

**Report:**  
**Development of a Foundation for Military**  
**Network Science**

**Prepared for DSTO**  
**by the Systems Engineering and Evaluation Centre**  
**(SEEC), University of South Australia**

**Authors: Lawson, E., Ferris, T., Cropley, D. and Cook, S.**

15 June 06

## Table of Contents

SUMMARY	3
Introduction	4
<b>Work Package 1: Foundational Elements</b>	6
1: What is meant by Network Science?	7
2: What Foundational Elements of Network Science already exist?	14
3 Existing discipline elements relevant to Network Science	27
4: Gaps in Foundational Elements of Network Science	27
<b>Work Package 2: Components and Criteria</b>	29
5: Required theories, methods and knowledge	30
6: Suitability and usefulness criteria	32
<b>Work Package 3: Industry Roles and Activities</b>	35
7. Industry Leadership	36
8. Industry participation	39
<b>Work Package 4: Applications</b>	41
9. Network-centric military operations	42
10. Long-range research	47
<b>Bibliography</b>	48
<b>Glossary</b>	52

### List of Figures

Figure 1: Relationships between technology, science, engineering and engineering science	7
Figure 2: Fully Connected Network of six Nodes	10
Figure 3: Hierarchical reductionist Representation of a System	11
Figure 4: Hierarchical Representation showing inactive potential connections	11
Figure 5: Generalised representation of a Network	13
Figure 6: Generalised Network including a Hub	24
Figure 7: Action-Learning Cycle (Kolb 1984)	33
Figure 8: Boyd's Original OODA Loop Sketch	34

### List of Tables

Table 1: State of Foundational Knowledge	27
--	----

## SUMMARY

This research report has been written in response to a Research Agreement between DSTO and the University of South Australia's Systems Engineering and Evaluation Centre (SEEC). It tests the assertion made by the US Committee on Network Science for Future Army Applications that:

*There is no science today that offers the fundamental knowledge necessary to design large, complex networks in such a way that their behaviours can be predicted prior to building them (National Research Council, 2005).*

We take this to refer to predictions that are deterministic, rather than stochastic. We agree that there is no deterministic science available in the sense that a unique outcome of every action/mission/campaign/war can be predicted by arithmetic combination of quantified capabilities, intentions and positions of the adversaries.

We find, however, that there is an abundance of fundamental knowledge about networks that can be classed as, or assembled into, a Science of Networks. While some of this knowledge is quantitative, much of it is qualitative and distributed among a number of disciplines. Even in its present state of fragmentation there are descriptors of technical, social and socio-technical systems, such as make up a military force, which can be examined usefully with military people to test the potential usefulness and the impact of network oriented methods on operating practices and training.

A methodology for conversion of these qualitative descriptors to quantitative parameters suitable for prediction and control requires research. Any result cannot be in absolute terms e.g., in the social domain there is no absolute unit of Emotional Intelligence or Tacit Knowledge or Transactive Memory. However a relative scale can be envisaged which would enable comparison of different combinations of the features that are necessary and sufficient to characterise a network, keeping in mind that any attempt to combine features must not breach the Principle of Dimensionality.

We take the view that technical systems that realise capabilities such as Intelligence, Surveillance and Reconnaissance (ISR), and also Information and Communications Technology (ICT) systems, are beyond the fundamental "science" stage and are covered by engineering practice. There are problems in those areas but they are problems of implementation rather than shortfalls in discovery, codification and standardisation of fundamental knowledge.

The areas that require attention then are:

- Discovery and codification of the necessary and sufficient characteristics of networks in the military context at all levels of command;
- Research into the quantification of those characteristics;
- Development of a predictive methodology for comparison of effectiveness of different network elements and configurations;
- Understanding the interaction of the social and organisational and the technical aspects of networks in the military context.

## Introduction

In March 2006, DSTO engaged the Systems Engineering and Evaluation Centre (SEEC) of the University of South Australia to report on the state of the foundational body-of-knowledge in Network Science in support of DSTO's provision of science and technology support to the Australian defence community. Presently it is a requirement that all equipment procurement projects include consideration of the implications of Network Centric Warfare (NCW). The Australian Department of Defence has issued the NCW Roadmap which provides the guidance for such consideration.

The motivation for this request arose from the following statements extracted from the 2005 report "Network Science" prepared by the Committee on Network Science for Future Army Applications (National Research Council, 2005):

*There is no science today that offers the fundamental knowledge necessary to design large, complex networks in such a way that their behaviours can be predicted prior to building them (Page 3). It (Network Science) creates fundamental knowledge that enables the a priori prediction of the behaviours of diverse networks in contrast to their a posteriori characterization. In short, network science consists of the study of network representations of physical, biological and social phenomena, leading to predictive models of these phenomena (page 3).*

The inference taken from these extracts is that in the context of the application of Network Science to the US Army of the Future, the prediction sought is deterministic rather than stochastic and the promise by the proponents of NCW is that deterministic predictions are possible. That seems an understandable and desirable objective for a military commander in the field who is concerned with controlling the outcome of each mission. Such case-by-case control needs a deterministic prediction capability.

Further to these extracts the report "Network Centric Operations Conceptual Framework Version 2 (June 2004)" adopts the following definitions of *network* from Webster's Dictionary (page 2):

1. A system or process that involves a number of persons, groups or organisations. Synonyms: organisation, system;
2. An interconnected or related chain, group or system (e.g., a network of hotels; a system of computers, terminals, and databases connected by communications lines.

A key concept in both definitions is that distinct entities are linked and interacting in an organised fashion to achieve some agreed purpose.

For this report we are assuming that in the US military and the Australian military environments the term network refers to technical, socio-technical and social systems

characterised by fast and accurate flow of information that is timely, comprehensive and appropriate to the mission. The purpose of expediting that information is so that it can support predictions of mission parameters, inform decisions by commanders at all levels and enable them to control the outcomes of missions to their advantage in pursuit of the Commander's Intent.

### **Statement of Work**

The research task requires addressing the following ten questions divided, as indicated, into four phases:

#### Work Package 1: Foundational Elements

1. What is meant by Network Science?
2. What foundational elements of Network Science already exist?
3. What existing discipline elements already address aspects that can be identified as relevant to a Network Science?
4. What gaps exist in the foundational elements of a Network Science?

#### Work Package 2: Components and Criteria

5. What theories, methods and knowledge are required to develop a suitable and useful Network Science?
6. What criteria are needed to determine the suitability and usefulness of a Network Science?

#### Work Package 3: Industry Roles and Activities

7. What areas of a Network Science should be led by Industry?
8. What areas of a Network science should Industry participate in?

#### Work Package 4: Applications

9. What role will a Network Science play in network-centric military operations?
10. What long-range research might be needed to implement network-centric operations, in particular for Australian military forces, in a framework of a Network Science?

**Work Package 1**  
**Foundational Elements**

## Work Package 1: Foundational Elements

### *Question 1: What is meant by Network Science?*

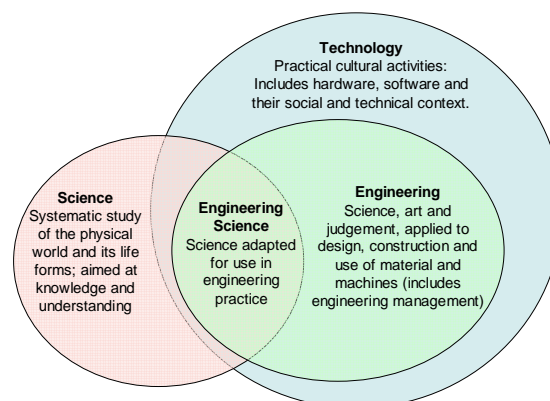
The task of Question 1 is to define what is meant by Network Science. This is addressed firstly by defining our understanding of what Science is, then describing the generalised Network from a fundamental position with, however, an awareness of the military context. Only then do we attempt to elucidate what Network Science may mean.

Science, as a purposeful human activity has been defined by Checkland and Holwell (cited in Cropley, Sproles & Cook 2005) as a combination of:

- An organised body-of-knowledge about a particular area of interest or endeavour;
- The methods used for acquiring that body-of-knowledge;
- The process and methods of applying the body-of-knowledge.

This definition is consistent with the *Concise Oxford Dictionary* (1976) definition of science which concerns both the organised body of the first point, and the processes of obtaining and verifying that knowledge, and which in turn follow from the etymology in the Latin *scientia* which demands epistemological strength of the methods used to obtain the knowledge. Thus the concept of science used here is both consistent with a particular theoretical construct of the nature of science and with the general tradition associated with the secular meaning of the word.

In researching the foundational elements of a science of networks this task recognises that relevant bodies-of-knowledge may be found in all of the four regions of Figure 1 (from Johnstone et al, 1999).



**Figure 1: Relationships between technology, science, engineering and engineering science (from Johnstone et al, 1999)**

The report “Network Centric Operations Conceptual Framework Version 2 (June 2004)” includes an indication of the areas of interest to Network Science by nominating four key interdependent and interrelated domains in which change must occur for transformation of the military from an Industrial Age to an Information Age organisation. These domains are defined in the June 2004 Framework (page 13) as follows:

- **Physical Domain:** where effects take place and where other supporting infrastructure and information systems exist;
- **Information Domain:** where information is created, manipulated and shared;
- **Cognitive Domain:** where perceptions, awareness, beliefs, and values reside and where, as a result of sense-making, decisions are made;
- **Social Domain:** Set of interactions between and among force entities.

A comprehensive science of networks would integrate the bodies-of-knowledge of each of these domains. They are examined in the following sections.

These four domains also serve to illustrate the gulf that besets much of the literature and intellectual endeavours on Network Centric Warfare, Network Centric Operations and Network Enabled Operations. The gulf exists between those who view the Network as a technical artefact, essentially implementing advanced Information and Communications Technology (ICT) systems and those who regard a Network as a cooperating and collaborating community of practice engaged in a purposeful human activity with or without ICT systems. We understand that both views are partially correct but that for Network Centricity to deliver on its promise they have to be reconciled.

In our attempt to bridge the divide this report is based on the following assumption. The technical artefacts that comprise the data gathering, information technology and communications elements of a networked military force are beyond the Science stage of Figure 1 and are positioned in the Engineering and Technology stages. Whilst there will always be certain technical matters for which new knowledge is useful in enhancing understanding, the core knowledge required to address these technical matters already exists and has been firmly established, at least in theory. However it must be acknowledged that practice in both products and processes lags the theory. The allusions to absence of knowledge and to the network representation of physical, biological and social phenomena in the extracts from the Report on Network Science for Future Army Applications are, for the purposes of this study, understood to refer to the emergence of patterns of behaviour and the collaborative cognitive processes of social

and socio-technical networks. These are areas where there is significant need for additional new knowledge, particularly to explain the way networks function under the broad range of influences experienced in real applications.

