 119). The interception force comprises 4 interceptors each taking on average 4.0 h to deal with an intercepted vessel. Incoming vessels can evade the interception in an average of 1.0 h if not intercepted within that time. The lines show results for three different concepts of operations, as discussed in the text. The double arrow shows the gain in effectiveness attributed to 'broadening of focus'.

responsibility, one for each intercepting asset. This CONOPS can be reasonably described as 'platform-centric' because each interceptor remains fixed its own sector of responsibility and concerns itself only with vessels entering its sector. The outcome depends on adversary tactics. If the incoming vessels obligingly spread out across the control line, so that each interceptor experiences the same arrival rate, then the result is the middle curve in Figure 3.1 (that is, the broken curve). However, incoming vessels intent on smuggling are more likely to bunch up and attempt to rush one sector. The extreme case, where all incoming vessels pass through a single sector, gives the bottom curve in Figure 3.1, the chain curve. The MOE corresponding to any given situation lies between these two extremes.

The full curve in Figure 3.1 shows the results for a different CONOPS, in which interceptors are positioned adaptively to match the pattern of incoming vessels. If this is achieved perfectly then, as soon as an interceptor completes an interception, it can begin the interception of another incoming vessel, if there is one not yet dealt with. The minimum gain in MOE available from this CONOPS is shown by the area between the full and broken curves in Figure 3.1, as indicated by the double arrow. To achieve this additional effectiveness, platform commanders must, when their platforms are idle, be willing to look beyond their sectors and go to the aid of an overloaded interceptor, even though this risks allowing a smuggler to slip through their own sector of responsibility. This is what is meant by 'broadening of focus'—each platform commander acts for the benefit of the whole force rather than concentrating on maximising the contribution of his or her platform to the MOE. Achievement of the broadening of focus can be significantly affected by the command style the Force Commander; some command styles will promote a broadening of focus, others will inhibit it.

⋀⋀⋀

The above results on maritime interception are presented in some detail because they provide a clear example of a gain in effectiveness obtained by the broadening of focus that is a central element in our conceptualisation of network centricity. This example has a natural metric: the fraction of incoming vessels that are intercepted. However, that metric is clearly scenario-dependent. Whether it is possible to abstract these concepts to produce a general scenario-independent metric for network centricity remains to be determined.

3.5 Summary

The process of replacing one set of characteristics of network centricity with another indicates that the most important feature of network centricity is the use to which the network is put, rather than the physical or technological characteristics of the network, as important as they might be. It is clearly possible for a high-capability network to be used in a platform-centric manner, behaviour that we have termed 'network-enabled platform-centric'. The reachback centre is a specific example of a platform-centric concept that requires a high-capability network for its implementation.

The question of metrics for network centricity then comes down to a metric that can quantify 'right use' of the network and the information that it delivers. Section 3.4 describes a scenario in which a gain in effectiveness is available through the adoption of a net-centric orientation, but it is not clear how to generalise this metric to make it scenario-independent.

The conclusions of this section must be tempered with the practical consideration of the size of the network available. Full internet-like capabilities will be achieved only when the number and variety of nodes in the network exceed certain critical values [55], the magnitudes of which are at present uncertain; this is yet another question that analysis might address.

4. Conclusions

This study began with an evaluative collation of properties of network-centric systems, as expounded in the literature on network-centric warfare. In view of the multitude of options facing military planners seeking to move their forces toward network centricity, it is important to have clear concepts of the nature of network centricity and how to recognise it. Elucidation of these are a main aim of this paper, together with the formulation of some metrics. The initial motivation was to inform a TTCP MAR-Group study of network-centric maritime warfare. Consequently, the emphasis falls naturally on the high-level characteristics of NCW.

Concerning the identification of network centricity, examination of the high-level properties of NCW shows that none is clearly diagnostic; that is, one can conceive of systems displaying them despite not being net-centric as we understand the term. This led to the compiling of another list of properties, derived from characteristics of the internet and other effective networks. This list is, we believe, better suited to the identification of network centricity and points to a key element in its nature, namely the manner in which the system is used. In our view, access to a high-capability network is not sufficient for a system to be network-centric. It is also necessary that the network be used in a manner that supports the force as a whole, rather than its use being focused on the needs of a particular unit or platform. This leads to the following definition of NCW:

> Network-centric warfare is the conduct of military operations using networked information systems to generate a flexible and agile military force that acts under a common commander's intent, independent of the geographic or organisational disposition of the individual elements, and in which the focus of the warfighter is broadened away from individual, unit or platform concerns to give primacy to the mission and responsibilities of the team, task group or coalition.

The emphasis on motivation—a human dimension—in the definition of network centricity parallels, though is distinct from, recent work emphasising human aspects in command and control [91–95]. As with command, network centricity is not just about hardware. The connection between network centricity and C^2 is not coincidental, for a significant function of a net-centric system is to support command and control; most of the characteristics of network-centricity discussed in §§2.1 and 3.1.1 concern aspects of C^2. Thus it is to be expected that the human dimension of C^2—'only humans command' [92]—should be reflected in the concept of network centricity.

We distinguish two intermediate states between the extremes of platform centricity and network centricity: network-enabled platform centricity and task-group centricity. The first refers to a situation in which the orientation is fundamentally platform centric, but networking is used to enhance capability. The second lies closer to true network centricity; the force is subdivided into task groups that are internally net-centric

but externally not. This is a possible structure for a coalition force, where the task groups comprise the platforms of each participating nation.

The recognition that the emergent properties of NCW are not diagnostic has a corollary: that metrics for these properties are inadequate as measures of degree of network centricity. That is, level of self-synchronisation, to take one example, cannot be reliably used as a metric for level of network centricity because one can conceive of circumstances in which a non-netted force shows a high degree of self-synchronisation (§3.2.1). The question of how to construct a general scenario-independent metric for degree of network centricity remains open.

Finally, we conclude by quoting an early comment that, although written well before the development of NCW as a concept, nevertheless clearly refers to the central military problem that NCW seeks to address [39(p. 269)]:

> 'Confronted with a task and having less information available than is needed to perform the task, an organisation may react in either of two ways. One is to increase the information-processing capacity,† the other is to design the organisation, and indeed the task itself, in such a way as to enable it to operate on the basis of less information. These approaches are exhaustive; no others are conceivable.'