We believe that this distinction between the technical and the social aspects is supported by the UK National Audits Office report “Driving the successful Delivery of Major Projects” (2005) that highlights the criticality of the cultural environment of projects in achieving successful outcomes. This UK NAO report lists the following four factors as necessary for successful project management:

1. Establishing and sustaining the right cultural environment;
2. Creating clear structures and boundaries;
3. Measuring progress and making decisions focussed on successful project delivery;
4. Reporting to enable strategic decisions.

Without going so far as to say that major defence procurement projects necessarily resemble a war between the contractor and the Materiel Organisations, an analysis of projects suggests that they show many of the characteristics of Network Enabled Operations in that their successful prosecution requires a complementary set of technical and social capabilities.

### **Representation of Networks**

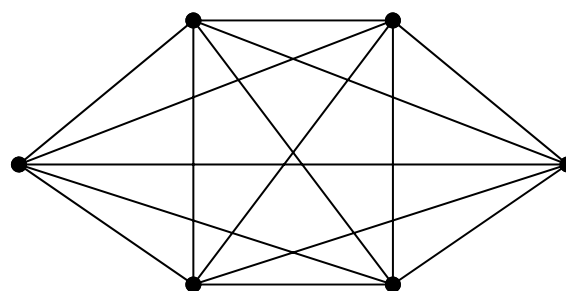
A **Network** is formed when a **number** (between two and infinity) of **distinct entities** that may be **similar** or **dissimilar** (nodes, elements, components, people, military formations, software instructions) are **connected** and **interact** such that **new properties** or **behaviours emerge** that are **beyond** the **capabilities** of any of the entities **acting alone**. These **emergent properties** cannot be **predicted** using **reductionist** consideration of the distinct entities. They are of interest because of the **functions** they perform and the **purposes** they serve, while the distinct and dissimilar entities included within a particular network boundary are those that are understood to be most significant in determining the **emergent properties**.

The properties of the network as a whole can be partially predicted using knowledge of the entities comprising the network and their attributes and properties. However, this knowledge is insufficient to predict the effects which become evident as a result of the complexity of the interactions of the entities and the complexity of the entities themselves, resulting in the possibility of unexpected outcomes when the network is assembled.

The inclusion of only those elements or nodes that are believed to be most significant in determining the emergent properties establishes a boundary for analysis of the network. The boundary is not a natural feature of networks and systems but is an artefact of convenience set as much by the purpose of the intervention as by the grouping of the elements. However the boundary must always be kept under review to ensure that excluded elements are not influencing the emergent properties. Nothing outside the boundary must be of any significance in determining the emergent properties. The boundary must also be chosen so as to minimise the complexity of the interface between the network and that which is outside the boundary. One of the limitations of the formalised processes of systems engineering as often practiced is that they place human social behaviour outside the boundary of the entity under consideration.

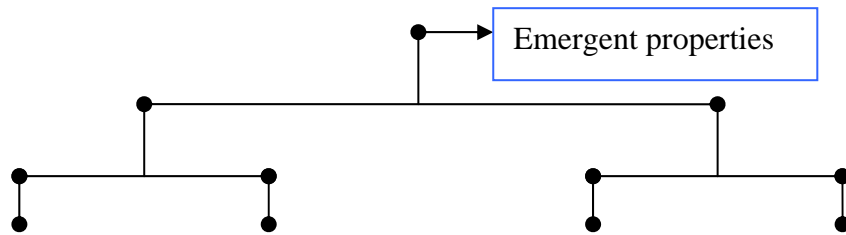
Figure 2, below, represents a fully connected network of six nodes. For a network comprising N nodes, each node can be connected to (N-1) nodes, resulting in a total of bi-directional links  $N(N-1)/2$ . For the six nodes network of Figure 2 the maximum number of links is 15. The representation is such that any node can be a multi-node network on a smaller scale, and each network can itself be a node of a larger scale network.

A moment's reflection shows that in a project team of say 20 people the number of possible connections is 190. It is obvious that if all these are active and of equal influence the outcome could be chaos. Some restriction allowing only those connections that are required is called for in the interests of emergent properties that are not chaotic.



**Figure 2: Fully Connected Network of six Nodes**

The description of a network given above also applies to Systems, commonly represented as a hierarchical, reductionist structure in natural science, engineering, families, Work Breakdown Structures, bureaucracies, the military, religions, computer programs, languages and sports. All these can be represented as in Figure 3 below.



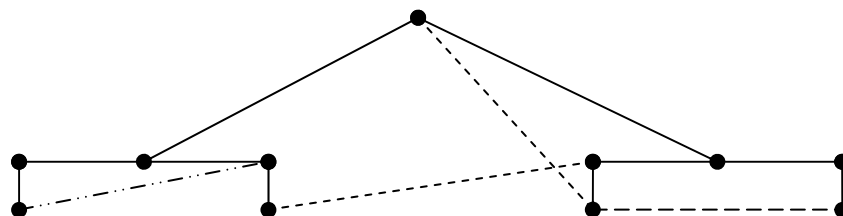
**Figure 3: Hierarchical reductionist Representation of a System**

Both the representations of figures 2 and 3 are useful in relating the emergent properties to the purpose of the group of elements or nodes and developing intervention measures to predict and control in some deliberate way the match between the emergent properties and the purpose.

The reductionist hierarchical representation can be arrived at from the network representation by excluding, suppressing or ignoring some or most of the possible connections between elements or nodes, as illustrated in Figure 4 below, redrawing Figure 3 as an 11 node network with 10 active links out of a possible 55 and showing as dotted lines 4 possible links out of the 45 that are inactive.

A useful indicator that a network has formed is the Clustering Co-efficient, the ratio of the number of actual connections to the number of possible connections. Kauffman (cited in Gribben p165) indicates that a collection of individuals undergo a phase transition to a network when the clustering coefficient equals 0.5. In Figure 4 the Clustering Co-efficient is  $14/55=0.25$ . Another indicator of the reach of a network is Degree of Separation, which is the minimum number of nodes that separate one node from another.<sup>1</sup>

Other indicators of a network that the military should be wary of include sensitivity to initial conditions, a number of possible states, unpredictable transitions from one state to another and non-linear response to perturbations.



**Figure 4: Hierarchical Representation showing inactive potential connections**

<sup>1</sup> The term Degrees of Separation was applied by Miligram (cited in Gladwell) whose experiment in the US in the 1960s demonstrated that a very small number of people are linked to everyone else in a few steps, and the rest of us are linked to the world through those special few.

The reductionist/integrationist methodology of Systems Engineering yields a representation of an entity that has emergent technical properties that are predictable, consistent, linear, repeatable, testable and traceable. By freezing or eliminating most of the possible connections of a fully connected network and organising the remainder into a prescribed hierarchy it allows the transfer of reliance for successful achievement away from people and towards traceability and efficiency through structure and processes, in the Taylorist tradition. There is much to commend in this Cartesian approach, however it has its limitations when the entities under consideration are novel and complex and include social elements or may be subject to rapid and unplanned changes in circumstances, such as a military force deployed against an adversary or in adverse conditions.

The properties that are associated with the network and the systems representations of complex technical and socio-technical entities include:

1. Emergent properties;
2. Hierarchical or multi-level structure;
3. Interdependence and co-evolution of elements. (Maxfield 1997);
4. Mutual constraints of interacting elements (Polanyi 1968);
5. Differential non-linearity under conditions of scale-up or scale-down;
6. Fuzzy boundaries.

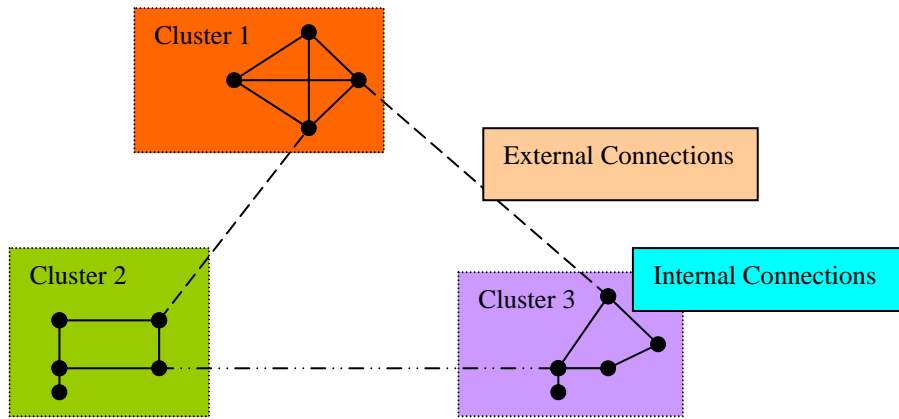
The reductionist, hierarchical representation does not attract attention to the effects of the properties 3 to 6 on the list above. Problems arise in dealing with an aggregation of many such Systems so represented, leading to the concept of System-of-Systems. System-of-Systems can be represented more effectively as a Network. This is a set of clusters of nodes or elements strongly connected within each cluster and with connections between clusters that range from strong to weak, intermittent to permanent and provide the channels for a wide range of transactions.

The foundational elements of Network Science describe (or will describe) the behaviour of the archetypal network in terms of:

- Nodes;
- Clusters;
- Connections<sup>2</sup>.

---

<sup>2</sup> Connections is the term commonly encountered in the literature on Networks to portray the idea that a prime quality of networks is that they are “joined up”. Links is another term. The characterisation of the connections and of the traffic carried on the connections is central to a predictive Network Science.



**Figure 5: Generalised representation of a Network**

Figure 5 shows a generalised representation of a network including three clusters with strong internal links that are connected together by external links which may vary from weak to strong.

Network science is taken to mean the systematic study of nodes, their connections and the emergent properties and behaviour arising out of their interactions, in order to establish:

- An organised body-of-knowledge;
- Methods for developing that body-of-knowledge;
- Methods for applying that body-of-knowledge.

***Question 2: What Foundational Elements of Network Science already exist?***

For this report foundational elements of Network Science are assembled under the same domain headings and definitions that are used in the report “Network Centric Operations Conceptual Framework Version 2 (June 2004)”:

- **Physical Domain:** where effects take place and where other supporting infrastructure and information systems exist;
- **Information Domain:** where information is created, manipulated and shared;
- **Cognitive Domain:** where perceptions, awareness, beliefs, and values reside and where, as a result of sense-making, decisions are made;
- **Social Domain:** Set of interactions between and among force entities (page 13).

A military network becomes effective when all domains interact as a system, the emergent properties of which are the Netforce as described by Keus (2005).

**Physical Domain**

We understand that in the military context, the Physical Domain comprises two components. The first includes those data acquisition systems that measure or describe the environment of an Area of Operations and as far as possible contribute to a picture of the Battle space. These systems include:

- Sensor systems such as radar, electro-optics, signals and electronic signals intercept;
- Human intelligence;
- Terrain maps, movement corridors and obstacles;
- The built environment of roads, airports, bridges, buildings, electricity and water supplies, radar and communications installations;
- Weather;
- Size, composition, location, disposition, direction and speed of movement of friendly and adversary forces.