To adopt NCW is to choose the first of these alternatives. The rationale for so choosing lies in the recognition that warfare is dominated by uncertainty and in the belief that more information means less uncertainty. However, it has been suggested that the uncertainty of war has its roots not so much in an inadequate information-processing capability as in the difficulty of predicting what the enemy will do [29,120], and no sensors are yet capable of reading the enemy's mind [38,41]. Hence, it is obliquely claimed that the impetus for NCW is misguided. There may well be scenarios for which this is the case. On the other hand, the general need for more high-quality information on the battlefield is undeniable. With sufficient information, it may be possible to identify all the possible courses of action open to the adversary so that, although this does not identify the enemy's actual plan, one's own planning can cover all contingencies. (This concept must, however, be applied with skill and flair. As the maxim has it: an enemy that has two possible courses of action open to it will always choose a third.) In short, one would be wary of facing a net-centric adversary without NCW capability of one's own.

† This should be read to include the capacity to generate the additional information required, as well as to process it.

Appendix A: On the Names of Metrics

One of the aims of this work is to develop examples of metrics for net-centric-system properties, since the ability to define such metrics is an indicator of real understanding of the system under study. Metrics are often arranged into a hierarchy that mirrors the hierarchy of properties, and names are assigned to groupings at various levels. However, there is no uniformity in the usage of the names. For example, a task force of the U.S. Military Operations Research Society proposed four levels of metrics; in order from lowest to highest these are termed 'dimensional parameters', 'measures of performance' (MOP), 'measures of effectiveness' (MOE) and 'measure of force effectiveness'. This terminology also appears in a NATO publication [121(p.10)]. Another hierarchy, also with four levels, that is gaining currency in Australia, uses the terms MOP, MOE, 'measure of outcome' and 'measure of capability', again from lowest to highest. That is, 'MOE' is the second lowest level of metric here, whereas the MORS/NATO scheme uses the same term for the next one up, the second highest.

In the present work, we are more concerned with the hierarchy of properties than with the names of metrics. However, it is routine to describe the most important goal of network centricity as 'improving military effectiveness', so we have adopted 'MOE' as the term for the metric that measures this. All other metrics refer to the performance of a subsystem of the system in question, so we term these 'MOPs'. On the rare occasion that it is expedient to refer to a level between these two, we use the term 'measure of system performance'.

(We believe that the use of 'MOE' to denote the highest-level metric has historical precedent, although a reference in support of this has not come to hand. For example, Morse and Kimball's famous book [122] contains a chapter entitled 'The use of measures of effectiveness', but they use the term generically to mean any metric. Koopman [123] uses 'MOE' in a similar manner. It seems that the concept of a hierarchy of metrics did not exist when these books were written. A third famous book from the early days of operational research, Quade's compilation [124], does not mention 'MOE' at all, and uses the term 'criterion' in place of 'metric'.)

A well structured piece of operational research must include an MOE, to ensure that that military effectiveness is the overriding consideration. Because of the difficulty of aggregation, arising from the unavoidable arbitrariness of weighting factors, there should be just one MOE [124(p.160)]. If it really is impossible to express the aims of the study in a single MOE, then it is preferable to run the analysis several times, once for each MOE, rather than attempt an aggregation.

Appendix B: Descriptions of Degrees of Network Centricity

One of the following may provide a suitable scheme for parameterising the level of network centricity as a discrete-valued variable.

B.1 Levels of Information Systems Interoperability (LISI) [125]

Level 0—Isolated Interoperability in a Manual Environment

- Isolated (stand-alone) systems.
- Data transfer by re-keying or extractable, common media (e.g. floppy disk).
- Fusion of information, if any, done off-line by individual decision-maker.

Level 1—Connected Interoperability in a Peer-to-Peer Environment

- Systems capable of electronic linking.
- Limited data-transfer capability—text e-mail, common graphic-file formats (.tif, etc.)
- Little capability for decision-makers to collectively fuse information.

Level 2—Functional Interoperability in a Distributed Environment

- Systems reside on local networks.
- Formal data models exist; only the logical data model is common; each program may define its own physical data model.
- Capability to transfer fused data in simple formats (e.g. graphics annotated with a text overlay).

Level 3—Domain-Based Interoperability in an Integrated Environment

- Systems connected by wide-area networks.
- Data models, both logical and physical, are implemented across functional areas that comprise a domain, allowing database-to-database interactions.
- Individual applications may access central or distributed data repositories.
- Group collaboration on data fusion.

Level 4—Enterprise-Based Interoperability in a Universal Environment

- Distributed global information space across multiple domains.
- Data and applications fully shared.
- Advanced forms of collaboration (e.g. the virtual office).

B.2 Network-Centric Operations Maturity Model [3(§8.1.3.1)]

Maturity Value 0—Platform-Centric Operations

- Organic sources of situational awareness.
- Traditional C^2.

Maturity Value 1

- Sharing of information between platforms for improved situational awareness.
- Traditional C^2.

Maturity Value 2

- Sharing of information between platforms for improved situational awareness.
- C^2 doctrine includes some level of collaborative planning.

Maturity Value 3

- Richer sharing of information between platforms to obtain an approach to true shared situational awareness.
- C^2 doctrine includes some level of collaborative planning.

Maturity Value 4

- Richer sharing of information between platforms to obtain an approach to true shared situational awareness.
- Existence of '...a Mission-Capability Package that allows integration across doctrine, organisation, training, material, and other aspects of the force and its supporting systems that permit self-synchronisation' [3].

B.3 DSTO-Communications-Division Capability Options [126]

- *Level 1—Do Nothing*: Essentially current capability (~2004 timeframe).
- *Level 2—Quick Fix*: More stovepipes—multi-channel secure voice, digital COMSEC, inter-ship LANs, multi-media archives.
- *Level 3—CIS Integration*: Fully automated COMCEN, electronic key management, multi-band radios and modems.
- *Level 4—Survivable CIS Integration*: Level 3 plus more communications bandwidth and robustness to jamming.
- *Level 5—Enhanced Battlespace Awareness*: Level 4 plus wideband sensor communications network and automated distributed picture compilation capability.
- *Level 6—Intelligence-Based Warfare*: Level 5 plus direct sensor-to-shooter communications with multi-static sensing, and integrated communications with capability for information operations.
- *Level 7—Full Network-Centric Warfare*: Level 6 plus whatever is necessary to enable cooperative engagements.

B.4 From a Study of C^2 and IO

Stevens *et al.* [127], in a study of ways of representing C^2 and IO in military simulations, used modelling options listed in the following Tables.

Table B1: Options relating to communications systems [127].

ID	Title	Description
C1	Assured communications with stochastic delays	No restrictions on availability of communications links, other than a random delay with a specified distribution.
C2	Unassured communications with simple constraints	As for C1, with simple additional restrictions, such as line-of-sight, frequency compatibility etc.
C3	Protocol-level communications	Protocols associated with specific communications systems are modelled.
C4	Physics-level communications	Propagation physics is explicitly modelled.

Table B2: Options relating to sensor systems [127].

ID	Title	Description
S1	Simple parametric sensors	Sensors are characterised by a small set of generic parameters.
S2	Detailed parametric sensors	As for S1, with a more detailed suite of parameters.
S3	Physics-based sensors	Sensor physics is explicitly modelled.

Table B3: Options relating to data fusion [127].

ID	Title	Description
F1	Ground-truth fusion	CTP (own, adversary or both) contain ground-truth data; sensors not modelled with this option.
F2	Perfect-correlation dead-reckoning fusion	Contacts from different sensors correlate perfectly ; dead reckoning is used to obtain position estimates.
F3	Imperfect-correlation dead-reckoning fusion	As for F2, but attribute matching and a simple measure of correlation is used for contact correlation.
F4	Imperfect-correlation, Kalman-filter fusion	Correlation as in F3, with a Kalman filter used for position estimation.

Appendix C: On Information

C.1 The Importance of Information to Warfare

The importance of information to success in war has been understood from ancient times. For example, Sun Tzu (*c.* 400's–200's BC) wrote, *inter alia*:

> 'A military operation involves deception. Even though you are competent, appear to be incompetent. Though effective, appear to be ineffective. When you are going to attack nearby, make it look as if you are going to go a long way; when you are going to attack far away, make it look as if you are going just a short distance.' [113(book 1)]
>
> '...the consummation of forming an army is to arrive at formlessness. When you have no form, undercover espionage cannot find out anything, intelligence cannot form a strategy.' [113(book 6)]
>
> '...those who do not know the plans of competitors cannot prepare alliances. Those who do not know the lay of the land cannot maneuvre their forces. Those who do not use local guides cannot take advantage of the ground.' [113(book 11)]
>
> 'A major military operation is a severe drain on the nation, and may be kept up for years in the struggle for one day's victory. So to fail to know the conditions of opponents...is extremely inhumane, uncharacteristic of a true military leader, uncharacteristic of an assistant of the government, uncharacteristic of a victorious chief. So, what enables an intelligent government and a wise military leadership to overcome others and achieve extraordinary accomplishments is foreknowledge.
>
> 'Foreknowledge cannot be gotten from ghosts and spirits, cannot be had by analogy, *cannot be found out by calculation*. It must be obtained from people, people who know the conditions of the enemy.' [113(book 13)] (emphasis added)

C.2 Modelling Information

The NATO 'Code of Best Practice' [121(¶49)] stipulates the following requirements for modelling information in a well designed C^2 model:

- Information should be represented as a commodity with definite attributes.
- Information should flow realistically around a battlespace.
- The collection of information involves multiple sources—information-collecting assets should be explicitly tasked.
- The processing of information (filtering, correlation, fusion etc.) should be explicitly represented.
- C^2 systems (including the network) should be explicitly represented as battlefield entities, subject to targeting, degradation etc.
- The perceptions of a military unit must be built, updated and validated *only* with the information available to the unit at the time.

- A commander's decision making must be based *only* on his or her perception of the battlespace at the time.
- Information operations—deliberate attack on and defence of information and information systems—should be represented.

These points should be addressed from both own and the adversary perspectives.

C.3 Information Operations

The network property security and the information properties secrecy and authenticity refer to the domain of information operations. They are relevant only if it is decided to include IO in the model. IO are very important; in the words of the 2000 Information Superiority Workshop conducted by the Joint Experimentation Directorate, US Joint Forces Command [75(p.11):

> 'Actions that a future enemy might take to contest friendly battlespace management were discussed. The consensus was that RED would have the greatest impact if it could cause BLUE's command and control and targeting functions to question the accuracy and validity of its information. Injection of an element of doubt would increase BLUE's decision cycle, and result in a slower tempo of BLUE operations.'

(What is meant by 'validity' here? Perhaps this is equivalent to 'authenticity', as defined in §2.3.)

Some other quotations on information operations:

> 'Information Operations are essential to achieving full spectrum dominance. The Joint force must be capable of conducting information operations, the purpose of which is to facilitate and protect US decision-making processes, and in a conflict, degrade those of an adversary.' [3(pp.2-14–15)]

> 'Information Age warfare will place a premium on information operations. Both sides will seek to employ a range of tools to ensure achieving and maintaining an information advantage. ... Information operations...include exploitation of the information systems of the adversary or items taken from it.' [16(p.109)]

> 'Information Operations is at the same relative stage in its growth and utility that special operations forces were 10–15 years ago; i.e., the joint forces are just beginning to understand the proper application and potential contribution of IO capabilities. When using IO, the distinction between strategic, operational, and tactical levels will become increasingly blurred.' [75(p.11)]

> 'These changes have resulted in the increasing importance of information. And as our dependency for information and connectivity grows, our control over our infostructure diminishes and our vulnerabilities increase.' [128(p.28-3)]

Acknowledgement

The authors thank Drs A.J. Knight and C.L. Davis for their numerous helpful discussions and comments on drafts of this paper.

References

[1] Anon. (2000) *Network-centric naval forces—a transition strategy for enhancing operational characteristics*, Report of the US Naval Studies Board.

[2] W. Perry, R.W. Button, J. Bracken, T. Sullivan & J. Mitchell (2002) *Measures of effectiveness for the information-age navy: the effects of network-centric operations on combat outcomes*, Report MR-1449-NAVY of the RAND Corporation.

[3] Anon. (2001) *Network Centric Warfare*, Report by the US Department of Defense to Congress, 27 July 2001.

[4] D.S. Alberts (2002) *Information age transformation; getting to a 21st century military*, rev. edn, Washington DC: CCRP Publications.

[5] D.S. Alberts and R.E. Hayes (eds) (2002) *Code of best practice doe experimentation*, Washington DC: CCRP Publications.