These may be configured as a sensor network with cross cueing, correlation of data and resolution of ambiguities. The foundational elements that support individual sensors and a sensor network are well established and reside in the technology zone. Standardisation of formats to ensure compatibility of data is more an issue of implementation, standardisation and co-ordination rather than one of foundational elements.

The second component of the physical domain as defined in the reference document includes the supporting infrastructure and information systems that transport, store and retrieve the data generated by the multiple sources that comprise a Military sensor grid and the decisions that arise from analysis of data. These systems generally come under the banner of Information and Communication Technologies (ICT) for which elements of foundational understanding exist in several bodies-of-knowledge including communications theory, error detection and correction, queuing theory, local and distributed databases, software engineering, computer processor and memory architecture, computer systems security and the related hardware engineering.

In the Communications field there is a wealth of research and established practice in telecommunications network analysis and design dating back decades. Conventional queuing theory<sup>3</sup> is routinely used to dimension communications networks and analyse their performance under various conditions. It also finds particular application in determining blocking probability in busy telephony networks and latency in packet-switched networks. Tools such as Opnet and the military equipment enhancement models provided by Netwars<sup>4</sup> are well established in analysing the performance of military C2 systems. Moreover queuing theory is but one example of the scientific basis to network design and management; more can be found in senior undergraduate or graduate texts on the analysis of systems<sup>5</sup>. For example, in 1997, The Institute for Telecommunication Research (University of South Australia) identified over 20 analysis methods that were considered sufficiently well developed at that time to provide useful mathematical insight into tactical command and control networks<sup>6</sup>.

While we would not wish to imply that we can predict the behaviour of very large technical networks with complete precision, it is simply misleading to imply that there is no scientific basis to network design and operation. In addition even in networks that are evolved without a central controlling authority, for example the global Internet, there exist mathematically definable attributes that provide operators and analysts the opportunity to study and predict behaviour. One outstanding area requiring research is the apparent clustering of failures of large networks. The occurrence of unpredicted events

---

<sup>3</sup> Kleinrock L., *Queuing Systems*, Wiley 1975.

<sup>4</sup> [http://www.opnet.com/products/library/newars\\_models.html](http://www.opnet.com/products/library/newars_models.html)

<sup>5</sup> Severance F.L. *System Simulation and Modeling, An Introduction*, Wiley, ISBN0-471-49694-4, 2001. Blanchard and Fabrycky,

Harms D.D., Kraetzl M., Colburn C.J., and Devitt J.S., *Network Reliability*, CRC Press, 1995.

<sup>6</sup> Lever K.V., Cook S.C. and Qureshi A.G. *Impact of Tactical Networks on Information Systems Performance*, DISC97-63312-01, Institute for Telecommunications Research, University of South Australia, 53 pages, 1997.

that are contiguous in space and/or time suggests that the modelling of events as random may not be as close to reality as modelling the magnitude and frequency of events according to an inverse power law.

However notwithstanding the wealth of research and established practice, problems are still being experienced in the implementation and operation of large scale ICT systems-of-systems in both the military and the civil fields. In civil applications, as evidenced by the series of Standish Reports, large scale complex distributed ICT system-of-systems being developed for service show a similar failure rate to that associated with military systems. This suggests that although the necessary and sufficient foundational knowledge is available the application of the knowledge bases is not yet widespread<sup>7</sup>.

Failures or partial failures are occurring in the engineering and technology zones and are traceable to:

- Contracting strategies that are inappropriate and adversarial;
- Unrealisable and poorly expressed requirements;
- Loss-leader bidding;
- Lack of progressive test and evaluation programs;
- The fallacy of COTS;
- Poor project management practices in the Social Domain;
- Shortage of experienced ICT systems engineers.

Additional complicating factors are experienced by some ICT systems. The World Wide Web, International Banking and Finance as well as the military expect their ICT systems to be subject to attack by adversaries in order to:

- Extract information and leave no trace;
- Insert misleading information or corrupt data streams, again covertly;
- Disable ICT systems.

As well the processes of introduction into service of new military systems are different from that of civil systems, which effectively go live as soon as they are switched on. The distinction between verification and validation becomes important. Whereas civil systems are immediately subjected to the issue of “Does the system do what is needed to do today’s jobs?” military systems are not subject to that scrutiny until the next conflict which may be some years after introduction into service. Instead, new military systems

---

<sup>7</sup> In 1998 the Standish Group reported that 26% of projects were successful, 46% fell short of time, cost and/or performance objectives and 28% were cancelled.

are tested and evaluated against the question “Does the system do what we asked for?” These differences indicate that the successes of civil systems may not translate directly into the military field. The analogy that was drawn in the initial exposition of NCW between civil and commercial ICT systems and military ICT systems needs to be examined for validity (Alberts, Garstka & Stein 2002).

The interface between the Physical domain and the Information and Cognitive domains is the Human-Machine Interface (HMI). The foundational elements for this critical element of networks reside in all four domains. Multidisciplinary research is required to ensure that information overload is not exacerbated by the flood of data that can be provided by an array of networked and communicating sensors.

### **Information Domain**

According to the definitions above, information is created, manipulated and shared in the Information Domain and perceptions, awareness, beliefs, and values reside in the **Cognitive Domain** and, as a result of sense-making, decisions are made.

For this report we have combined these two domains because the transform from data to information, knowledge and agreed meanings is an iterative process that cannot be reduced to a sequential process. Accordingly the following examination of foundational elements encompasses both the Information and Cognitive domains.

The critical activities by the Command Group in these two Domains are:

- Reception of new information;
- Correlation with existing knowledge;
- Analysis for Meaning in the immediate context;
- Sense-making;
- Distinguishing between novel situations and those that have precedents;
- Decision making.

This is an iterative recursive process. However it is possible to identify foundational elements that describe the basic processes involved. The transform from data to meaning involves learning and from the field of Education, Illeris distinguishes between cumulative, associative and accommodative knowledge, and has described the process of collective learning. Collective learning is a specific case of organisational learning, and is understood to be the same concept that Senge in the Fifth Discipline envisaged when he used the term Organisational Learning.

Collective learning occurs when a package of information is internalised by the members of a team which has formed an enduring agreement on the meaning of the information and the context of its application. According to Illeris there are three conditions which must be met for collective learning to occur. They are:

- 1) The collective group must be in a common situation;
- 2) The participants in the sphere the learning is concerned with must have extensive presuppositions, e.g. a “formed” team (Tuckman 1965) or a Community of Practice (Wenger 1998);
- 3) The situation must be of such a common emotionally-obsessed nature that there exists a clear basis for everyone to mobilise the necessary psychological energy for transcendent (accommodative) learning and to be prepared for the common nature of the situation.

According to Illeris the way knowledge is internalised depends on prior learning and may fall into one of the following three categories:

Assimilative, when the new information is adapted to and incorporated into established structures;

Cumulative, when there is no previous knowledge on which to build.

The new information cannot be related to established structures in Long term Memory and may be added as a new element of knowledge, rejected, or incorporated into an inappropriate established structure;

Accommodative, when the new information leads to the reconstruction of established structures through dissociation, liberation and reorganisation (Illeris, 2002).

**Assimilative** is the ideal mode in that new information correlates closely with existing knowledge and both reinforces as well as extends the structures of existing knowledge. This is the principle mode of Constructivist learning (Merriam and Caffarella, 1999, Vygotsky, 1978).

**Cumulative** implies that there are no existing structures from which valid meanings for the new information can be derived. A serious hazard is that the new material will be associated with inappropriate structures and invalid meanings will be attributed. In such cases there will be no recognition that an appropriate knowledge structure does not exist.

**Accommodative** is the mode which can lead to the most serious difficulties in a team. Accommodative learning requires that existing structures be changed in the light of new information. Among the many responses to the pressures for accommodative learning are:

- Denial ( if I ignore it, it doesn't exist);
- Issues of conflict (which version is correct);
- Pride and self esteem (I will lose face if I change my position);
- Authority (I am the senior person and have to be seen to be right);
- Rigidity (I am too set in my ways to change).

Any of these can generate resistance and divisiveness, halt progress and lead to incorrect outcomes in the cognitive domain.

Wegner (1991) has made useful progress in developing theories that support qualitative predictions of performance of small groups in terms of transactive memory. The concept of transactive memory explains that each member has custodianship of only part of the total package of knowledge that informs the group's activities and deliberations. A team which has developed a transactive memory has divided the details amongst the members, such that they all don't need to know everything. It is sufficient for each member to retain three pieces of knowledge. The first is the high-level structure of the system of knowledge relevant to the situation. The second is the identity of the custodian of the details of each element of that structure of knowledge, while the third is the detailed knowledge of the particular element for which he or she is responsible. A team with a resilient transactive memory would have redundancy and a peer-to-peer process for collective learning and allocating new classes of information.

Distributed Intelligence (Gardner 2004, Hutchins 1995, 2000) completes a structure of knowledge management with Collective Learning and Transactive Memory. The term has been associated with computer based systems to describe the accelerated performance that can be achieved when several computers work on the same problems and datasets simultaneously. Such parallel operations are more correctly called distributed processing. Prior to the computer era, libraries, books, lecture notes and the like were referred to as distributed intelligence and again a more precise term would be distributed information.

These distinctions are important in order to reserve the use of the term "Intelligence" for the operations that humans perform in their minds when they apply their knowledge and experience to make sense of and formulate a response to some information. Distributed

Intelligence is demonstrated when a group or team exploit their collective learning and transactive memory to jointly make sense of the information under consideration and agree on the responses. In systems terms, the distributed intelligence is an emergent property of the knowledge, experience, collective learning and transactive memory of the members and, as is the characteristic of a system, the whole is greater than the sum of the parts.

A group that experiences collective learning, has developed a transactive memory, and applies its distributed intelligence to sense-making and decision taking can be said to be truly networked. These three theories are foundational elements that could lead to *a priori* prediction and control of the performance of a command team in terms of network characteristics.

A critical activity in the Information and Cognitive domains is distinguishing between novel problems and situations and those that have been experienced previously. Where situations have precedents, a mature organisation will have a library of solutions, Standard Operating Procedures (SOPs), which have been found to work in similar situations. Much of the activity undertaken by any large organisation is governed by procedures and processes and this is essential for efficiency, devolution, accountability and quality assurance.