[6] S. Fewell, A. Arnold, J. Asenstorfer, J. Bell, B. Blair, J. Clothier, R. Gani, D. Harabor, J. Hayward *et al.* (2003) *Network centric warfare—a compendium of approaches, views and resources 2003*, in preparation as a general document of the Defence Science and Technology Organisation.

[7] A.K. Cebrowski & D.K. Watman (2001) 'War and wargaming in the information age', *World Def. Syst.* **3**(2), 71–6.

[8] P. Nagy (2001) 'Network-centric warfare isn't new', *Proc. US Nav. Inst.* **127**(9), 44–6.

[9] W.J. Holland Jr. (2001) 'Network centric warfare in ASW', *Nav. Forces* **22**(5), 8–12.

[10] G.A. Klein, C.E. Zsambok & M.L. Thordsen (1993) 'Team decision training: Five myths and a model' *Mil. Rev.* **73**(4), 36–42.

[11] D.J. Bryant, R.D.G. Webb, M.L. Matthews & P. Hausdorf (2001) *Common Intent: A Review of the Literature*, Contractor report CR-2001-041 of the Defence and Civil Institute of Environmental Medicine, Toronto Canada.

[12] J.J. Gartska (2000) 'Network centric wafare: an overview of emerging theory', *Phalanx Online* **33**(4).

[13] J. Stavridis (1997) 'The second revolution' *Joint Force Q.* **15**, 8–13.

[14] A.K. Cebrowski & J.J. Gartska (1998) 'Network-centric warfare, its origin and future' *Proc. U.S. Nav. Inst.* **124**(1) 28–35.

[15] T.K. Adams (2000) 'The real military revolution', *Parameters* **30**(3) 54–65.

[16] D.S. Alberts, J.J. Gartska, R.E. Hayes & D.A. Signori (2001) *Understanding Information Age Warfare*, Washington DC: CCRP Publications.

[17] T.G. Mahnken (1995) 'War in the information age' *Joint Force Q.* **10**, 39–43.

[18] R.M. Nutwell (1998) 'IT-21 provides big "reachbacks"', *Proc. U.S. Nav. Inst.* **124**(1) 36–8.

[19] J.R. Fitzgerald, R.J. Christian & R.C. Manke (1998) 'Network-centric antisubmarine warfare', *Proc. U.S. Nav. Inst.* **124**(9) 92–5.

[20] M.L. Boller & L.A. Levine (1998) 'The C^2 spine', *Mil. Rev.* **78**(3) 34–9.

[21] L. Cabral (1999) 'Submarine combat control information management assistants', *Proc. 6th Annual Specialists' Meeting of MAR TP-1*, Annex N, Maritime Systems Group of The Technical Cooperation Progremme.

[22] D.A. Harris (2000) 'An examination of the relationship between information and technical advances, and the revolution in military affairs', *Aust. Def. Force J.* **140**, 5–8.

[23] S. Metz (2000) 'The next twist of the RMA', *Parameters* **30**(3) 40–53.

[24] J.B. Scholz (2000) 'Network-enabled force synchronisation', *Aust. Def. Force J.* **144**, 70–6.

[25] M. Goodyer (2000) 'Some aspects of the revolution in military affairs and the impact on the ADF', *Aust. Def. Force J.* **145**, 15–21.

[26] E.A. Smith Jr. (2001) 'Network-centric warfare: what's the point?', *Nav. War Coll. Rev.* **54**(1) 59–75.

[27] J.D. Zimmerman (2002) 'Net-centric is about choices' *Proc. U.S. Nav. Inst.* **128**(1) 38–41.

[28] W.A. Woodcock (2003) 'The joint forces air command problem: is network-centric warfare the answer?' *Nav. War Coll. Rev.* **51**(1) 124–38.

[29] M. Vego (2003) 'Net-centric is not decisive' *Proc. U.S. Nav. Inst.* **129**(1) 52–7.

[30] J.L. Peterson (1997) 'Info war, the next generation' *Proc. U.S. Nav. Inst.* **123**(1) 60–2.

[31] C.J. Dunlap Jr. (1997) '21-st century land warfare: four dangerous myths' *Parameters* **27**(3) 27–37.

[32] T.P.M. Barnett (1999) 'The seven deadly sins of network-centric warfare' *Proc. U.S. Nav. Inst.* **125**(1) 36–9.

[33] W.K. Lescher (1999) 'Network-centric: is it worth the risk?' *Proc. U.S. Nav. Inst.* **125**(7) 58–63.

[34] G. Casten (2000) 'Building a beehive: observations on the transition to network-centric operations' *Nav. War Coll. Rev.* **53**(4) 124–37.

[35] T.G. Mahnken (2001) 'Transforming the US armed forces: rhetoric or reality?' *Nav. War Coll. Rev.* **54**(3) 85–99.

[36] W.J. Toti (2000) 'Stop the revolution; I want to get off' *Proc. U.S. Nav. Inst.* **126**(7) 30–3.

[37] T. Benbow (2001) 'The revolution in military affairs: an introductory survey', *J. Def. Sci.* **6**, 76–8.

[38] J.A. Gentry (2002) 'Doomed to fail: America's blind faith in military technology' *Parameters* **32**(4) 88–103.

[39] M. Van Crevald (1985) *Command in war*, Cambridge MA: Harvard Univ. Press.

[40] T.X. Hammes (1998) 'War isn't a rational business' *Proc. U.S. Nav. Inst.* **124**(7) 22–5.

[41] D.A. Jenik (2000) 'Beyond the rose-colored glasses', *Proc. U.S. Nav. Inst.* **126**(2) 60–3.

[42] B. Brehmer (2000) 'Dynamic decision making in command and control' in C. McCann & R. Pigeau (eds) *The human in command: exploring the modern military experience*, NY, Kluwer Academic, pp. 233–48.

[43] R.E. Griffin and D.J. Reid (2003) 'A woven web of guesses, canto one: network centric warfare and the myth of the new economy', 8th Internat. Command and Control Research and Technology Symp., Washington DC.

[44] R.E. Griffin and D.J. Reid (2003) 'A woven web of guesses, canto two: network centric warfare and the myth of inductivism', 8th Internat. Command and Control Research and Technology Symp., Washington DC.