However, when the situation is novel and falls outside the coverage of processes a different approach is required. This is common in military operations as both sides can be expected to be working very hard to create situations that are outside the immediate capability of the adversary. Innovation and Creativity is called for and this process has been well described by Cropley & Cropley (2000) as encompassing the following stages when applied to Systems Engineering. It can also be applied to the resolution of novel and complex problems in many fields including the Military. The stages are:

**Preparation:** Acquisition over a period of time of latent or tacit knowledge of the domain in which the issue or problem that requires creativity and innovation occurs;

**Immersion or Information:** Assembly and consideration of the information relevant to the issue or problem;

**Incubation:** Subconscious cross referencing of the information and the problem; the mental scrolling through of an array of possible solutions;

**Illumination:** Unbidden appearance of a solution; the happy idea that is a “best fit” between the information and the problem;

**Explication or Verification:** Follow-up detailed exposition and testing of the solution;

**Communication:** Sharing of the solution with colleagues for their criticism, modification, acceptance and use;

**Validation:** Demonstration that the artefact which embodies the solution solves the original problem.

Organisational structures, processes and standard operating procedures arise from validated solutions to recurring problems. Where the problem is novel, the stages of Immersion and Incubation allow for reflection to occur. These stages of innovation and creativity apply to groups as well as to individuals. A group that has experienced collective learning, developed a transactive memory and in applying its distributed intelligence to novel problems follows the innovation and creativity stages is called a High Performing Team.

We believe that High Performing Teams are essential to successful exploitation of the technological advantages of networking in the Physical domain. We move on to the Social Domain for it is in that domain that we find foundational elements that explain how a group of people can be formed into a High Performing Team.

### **Social Domain**

Foundational elements or properties of networks have been described by a number of authors including Capra (The Web of Life and The Hidden Connections), Gladwell (The Tipping Point), Gribben (Deep Simplicity), Prigogine and Stengers (Order out of Chaos), Bak (How Nature Works), Alberts and Czerwinski (Complexity, Global Politics and National Security), Eldridge and Gould (Punctuated Equilibrium). However these are qualitative *a posteriori* descriptions of observed behaviour.

Barabasi (Linked; The New Science of Networks), takes a further step into the study of Social Networks by quantitative analysis of some observed properties. He has advanced our understanding of networks by the confirmation that the rate of incidence of critical parameters as a function of magnitude follows an inverse power law rather than a Gaussian distribution as proposed and applied in Graph theory by the Hungarian mathematicians Erdos and Renyi.

According to Barabasi, Network Science is traversing the path of discovery associated with advances in knowledge. That is the sequence of:

- Empirical observation of the behaviour of a phenomenon;

- Models that reproduce the observations;
- Theories that predict the behaviours.

We understand that the present state of Network Science in the social domain with regard to this sequence is that there are plenty of empirical observations, that there are some models that reproduce the observations, but only a beginning of development of theories that predict behaviours.

The network representation requires the inclusion of social behaviour as this is an inevitable part of the socio-technical entities that underpin modern society, including military organisations. This applies not only to the entities but also to the temporary construct that brings them into existence e.g., an engineering project organisation or a software development team. When technology and people interact there is a compounding of the effect of the one on the other, so that the presence of technology of certain characteristics results in modifications of the human action, both individually and corporately. The insertion of technology into any situation results in changes to the relationships of the people because of the change of information available to the parties, thus changing the knowledge aspect of their basis for social interaction. This can then challenge the basis for the formal structures with codified relationships, and consideration must be given as to who has the authority to do what (Spinuzzi, 2003).

### **Network Fundamentals**

Barabasi, a physicist, appears to have made the most comprehensive observations of networks and his results indicate the following:

- The frequency of occurrence of network processes as a function of magnitude is not random but follows an inverse power law;
- Networks grow/shrink one node at a time;
- Newly joining nodes show a preference for attachment to the more well-connected existing nodes;
- A few nodes exhibit a very high connection count;
- Most nodes have a modest connection count;
- Some have not many connections;
- There is a path from every node to every other node;
- Some clusters have redundant parallel connections to other clusters; others are relatively isolated with few or one connection;

- The population of nodes forms into clusters with high traffic density on internal connections and low average traffic density of a different kind on external connections to other clusters.

Several authors note that for an assembly of elements to qualify as a network, it has to demonstrate the capability for self-organisation. We believe this to be close to the concept of self-synchronisation used by the proponents of NCW and we consider it to be a key factor in any considered and successful application of network science to military operations. Designing in this capability or, more correctly, establishing the conditions for its emergence without at the same time disrupting the chain of command is an area requiring research.

For a collection of individuals to qualify as a network the average number of connections per node must be a minimum of one and at least half of the potential connections must be made. The combination of strong and weak connections leads to rapid dissemination of information across a network without an unnecessary overhead of infrequently used communication channels. Whereas strong connections may support routine operations, it may be that the weak connections hold the key to self-organisation.

The suite of functions observed in a network includes:

- knowledge generation from new and pre-existing information;
- rapid dissemination of new information;
- formulation of decisions;
- synchronised actions.

These functions have been examined and described by Gladwell in “The Tipping Point”. He identifies three types of person in a flourishing social network:

- The Maven<sup>8</sup>, the collector of knowledge and broker of information;
- The Connector, who knows a very large number of people;
- The Salesperson, who gains acceptance of the new ideas.

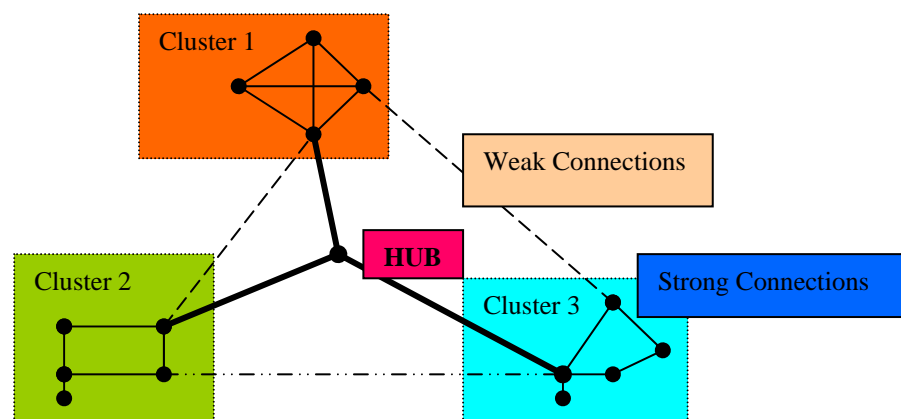
These three distinct types give variety and effect to the links between clusters and allow for the development of quantitative measures of the vitality of a given network. An existing or notional network can be examined for the presence of the three types and each rated on a relative scale. As an example of a possible quantitative measure, Barabasi has found that a top-of-the-box Connector will have at least ten times the average number of

---

<sup>8</sup> Maven is a Yiddish word that means one who accumulates knowledge. To avoid a term that may be unfamiliar to most readers this report uses Knowledge Broker hereafter.

connections for a given population. The actor John Carradine has 4000 links to other actors compared with a count of less than ten links for 41% of actors. Barabasi has found a similar anomalous ratio in his analysis of the Internet, and has defined a hub as a special case of a node that has such an above average number of connections and is accepted as a member of many clusters across many networks. This finding applies to both technical as well as social networks and is further refined by the concepts of robustness and fitness both of which Barabasi and his colleagues have modelled quantitatively.

Figure 6 completes the model of a generalised network with the addition of a Hub to Figure 5.



**Figure 6: Generalised Network including a Hub**

The discussion above suggests that Network Science may enable us to move beyond empirical observation and models that reproduce the observations to;

- Theories that predict the behaviours.

However we are not aware of theories that describe and predict the formation of the large-scale peer-to-peer networks that in recent years have proliferated on the Internet. We believe that the characteristics and interests of the foundation members establish the social capital of a given network, which is a more dominant factor than structure and process in determining the behaviour and outcomes of networks.

It may be of concern to the military or the business communities that the cohort of young people now entering the operational ranks may bring with them from their formative experiences with peer-to-peer networking, practices of communicating, analysing information, making decisions and sharing or avoiding responsibility that have little or no relationship to the organisation's espoused structure and processes. Given the

potential for social capital to be, inter alia, bridging, bonding, exclusive, supportive, benign or hostile there is a need for research in this area that specifically addresses the management of peer-to-peer networks in the context of military network centric operations.

Cohen and Prusak (2001) contend that networks do not enable the development and exploitation of social capital unless there is face-to-face contact in the early formation stages and regular gatherings to refresh the knowledge that each member has of the others' characters. They list four basic problems with virtuality:

- 1) *None of the technology of virtuality can currently carry even a fraction of the whole range of communications that people use to relate to one another and build capital.*
- 2) *Virtual connections and the attention we give them tend to be brief and intermittent; durable social connections and social capital take time.*
- 3) *Virtual connections tend to have a clear, limited purpose and consciously chosen and limited participants; social connections more often grow from chance encounters and broad-ranging conversation and chat.*
- 4) *Virtual communication such as e-mail and video conferencing may actually distract people from what is going on around them so they are, in effect, "neither here nor there." (Cohen & Prusak, 2001. p.163)*

We note that these problems were reported by Cohen and Prusak in 2001 and may be based on their observations in the mid to late nineties. We suggest that with further development of Internet technology and the arrival on the scene of a new generation they may need revisiting. Work by Pattison and Robins from the University of Melbourne<sup>9</sup> in Social Network Analysis (SNA) indicate that there are multiple networks operating in any organisation, for example, the reporting network, the workflow network and a daily exchange network. Further research is clearly needed but there are indications that even in an organisation where people are collocated the social networks and their activities bear little resemblance to the formal structure and processes respectively. The effect of distributed networks on the already uncertain relationship between formal structure and process and social networks requires research.

Our conclusion is that much knowledge that could be called Foundational Elements of a science of networks already exists but the elements are spread across a range of disciplines that are not noted for their ability to engage in transdisciplinary discourse. We

---

<sup>9</sup> Presentation on Multiple social networks in Organisations at DSTO Edinburgh on 9 June 2006.

suggest that multi-disciplinary research would accelerate the rate of development of a coherent body-of-knowledge that could be called Network Science.

**Question 3: Existing discipline elements relevant to Network Science**

In the previous sections several existing disciplines relevant to Network Science have been identified and discussed. Their current status for each of the domains analysed is summarised in the following Table 1 for each of the regions across the spectrum from science to technology illustrated in Figure 1. If an additional column was included for the integration of the bodies-of-knowledge spanning the four domains the entries would be in the Low to Non-existent range.

**Table 1: State of Foundational Knowledge**

	DOMAIN*			
	Physical	Information	Cognitive	Social
<b>Science</b>	High	Medium	Medium	Medium
<b>Engineering Science</b>	High	High	Medium	Low
<b>Engineering</b>	High	High	Low	Very Low
<b>Technology</b>	Medium	High	Very Low	Very Low

- \*High means that the foundational elements are known, standardised and are routinely applied to control and predict outcomes;
- Medium means that some foundational elements have been identified and standardised but not to a sufficient extent that outcomes can be deterministically predicted and controlled with confidence;
- Low means that foundational elements are still emerging from diverse sources; there is no agreement on how critical factors are identified in a given context and any coincidence between predictions and outcomes is serendipitous;
- Very Low means that some researchers believe that consistent relationships between predictions and outcomes are possible but there is neither standard application methodology nor agreement on what the determining factors are.