[45] R.E. Griffin and D.J. Reid (2003) 'A woven web of guesses, canto three: network centric warfare and the virtuous revolution', 8th Internat. Command and Control Research and Technology Symp., Washington DC.

[46] P.M. Morse & G.E. Kimball (1951) *Methods of Operations Research*, rev. edn, NY: Wiley & Son.

[47] M.P. Fewell & M.G. Hazen (2002) 'Cognitive issues in modelling network-centric command and control', Research report of the Defence Science and Technology Organisation (in preparation).

[48] D.S. Alberts, J.J. Gartska and F.P. Stein (1999) *Network centric warfare: developing and leveraging information superiority*, Washington DC: CCRP Publications.

[49] T. Moon, E. Kruzins & G. Calbert (2002) 'Analysing the OODA cycle', *Phalanx* **35**(2) 9–35.

[50] Anon. (2001) *Network Centric W arfare, Appendix*, Report by the US Department of Defense to Congress, 27 July 2001.

[51] R.B. Polk (2000) 'A critique of the Boyd theory—is it relevant to the Army?', *Def. Anal.* **16**, 257–76.

[52] J. Moffat (1999) 'The analysis of command and control' in *Modelling and analysis of command and control*, (Proc. Symp. of the RTO Studies, Analysis and Simulation Panel, Issy les Moulineaux, January 1999) NATO report RTO-MP-38 AC/323(SAS)TP/12, paper 1.

[53] P. Essens (2002) 'Human factors issues for future command' in *Human factors in the 21st century*, (Proc. Specialists meeting of the RTO Human Factors and Medicine Panel, Paris, June 2001) NATO report RTO-MP-077 AC/323(HFM-062)TP/38, paper 11.

[54] G. Wheatley & D.F. Noble (1999) 'A command and control operational architecture for future warfighters' in *Modelling and analysis of command and control*, (Proc. Symp. of the RTO Studies, Analysis and Simulation Panel, Issy les Moulineaux, January 1999) NATO report RTO-MP-38 AC/323(SAS)TP/12, paper 17.

[55] J.R. Cares, R.J. Christian & R.C. Manke (2002) *Fundamentals of distributed, networked military forces and the engineering of distributed systems*, Technical report NUWC-NPT TR 11366 of the U.S. Naval Undersea Warfare Center Division Newport.

[56] R. Darilek, W. Perry, J. Bracken, J. Gordon & B. Nichiporuk (2001) *Measures of effectiveness for the information-age army*, Report MR-1155-A of the RAND Corporation.

[57] W.L. Perry (2000) 'Knowledge and combat outcomes', *Mil. Op. Res.* **5**, 29–39.

[58] S.J.A. Edwards (2001) *Swarming on the battlefield: past, present and future*, Report MR-1100-OSD of the RAND Corporation.

[59] J. Arquilla & D. Ronfeldt (2000) *Swarming and the future of conflict*, Report BD-311-OSD of the RAND Corporation.

[60] R.C. Rubel (2001) 'War-gaming network-centric warfare', *Nav. War Coll. Rev.* **54**(2) 61–74.

[61] G. Kasten (2000) 'Building a beehive—Observations on the transition to network-centric operations', *Nav. War Coll. Rev.* **53**(4) 124–37.

[62] D. Inbody, C. Chartier, D. DiPippa & B. McDonald (eds) (2003) *Conf. Proc.—Swarming: Network Enabled C4ISR*, Joint C4ISR Decision Support Center, <www.dodccrp.org/Publications/pdf/Swarming_Conf_Pro.pdf>

[63] J.R. FitzSimonds (1999) 'The cultural challenge of information technology', *Nav. War Coll. Rev.* **51**(3) 59–75.

[64] J.A. Harley (1997) 'Information, technology and the center of gravity', *Nav. War Coll. Rev.* **50**(1) 66–87.

[65] P. Johnston (2000) 'Doctrine is not enough: the effect of doctrine on the behavior of armies', *Parameters* **30**(3) 30–9.

[66] Anon. (1996) *Multinational maritime operations*, Report of the US Naval Doctrine Command dated September 1996 (available at <www.ndc.navy.mil>).

[67] Anon. (1999) *Measuring the effects of network-centric warfare*, Report by Booz-Allen and Hamilton Inc. to the Office of the US Secretary of Defense.

[68] R.E. Hayes (2001) 'C4ISR framework of the future', *Phalanx Online* **34** (1).

[69] A.L. Money (2001) *Report on network centric warfare—Sense of the report*, US Department of Defense report to Congress.

[70] C.H. Builder, S.C. Bankes & R. Nordin (1999) *Command concepts: a theory derived from the practice of command and control*, Report MR-775-OSD of the Rand Corporation.

[71] Anon. (2002) *Force 2020*, Vision statement of the Australian Defence Force.

[72] P.H. Marland (2001) 'UK above water command and control modelling—network centric warfare (NCW) analysis', paper presented to the October 2001 meeting of the MAR AG-1 of The Technical Cooperation Programme.

[73] S.M. Britten (1997) *Reachback operations for air campaign planning and execution*, Report AU/AWC/RWP018/97-04 of the Air University of the US Air War College.

[74] J.M. Neal (2000) 'A look at reachback', *Mil. Rev.* **80**(5) 39–43.

[75] Anon. (2000) *Final After Action Report of the Information Superiority Workshop (Feb. 22–4, 2000)*, US Joint Forces Command, Joint Experimentation Directorate.

[76] R. Peters (1998) 'The new strategic trinity' *Parameters* **28**(4) 73–9.

[77] T.L. Thomas (2000) 'Kosovo and the current myth of information superiority' *Parameters* **30**(1) 13–29.

[78] T. Kaye & G. Caldorisi (2002) 'Achieving information superiority in coalition operations: seven imperatives for success', 7th Internat. Command and Control Research and Technology Symp., Québec City, paper 146 (available at <www.dodccrp.org>).

[79] J.H. Eriksen (ed.) (2001) *NATO glossary of terms and definitions*, Document AAP-6(2002) of the North Atlantic Treaty Organization, <www.rta.nato.int/Glos/Index_En.htm>.

[80] R.W. Riscassi (1993) 'Principles for coalition warfare' *Joint Force Q.* **1**, 58–71.

[81] R.J. Hillier (2002), Keynote address to 7th Internat. Command and Control Research and Technology Symp., Québec City (available at <www.dodccrp.org>).

[82] R.H. Scales Jr (1998) 'Trust, not technology, sustains coalitions' *Parameters* **28**(4) 4–10.

[83] M. Hura, G. McLeod, E. Larson, J. Schneider, D. Gonzales, D. Norton, J. Jacobs, K. O'Connell, W. Little, R. Mesic & L. Jamison (2000) *Interoperability: a continuing challenge in coalition air operations*, Report MR-1235-AF of the RAND Corporation.

[84] P.T. Mitchell (2003) 'Small navies and network-centric warfare', *Nav. War Coll. Rev.* **51**(2) 83–99.

[85] A.J. Rice (1997) 'Command and control: the essence of coalition warfare', *Parameters* **27**(1) 152–67.

[86] W.A. Owens (1996) 'The emerging U.S. system-of-systems', paper 63, Strategic Forum of the Institute for National Strategic Studies, [US] National Defense University, available at <www.ndu.edu/inss/strforum/forum63.html>.

[87] A. Behm (2002) 'Strategic setting' and G.C. Fant (2002) 'Swedish armed forces—towards the future', presentations at *Saab technologies seminar*, September 2002, Canberra Australia.

[88] D. Matthews, M. Burke & P. Collier (2000) 'Core concepts of joint systems', Proc. Conf. on Systems Engineering and Test and Evaluation in the Changing Enviromnent of the 21st Century, Brisbane, paper 12, available at <www.seecforum.unisa.edu.au/Sete2000/SETE 2000.htm>).

[89] R. Staker (2002) *Towards a theory of systems of systems*, internal colloquium of the Defence Systems Analysis Division, Defence Science and Technology Organisation.

[90] M.W. Maier (n.d.) 'Architecting principles for systems-of-systems', White paper of The Information Architects Cooperative, available at <www.infoed.com/Open/PAPERS/systems.htm>.

[91] R. Pigeau & C. McCann (1995) *Putting 'command' back into command and control*, Paper presented at the *Command and Control Conference*, Canadian Defence Preparedness Association, Ottawa Ontario.

[92] R. Pigeau & C. McCann (2000) 'Redefining command and control' in C. McCann & R. Pigeau (eds) *The human in command: exploring the modern military experience*, NY, Kluwer Academic, pp. 163–84.

[93] R. Pigeau & C. McCann (2002) 'Reconceptualizing command and control', *Can. Mil. J.* **3**(1), 53–64.

[94] R. Pigeau & C. McCann (2002) 'A conceptual framework for command and control', *HUM-AG-18 final report*, Annex D, report of the Human Resources and Performance Group of The Technical Cooperation Programme.

[95] C. McCann, R. Pigeau & A. English (2003) *Analysing command challenges using the command and control framework: pilot study results*, Technical report TR 2003-034 of Defence R&D Canada—Toronto.

[96] N.F. Ashworth (1987) 'Command and control', *Def. Force J.* **63**, 34–6.

[97] N. Sproles (2001) 'The C^2 triad, or making the muddy waters clear', *Aust. Def. Force J.* **151**, 15–22.

[98] N. Sproles (2002) 'Dissecting command and control with Occam's razor or Ask not what "command" and "control" means to you but what you mean by "command and control"' *Aust. Def. Force J.* **155**, 19–26.

[99] B.D. Adams & R.D.G. Webb (2002) 'Trust in small military teams', 7th Internat. Command and Control Research and Technology Symposium, Québec City, paper 6, available at <www.dodccrp.org>.

[100] A.L.W. Vogelaar & E.-H. Kramer (2000) 'Mission command in ambiguous situations' in C. McCann & R. Pigeau (eds) *The human in command: exploring the modern military experience*, NY: Kluwer Academic, pp. 217–31.

[101] J.P. Kahan, D.R. Worley & C. Stasz (1989) *Understanding Commanders' Information Needs*, Report R-3761 of the RAND Corporation.

[102] M.R. Endsley (1995) 'Toward a theory of situational awareness in dynamic systems', *Hum. Fact.* **37**, 32–64.

[103] G.L. Kaempf, G. Klein, M.L. Thorsden & S. Wolf (1996) 'Decision making in complex naval command-and-control environments', *Hum. Fact.* **38**, 220–31.

[104] R.S. Seymour, V. Demczuk, A. Filippidis, H.T. French, A.-M. Grisogono, W. Johnson, D. Reid, D. Sands & Y. Yue (2001) 'Measuring the benefits of networked C^4ISR systems—a framework for experimental system development and analysis', *Proc. Land Warfare Conf. 2001*, Sydney, November 2001.

[105] J.N. Agar (2000) 'Is there a military utility to information operations?', *Def. Anal.* **16**, 277–98.

[106] A.-M. Grisogono (2003) *The knowledge analysis framework—metrics for the information age*, 8th Internat. Command and Control Research and Technology Symp., <63.249.165.71/8th_ICCRTS/Pres/plenary/2_0830grisogono.pdf>.

[107] Y. Yue, R.S. Seymour, A.-M. Grisogono, M. Bonner & H.T. French (2003) 'An example of deriving command and control metrics based on a knowledge analysis framework', *Proc. SPIE* **5102** (in press).

[108] M. Burke (2000) *Thought systems and network centric warfare*, Research report DSTO-RR-0177 of the Defence Science and Technology Organisation.

[109] R.G. Body (2000) 'Understanding the value of information—an OR approach', *Proc. Defence Operations Analysis Symposium 2000*, session 3, paper 1, General document DSTO-GD-0239 of the Defence Science and Technology Organisation.

[110] C.C. Davis, R.F. Decro & J.A. Jackson (2000) 'A value focused model for a C^4 network', *J. Multicrit. Dec. Anal.* **9**, 138–62.

[111] E. Gibbon (1788) *The history of the decline and fall of the Roman empire*, vol. 8 (chapter 64), edition published in 1990 by The Folio Society, London.

[112] J.M.K. Spurling (1983) 'Logistic systems, military' in P.W. Goetz (ed. in chief) Encyclopædia Brittanica, 15th edn, Macropædia, vol. 11, p. 78.

[113] Sun Tzu (~300s BC) *The art of war* (trans. T. Cleary, 1988) Boston: Shambala Publications.

[114] M. Banham (2002) *Defining the ADF's approach to network-enabled operations* (draft).

[115] R.J. Rielly (2000) 'Confronting the tiger: small unit cohesion in battle', *Mil. Rev.* **80**(6) 61–5.