**Question 4: Gaps in Foundational Elements of Network Science**

While several minor gaps have been identified throughout the body of this report, two major gaps are described in this section. The first is the absence of multi-disciplinary collaboration. By this we mean that fragments of knowledge that are seen as foundational to network science exist in a number of disciplines, e.g., physics, education, psychology, philosophy, education, sociology, biology medicine, communications, systems and software engineering and project management. These divisions of the total knowledge base of western society are a result of the Age of Specialisation and the organisation and codification of knowledge into fields. It could be said that each specialist field embodies a network with very strong internal connections but with external connections that range from very weak to non-existent. This is seriously inimical not only to transdisciplinary discourse, let alone multi-disciplinary research, but also to the prospect of success for a military network comprising elements of different disciplines. The different disciplines in

the military network may be encountered in the interfaces between the four domains discussed earlier, particularly between the physical domain, and the human domains, but also in the diversity of disciplines represented by the people participating in the social domain, where there is a need for communication between people under conditions of high stress.

As an example, Barabasi (a physicist working in cancer biology) refers to a paper “The Strength of Weak Ties” by Mark Granovetter, a Graduate student in sociology which took four years to be accepted for publication, that triggered off Duncan Watts, a mathematics PhD student, who was studying the apparent self-synchronisation of crickets and with his supervisor, Steven Strogatz, introduced the concepts of *clustering coefficient* and *separation* between nodes. That enables the formation of some measurement of the structure of the network. But it tells us nothing about the life cycle of clusters or of the traffic on the “weak ties” between clusters. We find theories about those properties in social and socio-technical systems somewhere else in say the works of Bourdieu on Forms of Capital, Lave and Wenger on Communities of Practice, Janis Irving on Groupthink and Cohen and Prusak on Social Capital.

The second gap is the absence of research into quantitative measures of properties of entities. Peter Sydenham’s work in measurement science is at the forefront of this initiative and David Crompton’s thesis carries it on. This is relevant to Network Science in that it extends the notion of measurement beyond putting numbers against a symbolic representation of a physical phenomenon to consideration of a quantised expression of meaning, use, and value. The knowledge already available allows us to establish a set of parameters that are central to the characterisation of the basic elements of networks, namely nodes, hubs, clusters and links. None of these parameters can be described in terms of the classic measurands, for example those derived from length, mass or time. However scales that allow relative comparisons between networks are possible. The combination of these quantised descriptions of different parameters has to be treated as a multi-dimensional problem.

**Work Package 2**  
**Components and Criteria**

## Work Package 2: Components and Criteria

### *Question 5: What theories, methods and knowledge are required to develop a suitable and useful Network Science?*

The approach taken to this question is to examine the network of agencies that are or would be involved in the development, acquisition and fielding of a military capability based on Network Science. The intention is to draw a distinction between the product and the process. Product encompasses the equipments and systems which enter service and which deliver specific capabilities by virtue of their functions and emergent properties. Process refers to the activities of the several agencies that are associated with the development, acquisition and test and evaluation of the product up to the point of acceptance into service. Our contention is that there is not much value in having a sound knowledge of the foundations of a science of networks that is of use and value to the military if the capability to translate that knowledge into practice does not exist.

The report on Network Science that caused DSTO to initiate this study asserts in the Executive Summary that:

*In spite of society's profound dependence on networks, fundamental knowledge about them is primitive....There is a huge gap between what we need to know about networks to ensure the smooth working of society and the primitive state of our fundamental knowledge. This gap makes the military vision of NCO problematic, at best.*

We would qualify those assertions as we believe that fundamental knowledge is not primitive. It is however dispersed among several disciplines and not readily accessible. We agree that the military vision of NCO as espoused by the CCRP is problematic, but believe that this is due more to an immature state of knowledge on how to bring military networked systems into being, and the limits of deterministic prediction and control rather than a lack of fundamental knowledge.

We accept the claims that networking should be a force multiplier; that superior information of the battle space rapidly disseminated should facilitate the concentration of force and/or effects within the decision cycle of an adversary leading to mission success. Importantly however the extent to which network science can secure prediction and control sets limits on the magnitude of the force multiplier effect. This is particularly so in the military context which is characterised by a strong attachment to centralised command and control and the chain of command, with good reason based as it is on centuries of experience.

These considerations indicate that the introduction of networking capability into the military would mark a punctuated equilibrium episode in the management of military

missions and campaigns. The emergent properties in terms of military capability cannot be predicted. This is not because the state of knowledge of networks is primitive but because the properties that emerge from the interaction of networks with the military environment cannot be predicted. Two broad approaches are available to resolve the issues associated with the network-induced punctuated equilibrium. The first is to recognise that the military environment is characterised by deep structure implementing controlled intentions. In such an environment the force multiplier gained by ICT driven networking may not be as spectacular as the gains from the second approach of converting the military from the command structure into one characterised by flexible structures and opportunistic intent. The risks associated with the second approach are very high.

What is not known is the point of balance between the two extremes that the Australian Military can accept. Experimentation through intermediate stages is the low risk path to establishing an acceptable point of balance. Only through experimentation can the theories, methods and knowledge from the bodies-of-knowledge on Networks which will be suitable and useful to the Australian military be identified. Some theories, methods and knowledge may be found not to be useful and suitable and that would be a good outcome in itself.

As well, the risks associated with the accepted acquisition processes are very high. In general acquisition proceeds from a family of specifications that in the most favourable cases are based on knowledge of what is available, affordable, effective and testable as well as useful. When networks are considered in the broadest sense, that is social as well as technical, knowledge that would form the basis of specifications is not currently available. It is essential that the program of experimentation by the military referred to above involve the DMO, DSTO and Industry. This is discussed further under Question 8; “What areas of Network Science should Industry participate in?”

***Question 6: What criteria are needed to determine the suitability and usefulness of a Network Science?***

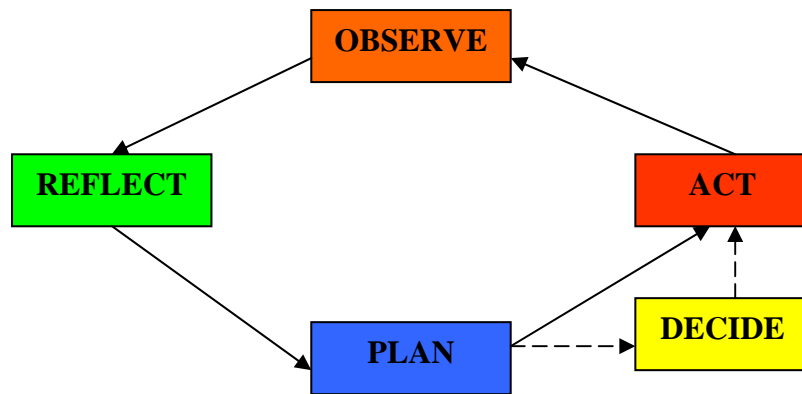
A hierarchy of criteria to determine the suitability and usefulness of a Science of Networks can be proposed but these must be developed in association with the military lest Network Science becomes yet another solution looking for a problem.

We understand the purpose of the Physical Domain of the Network is to provide relevant, timely and accurate input into the Information Domain in order that the military decision makers operating in the Cognitive and Social Domains can extract meaning, make sense of the information and formulate effective decisions. There are a number of diverse sub-systems implicit in that description performing interdependent functions. They are:

- The sensor grid that collects relevant, timely and accurate data about the area of operations;
- A processing and fusion capability that reconciles anomalies, rejects misinformation and converts the accepted data into standardised information;
- A communications grid that disseminates that information to the decision makers and the decisions to the warfighters;
- The decision makers who must extract meaning from the information and decide on the next move in the campaign;
- The warfighters who translate the decisions into action and change the physical conditions of the area of operations, which is detected and reported by the sensor grid.

From this description the Networked military force could be viewed as a feedback control system and criteria established in terms of time constants, threshold, non-linearity, transport delays, hysteresis, saturation and noise.

Alternatively, the networked force could be regarded as participating in an Action-Learning cycle (Kolb 1984) shown in Figure 7 below.



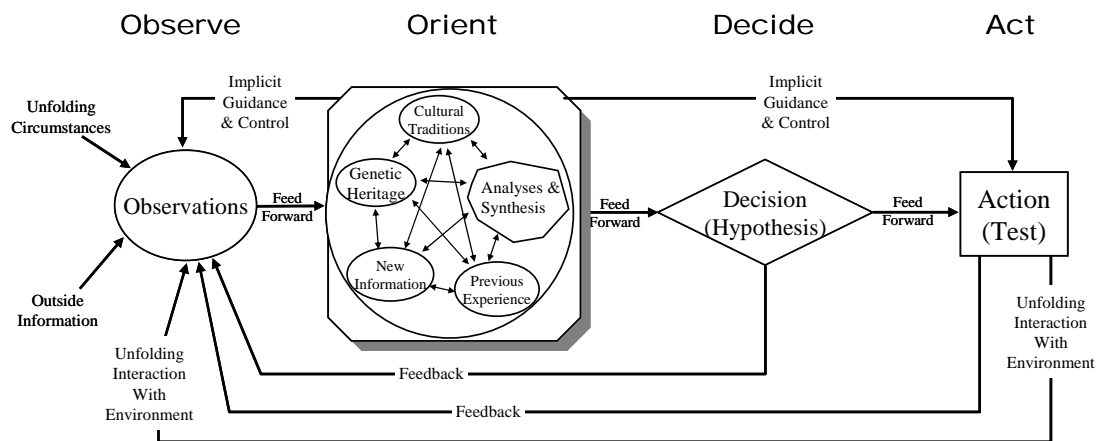
**Figure 7: Action-Learning cycle (Kolb 1984)**

The Action-Learning model is more attractive than the abbreviated version of the OODA Loop often encountered in military documents in that it includes a Reflection phase during which the new information that has been observed would be acquired, assimilated and given meaning by the participants. The Action-Learning cycle, while it could be improved by the addition of a Decide phase as shown in Figure 7, defines the processes of collaborative learning that is central to the social aspects of networked operations. A learning phase is not anticipated by the abbreviated OODA Loop model which implies a sequential, mechanistic progression from Observe to Orient to Decide to Act.

However the original depiction of the OODA Loop by Boyd shown in Figure 8 is much richer in detail and shows features that are not usually examined. They are:

1. Expansion of the Orient phase to include the elements of learning;
2. Inclusion of a feedback loop from Orient to Observe (refining the Observations before Decision);
3. Explicit connection from Action to Observation reinforcing the notions of continuous operations and decision cycle times.

The advantage of the Action-Learning model over the feedback control system model is that it concentrates attention on the development of the meaning of the data collected by the sensors and provided by other sources. Boyd's original sketch (below) seems to be capable of encompassing both action-learning and feedback control.



Note how orientation shapes observation, shapes decision, shapes action, and in turn is shaped by the feedback and other phenomena coming into our sensing or observing window.

Also note how the entire "loop" (not just orientation) is an ongoing many-sided implicit cross-referencing process of projection, empathy, correlation, and rejection.

From "The Essence of Winning and Losing," John R. Boyd, January 1996.