[116] A. Rand, N. Branden, A. Greenspan & R. Hessen (1967) *Capitalism: the unknown ideal*, NY: New American Library.

[117] A. Rand & N. Branden (1989) *The virtue of selfishness: a new concept in egoism*, NY: New American Library.

[118] J.M. Neal (2000) 'A look at reachback', *Mil. Rev.* **80**(5), 39–43.

[119] M.G. Hazen & R.M.H. Burton (2003) *An application of queueing theory to the analysis of maritime interdiction operations: the impact of net-centric maritime warfare,* Technical report TR-MAR-6-2003 of The Technical Cooperation Program.

[120] L.G. Shattuck & D.D. Woods (2000) 'Communication of intent in military command and control systems' in C. McCann & R. Pigeau (eds) *The human in command: exploring the modern military experience,* NY: Kluwer Academic, pp. 279–91.

[121] North Atlantic Treaty Organisation, Research Study Group (RSG-19) on Modelling of Command and Control of the former Defence Research Group 7 (1999) *Code of best practice on the assessment of* C^2, Report RTO-TR-9 AC/323(SAS) TP/4 of the NATO Research and Technology Organisation.

[122] P.M. Morse & G.E. Kimball (1951) *Methods of Operations Research,* Military Operations Research Soc. 'Heritage Series' (reprinted in 1998).

[123] B.O. Koopman (1980) *Search and screening: general principals with historical applications,* Military Operations Research Soc. 'Heritage Series' (reprinted in 1999).

[124] E.S. Quade (ed.) (1964) *Analysis for military decisions,* Military Operations Research Soc. 'Heritage Series' (reprinted in 2000).

[125] C4ISR Architecture Working Group (1998) *Levels of information systems interoperability (LISI),* Report of the US Department of Defense.

[126] D. Gossink, N. Tomecko, A. Ween, D. Sutton, J. Asenstorfer, M. Britton & L. Zhang (2000) 'A scenario-driven methodology to evaluate capability improvement for communications architectures', *Proc. Defence Operations Analysis Symposium 2000,* session 4, paper 1, General document DSTO-GD-0239 of the Defence Science and Technology Organisation.

[127] W.K. Stevens, W.L. Decker & C.M. Gagnon (1999) 'Representation of command and control (C2) and information operations (IO) in military simulations', in *Modelling and analysis of command and control,* (Proc. Symp. of the RTO Studies, Analysis & Simulation Panel, Issy les Moulineaux, January 1999) Report RTO-MP-38 AC/323(SAS)TP/12 of the NATO Research and Technology Organisation, paper 25.

[128] D.S. Alberts (1999) 'The way ahead' in *Modelling and analysis of command and control,* (Proc. Symp. of the RTO Studies, Analysis & Simulation Panel, Issy les Moulineaux, January 1999) Report RTO-MP-38 AC/323(SAS)TP/12 of the NATO Research and Technology Organisation, paper 28.

DISTRIBUTION LIST

Network-Centric Warfare—Its Nature and Modelling

M.P. Fewell and Mark G. Hazen

AUSTRALIA

DEFENCE ORGANISATION

Task Sponsor Director General Navy Strategic Policy and Futures
Director Navy Strategy and Futures
Deputy Director Future Maritime Warfare

S&T Program

Chief Defence Scientist
FAS Science Policy
AS Science Corporate Management
Director General Science Policy Development
} shared copy
Counsellor Defence Science, London (Doc Data sheet)
Counsellor Defence Science, Washington (Doc Data sheet)
Scientific Adviser to MRDC Thailand (Doc Data sheet)
Scientific Adviser Joint
Navy Scientific Adviser
Scientific Adviser – Army (Doc Data sheet and distribution list)
Air Force Scientific Adviser (Doc Data sheet and distribution list)
Scientific Advisor to the DMO (Doc Data sheet and distribution list)
Director Trials

Systems Sciences Laboratory

Director, System Sciences Laboratory
Chief of Air Operations Division
Chief of Electronic Warfare and Radar Division
Chief of Land Operations Division
Chief of Maritime Operations Division
Chief of Weapons Systems Division
Research Leader Air Operations Analysis
Research Leader Emerging Weapons and Technologies
Research Leader Land Systems
Research Leader Maritime Combat Systems
Research Leader Maritime Operations Research
Research Leader Maritime Sensor Systems
Research Leader Microwave Radar
Research Leader Operations Analysis and Evaluation
Head Land Response Systems, LOD
Head Maritime Operations and Tactics Analysis, MOD
Head Maritime Tactical Experimentation, MOD
Head Military Evaluation Discipline, LOD
Head Navy Capability Studies, MOD
Head Operations Research Capability, AOD

Head Strategic and Land Warfare, EWRD
Head Submarine Combat Systems, MOD
Head Surface Combatant Combat Systems, MOD
Head Undersea Warfare Analysis, MOD
LCDR K. Baddams, MOD
Dr K. Brinschwitz, MOD
Mr P. Gaertner, LOD
Dr G. Kemister, AOD
Dr. B. Kirby, LOD
Dr A. Knight, MOD
Dr R. O'Dowd, MOD
Dr Y. Yue, LOD
Dr M.P. Fewell, MOD (5 copies)

Information Sciences Laboratory
Director, Information Sciences Laboratory
Chief of Command and Control Division
Chief of Information Networks Division
Chief of Intelligence, Surveillance and Reconnaissance Division
Chief of Defence Systems Analysis Division
Research Leader Information Architecture
Research Leader Joint Systems
Research Leader Military Information Enterprise
Research Leader Military Systems Experimentation
Research Leader Theatre Command Analysis
Head Military Systems Synthesis, DSAD
Head Systems of Systems, DSAD
Head Tracking and Sensor Fusion, ISRD
Dr J. Bell, DSAD
Dr G. Calbert, C2D
Mr K. Dean, DSAD
Ms S. Fewell, DSAD
Mr J. Fidock, C2D
Ms M. Hue, IND
Dr J. Legg, ISRD
Dr M. Ling, DSAD
Mr M. Slade, DSAD
Mr R. Staker, DSAD
Mr C. Walmsley, C2D

Platform Sciences Laboratory
Research Leader Undersea Platform Systems

DSTO Library and Archives
Library Edinburgh (1 copy plus additional Doc Data sheet)
Australian Archives

Capability Systems Staff
Director General Maritime Development
Director General Aerospace Development (Doc Data Sheet)
Director General Information Capability Development
Director Information Infrastructure Development
Director Maritime Architecture Agency

Office of the Chief Information Officer

Chief Information Officer (Doc Data sheet)
Deputy CIO (Doc Data sheet)
Director General Information Policy and Plans (Doc Data sheet)
AS Information Strategy and Futures
AS Information Architecture and Management (Doc Data sheet)
Director General Australian Defence Information Office (Doc Data sheet)
Director General Australian Defence Simulation Office (Doc Data sheet)
Director Information Management Futures
Director Information Futures Planning (NCW)

Strategy Group

Director General Military Strategy
Director General Preparedness (Doc Data sheet)
Director Future Warfare and Concepts
Director Force Structure Guidance

HQAST

SO (ASJIC) (Doc Data sheet)

Navy

SO (Science), COMAUSNAVSURFGRP, NSW (Doc Data sheet and distribution list)
Director General Navy Capability, Performance and Plans, Navy HQ (Doc Data sheet)
Director Navy C4ISREW
Director Navy C4 Systems Group

Army

SO (Science), Deployable Joint Force Headquarters (DJFHQ) (L), Enoggera (Doc Data sheet)
SO (Science) – Land HQ, Victoria Barracks NSW (Doc Data sheet and Executive Summary)

Intelligence Program

Director General Scientific and Technical Analysis, Defence Intelligence Organisation
Manager, Information Centre, Defence Intelligence Organisation
AS Corporate, Defence Imagery and Geospatial Organisation (Doc Data sheet)

Defence Materiel Organisation

Head Airborne Surveillance and Control (Doc Data sheet)
Head Aerospace Systems Division (Doc Data sheet)
Head Electronic Systems Division (Doc Data sheet)
Head Maritime Systems Division (Doc Data sheet)
Head Land Systems Division (Doc Data sheet)

Defence Libraries

Library Manager, Defence Library Service – Canberra
Library Manager, Defence Library Service – Sydney West (Doc Data Sheet)

OUTSIDE AUSTRALIA

INTERNATIONAL DEFENCE INFORMATION CENTRES

US Defense Technical Information Center (2 copies)
UK Defence Research Information Centre (2 copies)
Canada Defence Scientific Information Service
NZ Defence Information Centre

ABSTRACTING AND INFORMATION ORGANISATIONS

Library, Chemical Abstracts Reference Service
Engineering Societies Library, US
Materials Information, Cambridge Scientific Abstracts, US
Documents Librarian, The Center for Research Libraries, US

THE TECHNICAL COOPERATION PROGRAM

Maritime Systems Group

Chair, Action Group 1
Canadian National Leader, Action Group 1
New Zealand National Leader, Action Group 1
United Kingdom National Leader, Action Group 1
United States National Leader, Action Group 1
Dr R. Klingbeil, Member, Action Group 1

DEFENCE RESEARCH AND DEVELOPMENT CANADA

Director-General DRDC-Atlantic, Dartmouth
Director General Operational Research, National Defence HQ, Ottawa
Mr Mark G. Hazen, DRDC-Atlantic, Dartmouth (10 copies)

SPARES (5 copies)

Total number of copies: 115

DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION
DOCUMENT CONTROL DATA

1. PRIVACY MARKING/CAVEAT (OF DOCUMENT)

2. TITLE

Network-Centric Warfare—
Its Nature and Modelling

3. SECURITY CLASSIFICATION (FOR UNCLASSIFIED REPORTS THAT ARE LIMITED RELEASE USE (L) NEXT TO DOCUMENT CLASSIFICATION)

Document	(U)
Title	(U)
Abstract	(U)

4. AUTHOR(S)

M.P. Fewell and Mark G. Hazen

5. CORPORATE AUTHOR

Systems Sciences Laboratory
PO Box 1500
Edinburgh South Australia 5111 Australia

6a. DSTO NUMBER	6b. AR NUMBER	6c. TYPE OF REPORT	7. DOCUMENT DATE
DSTO-RR-0262	AR-012-876	Research Report	September 2003

8. FILE NUMBER	9. TASK NUMBER	10. TASK SPONSOR	11. NO. OF PAGES	12. NO. OF REFERENCES
E9505-25-9	NAV 01/389	DGNSPF	52	128

13. URL on the World Wide Web

http://www.dsto.defence.gov.au/corporate/reports/DSTO-RR-0262

14. RELEASE AUTHORITY

Chief, Maritime Operations Division

15. SECONDARY RELEASE STATEMENT OF THIS DOCUMENT

Approved for public release

OVERSEAS ENQUIRIES OUTSIDE STATED LIMITATIONS SHOULD BE REFERRED THROUGH DOCUMENT EXCHANGE, PO BOX 1500, EDINBURGH, SA 5111

16. DELIBERATE ANNOUNCEMENT

No Limitations

17. CITATION IN OTHER DOCUMENTS Yes

18. DEFTEST DESCRIPTORS

Network centric warfare, Command, control and information systems, Information networks, Computer networks, Battlefield information systems, Combat effectiveness, Information dissemination, Military strategy

19. ABSTRACT

This study examines the concept of network-centric warfare with the aims of characterising network centricity as clearly as possible and identifying metrics for 'level of net-centricity'. Properties of network-centric systems, as expounded in the literature, were critically examined to derive examples of suitable metrics. This examination suggests that, except for the provision of reachback, none of the properties is clearly diagnostic of network centricity: it is possible to conceive of systems displaying one or more of them despite not being net-centric as we understand the term. This means that metrics for these properties are not well correlated with the degree of network centricity of the system. Another list of properties was compiled, derived from characteristics of the internet and other effective networks, that is better suited to the identification of network centricity. Consideration of this led to the conclusion that access to a high-capability network is not sufficient for a system to be network-centric, it is also necessary that the network be used in an appropriate manner—a manner supporting the force as a whole, rather than being focused on the needs of a particular unit or platform. Not only must the right information be available to the right person at the right time in the right form, but also it must be put to the right use. This emphasis on motivation in the definition of network centricity parallels, though is distinct from, recent work emphasising human aspects in command and control (C^2). As with C^2, network centricity is not just about hardware. The question of defining a general metric that faithfully indicates level of network centricity is examined with the aid of a specific example, but remains open.