Defense and the National Interest, <http://www.d-n-i.net>, 2006

**Figure 8: Boyd's Original OODA Loop Sketch**

The science of sensors is well established, while the problems of implementation of intelligence, surveillance and reconnaissance systems lie in the realms of technology and engineering practice as does the implementation of information technology and communications systems. Criteria for the suitability and effectiveness of the Physical Domain are well established. For example, The Shannon criteria of effectiveness refer to the statistical properties of communications systems. However it tells the decision makers nothing about the meaning of the bits of information transmitted and received. Suitability and effectiveness criteria are less obvious in the Information and Cognitive Domains.

It is our understanding that the aspect of Network Science dealing with those domains would address the meaning of the material presented to the decision makers and since there is very little research available that takes the step from qualitative to quantitative it is not possible at this stage to define criteria of suitability and usefulness. Qualitative criteria of suitability and effectiveness in the Social Domain are available but require further work in collaboration with the DSTO and the Military. There is sufficient material to support useful interaction with DSTO and the Military to progress the issue of criteria for each of the domains.

**Work Package 3**  
**Industry Roles and Activities**

### **Work Package 3: Industry Roles and Activities**

#### ***Question 7: What areas of a Network Science should be led by Industry?***

We understood that the Industry referred to as a potential leader in areas of Network Science is the sector whose major business activity is the supply and support of the Australian Defence Forces. The capabilities and technologies of this sector are shaped by the equipment procurement and support practices of the Australian Department of Defence. Since most equipment is sourced overseas, in-country investment in foundational research by this sector rarely flows through to profitable orders. The business case for foundational research cannot be made and is only ever occasionally supported out of company funds. The lack of investment in foundational research is a recognised weakness, albeit a consequence of the purchasing practices of its major (sole in many cases) customer.

DSTO is regarded by many in this industry sector as the repository of foundational knowledge of defence science and technology. From time to time industry speakers claim that the virtual monopoly by DSTO of defence science and technology funding constitutes a barrier to participation in foundational research. The cheap and seductive option of “dual-use” technology by which the military benefits from developments in the civil sector has proven illusory.

This situation of an industry that does not have a record of investment in defence science and technology that flows through to product and profit has arisen over a number of epochs in the history of Australia since Federation. The first epoch extends from World War 1 to the fall of Singapore in 1942 during which Australian Defence Industry was almost solely owned by the Australian Government. It was in effect part of the Australian contribution to the total military instrument of power that existed to defend the world-wide British Empire, of which Australia was a part. Integration with the military forces of the Empire was the prime driver of doctrine, training and structure. Procurement practices were such that most platforms and systems were sourced in the United Kingdom. This integration with the military forces of the British Empire is very well described in the following extract from a letter written in November 1943 by Field Marshall Blamey to the Chief of the Imperial General Staff, General Brooke, on the subject. The letter included the following:

*I have been somewhat disturbed of late at the trend of relationships between the Headquarters of the various military forces of the Empire, and particularly between*

*ourselves and W.O<sup>10</sup>. These relationships were laid down originally at the Imperial Conference in 1909, and had been developed steadily until recent years. The pivot of all our relationships was the Imperial General Staff, and although this conception has tended to weaken, the results of its formation still remain, to the immense advantage of the whole of the forces of the Empire.*

*The main principles that have been enunciated under the aegis of the Imperial General Staff, and determined at various Imperial Conferences, have led to the development of the Empire land forces on identical lines. **The result is that throughout the Empire the Army has a common doctrine of war; a common system of organisation, both in relation to the command and staff system, and the organisation of units and formations; common principles and methods of training; and common equipment.*** Bold added (Long 1963).

With the fall of Singapore the vulnerability of Australia to invasion was made starkly apparent. The British Empire was no longer the dominant force in the world. Dependence on the military power of another country was seen as unacceptable but our size made self-sufficiency impractical. Pragmatically, our national security is best served through a network of alliances. The polarisation of the Cold War coupled with the withdrawal of the UK from east of Suez in the mid-sixties made for an easy strategic decision to complete the transfer from the UK to the US as the major Alliance partner under the ANZUS Treaty. That second epoch included the wars in Korea and Vietnam during which the three services of the Australian Defence Force operated as a component of the major power or coalition which provided most of the military power.

The third epoch opened with the Guam doctrine of US President Nixon after the Vietnam War and was a turning point in raising the level of discussion on the balance between dependence on Alliances, self-sufficiency and self-reliance. Sixty years on from the Singapore Shock, realistic planners accept that there is no single durable solution to the problem of defining Australia's military capabilities. Many factors combine to ensure that the outcome is a zone of best fit which from time to time will favour one of the determinants of defence capability, namely, self-reliance, major power alliances, economics, technology and geo-politics. In the current era of rapid change characterised by time constants that are less than the life-cycle of equipment and systems there may be less scope than is desirable for adjustment as circumstances change.

For a brief period from the Dibb Report in 1986 to the end of the Cold War, Australia pursued a policy of Self-reliance within the framework of Alliances. This included investment in industry capabilities primarily through the requirement for Australian Prime contractors on major projects such as the Submarines, Anzac Ships and JORN. The well-publicised failures in those mega-projects coupled with the rationalisation of defence industry world-wide in the aftermath of the collapse of the

---

<sup>10</sup> W.O. refers to the War Office established in the UK.

USSR has led to the current epoch in which equipment procurement and support contracts are placed on companies that are largely overseas owned.

Consequently, not only equipment and systems are overseas sourced, but the technologies embedded in them are developed overseas. In such an environment it is difficult to see that the Australian branches of UK, US and European defence companies are in a position to take a lead in Australia in research into the foundations of Network Science. Technology embedded in defence equipment and system procurements is developed in the countries of origin and underpinned by the research conducted in those countries.

The same is true of other advanced technology sectors of Australian secondary industry, such as communications, information technology, automobile and finance. One of the effects of Globalisation is the centralisation of research capabilities.

Given this condition of market failure it appears that for as long as the current regime of acquisition of military systems is maintained DSTO must continue as the main instrument for defence research in Australia. As a consequence it is our view that any program of research into Network Science as it relates to the Australian Defence Forces should be led by DSTO. The option of relying on overseas developments is not considered an adequate response to the challengers presented by Network Centric Warfare. This does not preclude participation by Australian Industry and Universities. This issue is discussed in the following section.

***Question 8: What areas of a Network Science should Industry participate in?***

As discussed in the previous section, Defence Industry in Australia has its capabilities driven by its major monopsonist customer and there is no reason to believe that this situation is about to change. The nature of the work performed in the defence industry has led to companies participating in the sector employing people with a range of skills suitable for the conduct of their current business. Since this business does not involve significant amounts of fundamental research into the situations in which their technical products are deployed, there has been no reason for the industry to develop expertise of a research capable kind to undertake research into an issue such as Network Science. This is in part because much of that work is performed on the government side of the acquisition relationship prior to the establishment of contracts to supply

It is to be expected that the Australian Defence Force will acquire systems and equipments that are network-capable. The NCW Roadmap mandates this capability. As has been the case with other technologies introduced into the country already, industry will be required to provide in-country maintenance and through-life support, including adaptation and modification. Industry capabilities to support that level of engagement are realised through the government policy of inwards technology transfer by participation in the procurement contract. This leaves little scope for industry participation in Australian basic research programs as a precursor to product and system development, manufacture and through-life support.

In the case of the impending across-the-board introduction of networking capability into the Australian military this established method of infiltrating technology into Australian Industry is not considered satisfactory. The networking capability cannot be acquired and fielded overnight. Its development will be paced by the timetable of acquisition of new and replacement systems. The risks associated with development of a capability over a number of years and via a plethora of equipments and systems sourced from a number of competing suppliers and selected by a suite of criteria including but not primarily networking capability, are very high.

The four defence communities comprising the:

- Military as the users;
- Defence Materiel Organisation (DMO) as the acquirers;
- Defence Science and Technology Organisation (DSTO) as the advisers, and

- Industry, as the suppliers

all need to engage in a program of learning what networking capability entails in the Australian context. The Australian military is in some aspects unique in that it is required to operate as a stand-alone force, as the leader in a multi-national force in our region of Direct Military Interest (DMI) and as a member of a coalition force anywhere in the world. The solutions to problems posed by net centricity differ for each of those operational scenarios. There are programs in the defence group that could fund, and collaborative agreements between DSTO industry and centres of excellence in universities that could implement concept demonstrator projects that would enable all parties to test and evaluate networking concepts.

While the extent to which the Australian implementation of Network Centric Operations will be indigenous remains to be determined, it is nevertheless critical that the defence agencies comprising the operators, acquirers and advisers are in a position to prepare effective performance specifications that are based on knowledge of what is useful, feasible, available, testable and affordable. Industry participation in the development, test and evaluation of that knowledge is also considered critical in establishing in-country ability to interpret defence's requirements and respond to them intelligently over a range of materiel acquisition projects spaced over an extended timescale.

# **Work Package 4**

## **Applications**

## Work package 4: Applications

### *Question 9: What role will a Network Science play in network-centric military operations?*

In addressing this question we are aware of the comprehensive report *The Network Centric Warrior: The Human Dimension of Network Centric Warfare*; DSTO-CR-0373 (Warne et al 2004). We do not propose to work over the ground covered in that report. We have elected to concentrate on an issue which seems to have had insufficient attention but which is critical to the exploitation of networking capability.

The war-fighting practices of the military, particularly those of the Army rest on centuries of combat experience. But the effectiveness of these practices may be under challenge in this post-Cold War era characterised by Operations Other Than War and now the need to deal with non-governmental trans-national terrorist networks. As they prepare for Network centric warfare (NCW) or Network enabled operations (NEO), a major issue that only the military can address is not so much the development and fielding of an integrated surveillance, reconnaissance and intelligence grid, a communications network and an information processing grid, but the basic decision at which point between the Political leader and the individual warfighter the transition from Directed control to Directive control takes place.

Under conditions of Directed Command and Control the Commander's intent is conveyed as "What" the military mission is to accomplish, as well as "How" the mission is to be conducted. Under such a regime the Commander is the only one where the intelligence appreciation of the battlefield has any relevance and the warfighters' have no alternative to following the Commander's orders. In fact in almost every military campaign or mission there has to be a transition from directed to directive control which allows the local commander some flexibility in "How" a mission is to be prosecuted. At all times those in immediate command of the warfighters have to reconcile the Commander's Intent with the Rules of Engagement, the preservation of a viable fighting force (in terms of personnel and equipment), the protection and evacuation of the wounded, avoidance of non-combatant casualties and resupply.

The vision that could be inferred from the early writings on NCW by the CCRP was that perfect knowledge of the battle space, communicated simultaneously and without corruption and delay to all field force units would lead them to independently arrive at a unanimous decision on an optimum plan of action, including weapons, timing and location. This vision

has echoes of the unfulfilled and unfulfillable promise of Artificial Intelligence and falls just short of promising that information that is complete and accurate, when perfectly processed and instantaneously transmitted without error to the cognitively perfect warfighters can lead to decisions that are guaranteed to result in synchronised action and successful outcomes without the need for a co-ordinating authority.

We know enough from the wealth of qualitative material on social and socio-technical systems that this is an unrealistic expectation currently and for the foreseeable future beyond the capability of technical systems.

Alberts et al in the CCRP publication *Understanding Information Warfare* (2001) described NCW as comprising the following three classes of hypotheses (page 59).

1. Hypotheses of the first class deal with the relationship between *information sharing*, *improved awareness*, and *shared awareness*;
2. Hypotheses in the second class include those that involve the relationship between *shared awareness* and *synchronisation*. For example, the effect of different degrees of *shared awareness* or *collaboration* on *synchronisation*;
3. The third class of hypotheses involves the link between *synchronisation* and *mission effectiveness*.

It may be that these are not strictly hypotheses as understood by the science community. Nevertheless they are a statement by the US military community that it had observed the effect of Information and Communications Technology on the international finance and commerce communities and their use of military terms such as defending a position, attacking a weak point, marshalling forces, strategic withdrawal, getting inside an adversaries' decision cycle, and raising the tempo of operations.

The proponents of NCW saw no reason why the US military could not similarly derive improved performance from the application of ICT. The inference that can be taken is that the hypotheses is that they encapsulate a belief that the advent of networked communications and information technology in the military domain would lead to enhanced mission effectiveness through the causal chain outlined in the hypotheses.

One role of the military is to participate in the processes that are converting the consequential requirements embodied in the three hypotheses into real systems that reliably produce the desired outcomes. The techniques of systems engineering may be appropriate in separating wishful thinking from achievable requirements and identifying and isolating areas of technical and social risk.

Later writings on NCW, NCO and NEO have moved away from the earlier simplistic technology-based vision. However the idea is very “sticky” and persists. One problem with the original vision of NCW based on the early CCRP documents and presentations is that it does not distinguish between the four domains discussed above, Physical, Information, Cognitive and Social. There is particular misunderstanding of the different character of events in the multiple domains as they depend on the status of the other domains. Weaver (1964) distinguished, in the case of electronic communication systems, this problem of domains by noting that the technical communication system has the role of transferring the signal from sending apparatus to receiver without corruption.

However, Weaver noted that the reproduction of the symbols conveying the message at the receiver is not evidence that the communication has been effective. What is needed is for those symbols to generate the same cognitive awareness in the person at the receiving end of the system and ultimately to lead to the implementation of the action that was intended by the sender at the time of formulation of the message. Although Weaver did not explain the processes of the transformations of the message between the domains he showed awareness of the different nature of those domains and the need for their integration to enable a communication system to be effective.

In participating in the development of NCW capability the military has a critical role in establishing the transition point in the chain of command from Directive to Directed control. Directive control (called Mission control by the UK Military and *Auftragstaktik* by the Germans) occurs when the Commander’s Intent is confined to “what is the required outcome of a particular mission”. The control is “Directed” when the Commander’s Intent includes “how the warfighters are to go about accomplishing the objectives of the mission”. Were the core NCW Systems Requirement realised then “Directive” control would be all that is necessary from the commander and all else would follow.

However unfettered Directive control opens up the opportunity for the inept or less able just as much as it does for the exceptionally brilliant field commander. Some Directed control must always be exercised by the Battle Group Commander.

There are also down-sides to extensive knowledge of the battle space. The first is that while it may be extensive, it can never be complete or accurate and may be in need of filtering. Insofar as the knowledge is incomplete it can also be misleading because in the omissions there may be anything ranging from the inconsequential to a significant opponent asset. An enemy can be expected to engage in deceptive practices and attempt to inject false information and may resort to attempts to block or impair the communication channel.

Another downside is that instant transmission of that knowledge to all levels of the command structure subjects the upper echelons to an irresistible inclination to interfere. Examples such as the personal engagement of President Johnson in the Vietnam War and the involvement of Secretary Rumsfeld in Iraq suggest that the development of networks with the intention of facilitating self-synchronisation may lead to the exact opposite, namely the application of real-time Directed control from the higher military command and the political level. While we may be trying to develop the Strategic Corporal we may instead be facilitating the emergence of the Tactical Prime Minister.

A third downside is that any increase in the volume of information available to commanders is certain to exacerbate the overload of their cognitive and working memory capacities, leading inevitably to their ignoring excess information. The decision making capabilities of commanders at all levels is a subject in need of research in its own right and may lead to advanced methods of presentation of information that are in effect a new language. This is a separate issue from that of encryption to protect information from being accessed by an enemy.

Keus (2005) seems to imply that the position of NATO is that the role of commander will be preserved in any practical implementation of NEO and from that we suggest that the choice of directed or directive control in any instance is made at that level. Above the commander, only directive control can be allowed, that is the “What” of the mission. Below the commander, some circumstances might require directed mission control, which dictates the “How” as well as the “What”. Other circumstances may call for directive control which establishes the “What” and allows the field force units to determine the “How”. Keus would also expect the Commander to assign the “Who”, which are the force units assigned to the particular mission.

As noted above, centuries of combat experience have confirmed Command as the principal mode of decision making by the military as this, supported by intensive repetitive training, ensures that personnel who are in harm’s way continue to function effectively. However, within the Headquarters the Commander may take advice from other senior subordinates, leading to some interactive decision-making prior to the construction and promulgation of the final decision. Yet it appears that decision making modes other than Command are needed to support anything resembling self-synchronisation. The NCW Roadmap provides no guidance on the view of the military on the interdependence of the decision making mode, leadership and the advanced Intelligence, Surveillance and Reconnaissance (IS&R) systems, the Information and Communications technology (ICT)

systems and the Human Interface (HI) systems foreshadowed under the banner of Network-Centric Warfare.

The answer to the question posed by this section is twofold:

1. If the Command mode of decision making is retained, the role of Network Science in military operations is mainly to support the implementation of the technical systems that provide the IS&R, the ICT and the HI capabilities. Those aspects of Network Science that deal with social systems and cognitive capabilities would have a role in supporting the decision maker in assimilating the information presented which is increased by some orders of magnitude as a result of the networked systems;
2. If decisions are made between field units that are not co-located, by any method that modifies the Command structure, the role of Network Science in the technical domain remains essentially the same as in (1) above. However the role of the aspects of Network Science that reside in the social domain that deals with purposeful collaborative human activities is considerably expanded.

The dilemma can be illustrated by reference to Figure 6 which shows a generalised representation of a network. Central to the realisation of the force multiplier effect of Networking is the Hub. This is the node or person that is connected to everything and everybody. The Hub and the Commander cannot be one and the same person as they have different roles. The Commander heads a structure of the Chain of Command through which authority over smaller and smaller operational units is devolved via standard operating procedures that have evolved over many years. The Hubs on the other hand have to be all over the network using their connections to analyse information and synthesise different configurations of the warfighter units to take advantage of opportunities as they present themselves. How the military trade off the roles of Commander and Hub is central to the exploitation of the power of networking.

***Question 10: What long-range research might be needed to implement network-centric operations, in particular for Australian military forces, in a framework of a Network Science?***

In response to the question posed by this section, we know enough from the social sciences to assist a Commander, exercising the Command mode of decision making, to determine if the units available for a particular mission can be trusted with directive control and may be capable of self-organisation or that they are not capable of self-organisation and may require directed control or at least, centralised co-ordination. But the knowledge is across several disciplines and multi-disciplinary collaborative research is required to establish a common body-of-knowledge. In the technical domain, research is required to determine and test concepts related to the equipment needed to support a changed mode of interaction of the parties.

A preliminary list of areas requiring long-range research to support the implementation of network-centric operations is as follows. Not all of these could be considered as elements of Network Science. However they are listed as issues that need to be addressed to support the development, acquisition and introduction into service of even the most basic level of networked IS&R, Communications, and Information Technology systems.

- Cognitive paralysis;
- Working memory overload;
- Formation of Transactive memory;
- Practice of Distributed Problem solving, collaborative decision making;
- Self organisation/self synchronisation;
- Quantitative measures meaning in relation to network effectiveness;
- Leadership and Directive Command and Control;
- The role of Hubs in relation to that of the Commander;
- Network formation and maintenance;
- Failure proofing, information security and interference protection;
- Multi-national network enabled operations;
- Identification and development of Connectors, Knowledge Brokers and Salespersons in a military environment.

This is a preliminary list which indicates the range of areas in need of long range research to support the advent of Network Centric Warfare capability into the Australian military.

## Bibliography

1. Ager, J. N. (2000). Is there a Military Utility to Information Operations? Defense Analysis **16**(3): 277-298.
2. Alberts, D. S. and Czerwinski, T. J. Eds. (1997). Complexity, Global Politics, and National Security. DoD C4ISR Cooperative Research Program. (CCRP) Washington DC, Institute for National Strategic Studies.
3. Alberts, D. S., Garstka, J. J. et al. (2002). Understanding Information Age Warfare. DoD CCRP. Washington DC, Institute for National Strategic Studies.
4. Alberts, D. S., Garstka J. J., et al. (2002). Network Centric Warfare; Developing and Leveraging Information Superiority. CCRP. Washington DC, Institute for National Strategic Studies.
5. Bak, P. (1996). How Nature Works; The Science of Self-organised Criticality. New York, Copernicus Press.
6. Barabasi, A.-L. (2002). LINKED: The New Science of Networks, Perseus Publishing, Cambridge MA.
7. Belbin, M. (1996). Team Roles at Work. Oxford UK, Butterworth-Heinemann.
8. Borgatti, S. P. and P. C. Foster (2002). The Network Paradigm in Organisational Research: A Review and Typology. Journal of Management **29**(6): 991-1013.
9. Bourdieu, P. (1986). The Forms of Capital. Handbook of Theory and Research for the Sociology of Education. J. G. Richardson. New York, Greenwood Press: 241-258.
10. Capra, F. (1997). The Web of Life. London, Harper Collins.
11. Capra, F. (2003). The Hidden Connections, Harper Collins, London.
12. Checkland, P. and Holwell, S. (1998). Information, Systems and Information Systems. Chichester (UK), John Wiley & Sons Ltd.
13. Cohen, D. and Prusak, L. (2001). In Good Company; how social capital makes organisations work. Boston, Harvard Business School Press.
14. The Concise Oxford Dictionary of Current English, 6<sup>th</sup> ed., Oxford. UK, Oxford University Press.
15. Cropley, D. H. and Cropley, A. J. (2000). Creativity and Innovation in the Systems Engineering Process. Proceedings of the INCOSE 2000, Conference,

Systems Engineering: A Decade of Progress and a New Century of Opportunity, Minneapolis, Minnesota, USA, INCOSE.

16. Cropley, D. H., Sproles, N. and Cook, S. C. (2005). The Science of Command and Control (C2). Journal of Battlefield Technology **8**(1): pages15-24.
17. Director General Capability and Plans (2005). NCW Roadmap, Defence Publishing Service, Canberra ACT.
18. Eldridge, N. and Gould, S. J. (1972). Punctuated Equilibria: An Alternative to Phyletic Gradualism. Models in Paleobiology. T. J. M. Schopf. San Francisco, California, Freeman, Cooper & Company.: 82-115.
19. Gardner, H. (2004). Intelligence in Seven Steps. Seattle USA, New Horizons for Learning.
20. Garstka, J. and Alberts, D. (2004). Network Centric Operations Conceptual Framework Version 2.0. Washington, D.C., DoD Command and Control Research Program.
21. Gladwell, M. (2000). The Tipping Point; How Little Things can make a Big Difference. London UK, ABACUS.
22. Gribben, J. (2004). Deep Simplicity, Penguin Books, UK.
23. Hutchins, E. (1995). Cognition in the Wild, MIT Press Cambridge Massachusetts.
24. National Research Council (2005). Network Science. Washington, D.C., Committee on Network Science for Future Army Applications. <http://www.nap.edu/catalog/11516.html>
25. Illeris, K. (2002). The Three Dimensions of Learning, Roskilde University Press, Denmark.
26. Janis, I. L. (1972). Victims of Groupthink. Boston USA, Houghton Mifflin Company.
27. Johnstone S., Goestelow, P., and Jones, E., (1999), Engineering and Society: An Australian Perspective, 2<sup>nd</sup> Edition, Longman, ISBN 0 582 811716.
28. Keus, H. E. (2005). NETFORCE PRINCIPLES An Elementary Foundation of NEO and NCO. 10th CCRT Symposium, McLean, Virginia.
29. Kolb, D. A. (1984). Experiential Learning: Experience as the Source of Learning and Development, Englewood Cliffs, NJ: Prentice Hall.
30. Kuhn, T. S. (1996). The Structure of Scientific Revolutions. Chicago USA, University of Chicago Press.

31. Lave, J. and Wenger, E. (1999). Situated Learning, Legitimate Peripheral Participation. Cambridge UK, Cambridge University Press.
32. Long, G. (1963). Australia in the War of 1939-1945; The Final Campaigns, Australian War Memorial, Canberra.
33. Maxfield, R. R. (1997). Complexity and Organisation Management. Complexity, Global Politics and National Security. D. S. Alberts and T. J. Czerwinski. Washington DC, Institute for National Strategic Studies: 171-218.
34. Merriam, S. B. & Caffarella, R. S. (1999) Learning in Adulthood, A Comprehensive Guide, Jossey-Bass, San Francisco.
35. National Audits Office, U. K. (2005). Driving the Successful delivery of Major Projects [www.naodefencevmf.org](http://www.naodefencevmf.org), MOD (UK).
36. Polanyi, M. (1968). Life's Irreducible Structures. Science **160**: 1308-1311.
37. Polk, R. B. (2000). A Critique of the Boyd Theory-Is it Relevant to the Army? Defense Analysis 16(3): 257-276.
38. Prigogine, I. and I. Stengers (1984). Order out of Chaos. London UK, Heinemann.
39. Putnam, R. D. (2000). Bowling Alone; The Collapse and Revival of American Community. New York, Simon & Schuster.
40. Reichtin, E. (1991). Systems Architecting; Creating and Building Complex Systems. Englewood Cliffs, NJ, Prentice Hall.
41. Roland, J. (1958) On "knowing how" and "knowing that". The philosophical review, 67, 379-388.
42. Senge, P. M. (1990). The Fifth Discipline. Milson's Point NSW., Random House Australia.
43. Spinuzzi, C. (2003) Tracing genres through organizations a sociocultural approach to information design, Cambridge, Massachusetts, The MIT Press.
44. The Standish Group (1995). Chaos: A Recipe for Success, The Standish Group.
45. Tuckman, B. W. (1965). Developmental Sequence in Small Groups. Psychological Bulletin **63**(6): 384-399.
46. Wenger, E. (1998). Communities of Practice, Learning, Meaning and Identity. Cambridge UK. Cambridge University Press.
47. Vygotsky, L. (1978). Mind in Society: The Development of Higher Psychological Processes, Harvard University Press.

48. Warne, L., Ali, I., Bopping, D., Hart, D., Pascoe, C., (2004) The Network Centric Warrior: The Human Dimension of Network Centric Warfare. DSTO-CR-0373.
49. Weaver, W. (1964) Recent contributions to the mathematical theory of communication. In Shannon, C. E. & Weaver, W. (Eds.) The mathematical theory of communication. Urbana, Illinois, The University of Illinois Press.
50. Wuthnow, R. (1994). Sharing the Journey: Support Groups and America's New Quest for Community. New York. Free Press.

## GLOSSARY

**Action-Learning Cycle:** A graphical representation by Kolb (1984) of the process of learning through experience; the four phases are Observe, Reflect, Plan, Act. A fifth phase, Decide, is implicit; see also OODA Loop.

**ANZUS:** The ANZUS Alliance initially a mutual defence alliance between Australia, New Zealand and the United States. New Zealand was effectively excluded following its refusal to grant entry by US warships that might have been carrying nuclear weapons.

**Capital, Forms of:** Five forms of capital were enunciated by Pierre Bourdieu (1986) as present in societies and operative in determining their characteristic culture. They are Embodied, Social, Institutionalised, Objectified and Economic.

**CCRP:** Acronym for The Command and Control Research Program, established by the US DoD with the mission of improving DoD's understanding of the Information Age; The CCRP publications are a source of information on the development of Network Centric Warfare Capability in the US Military.

**Chunks:** A sign of experienced practitioners is that their long term memories are organised into chunks characterised by associative linkages; Identified by Miller (1956) as a way by which an expert escapes from the limitations of cognitive channel capacity; Kline (1995) estimates that an expert will command 50,000 to 60,000 chunks; Also called Schemata.

**Cluster:** A network of a limited number of nodes, between 8 and 15, with strong links between all elements; also applied to teams or small groups. Also called "sympathy group" by psychologists (Gladwell p 177)

**Clustering Coefficient:** The ratio of the actual numbers of links in a network to the maximum number possible, given by  $N(N-1) \div 2$  where N is the number of nodes or members in the network; Attributed to Watts and Strogatz cited in Barabasi (p 46); Kauffman (cited in Gribben p165) indicates that a collection of individuals undergo a phase transition to a network when the clustering coefficient equals 0.5.

**Co-evolution:** (Maxfield 1997) A large part of the environment in which agents (nodes) exist consists of interactions with other agents, who themselves are adapting and evolving. The emergent properties from a network in which the agents are in a state of continuous evolution are also going to be evolving. Interdependence is a term applied to agents whose characteristics at any given moment are dependent on those they are connected to.

**Collective Learning:** A term applied by Illeris (2002) when the members of a team form and commit to their transactive memory, an enduring agreement on the meaning of a package of information and the context of its application; similar to Senge's concept of the Learning Organisation (1990).

**Connector:** The term applied by Gladwell in "The Tipping Point" to the node that has many times more links to other nodes than average; taken as applying to people in social networks. Connectors collect people.

**Degrees of Separation:** The number of links separating any node from any other node; in the late 1960s Stanley Milgram conducted the experiment that is sometimes taken as demonstrating that every person is connected to any other person by an average of six links. Milgram's experiment showed "that a very small number of people are linked to everyone else in a few steps, and the rest of us are linked to the world through those special few". (Gladwell page 37)

**Distributed Intelligence:** The capability demonstrated by a group or team to exploit their transactive memory in order to jointly make sense of the information under consideration, place it in a context and agree on the response. (Gardner 2004)

**Distributed Cognition:** Interchangeable with Distributed Intelligence; term used by Hutchins and Klausen (2000).

**Emotional Intelligence:** There seem to be two meanings to this term used by Goleman (1996). The first is that the human mind retains not only the factual information associated with an event but also the emotional response of the person to that event. A recurrence of that event or similar will activate both classes of memory and the person's response will be determined by both. An extreme response is the fight or flight reflex. The second relates to empathy, which is the ability to discern the emotional state of other people and manage interactions accordingly.

**Hub:** Special case of Connector; a node that by virtue of a very large number of links, is a recognised member of a number of clusters; can be taken as applying to technical networks, e.g. the Internet.

**Interdependence:** See Co-evolution.

**Inverse Power Law:** The expression of the relationship between the magnitude of a parameter and its frequency of occurrence.

**Knowledge, Forms of:** According to Illeris (2002), the way people internalise knowledge depends on prior learning and may be *Assimilative*, *Cumulative*, or *Accommodative*.

**Link:** The term denoting the connections between nodes of a network.

**Maven:** A Yiddish word that means one who accumulates knowledge; applied by Gladwell to the people in social networks who collect and broker information.

**Miller's Number:** George Miller (1956) hypothesised that the cognitive channel capacity of humans was  $7 \pm 2$ . His analysis of several sets of data did not support the hypothesis. However the notion has stuck and led to the widespread use of Miller's Number to explain cognitive overload. His greater contribution is his finding that "chunking" explains the capability of experts to extend their cognitive capacity beyond that of beginners (Baddeley 1994).

**Network:** An arrangement of distinct elements that interact to generate emergent properties that are different from the properties of any of the elements.

**Node:** The general term applied to elements in a network.

**OODA Loop:** A graphical representation by Captain Byrd of the USAF of the phases of acquisition and engagement of a target; four phases are Observe, Orient, Decide, Act; similar to the Kolb Action-Learning cycle without a Reflection phase.

**Phase Transition:** The rapid change of an entity from one state to another with different properties from the previous state. (Gribben p 164)

**Punctuated Equilibrium:** The name (attributed initially to Eldridge and Gould in the field of Paleobiology) to a phase transition episode; suggestive of the transition from one stable state to another different stable state.

**Salesperson:** The term applied by Gladwell to the people who have the ability to persuade others to accept new ideas.

**Schemata:** See chunks.

**Self-organising Criticality:** A necessary precondition for an organisation faced with change to make the phase transition to a new state that accommodates the new environment; believed to occur when the dormant links in a network become active and drive the organisation to a new structure or state.

**Social Channel Capacity:** The characteristic of humans in a social setting that limits to around 150 the number of people with whom humans can have a genuine relationship. (Dunbar cited in Gladwell p 179)

**Structure and Process:** A composite term referring to the explicit arrangements by which an organisation is managed.

**Sympathy Group:** See Cluster.

**Tacit Knowledge:** a term applied by Polanyi to the knowledge people have that they don't know they have; contrasted with explicit knowledge; estimated by Takeuchi to comprise up to 80% of the knowledge required to manage an organisation successfully.

**Transactive Memory:** A key indicator of a well-formed group in which each member is responsible for knowing the details of a portion of the total knowledge base of the group. Each member knows the "table of contents" of the knowledge base, where the details reside, and the details for which each member is responsible; Collective Learning is a precursor of Transactive Memory which is in turn a precursor of Distributed Intelligence (Wegner, D. M. 1987).