

Information sharing and gathering in NCW environment: voices from the battlespace.

Irena Ali – Defence Science and Technology Organisation, Defence Systems Analysis Division, Department of Defence, Fernhill, Canberra ACT 2600, Australia.

Email: irena.ali@dsto.defence.gov.au

Ph: 61 2 62566252

**Topic: Social Domain Issues
Cognitive Domain Issues**

Abstract

Increasingly, literature on network centric warfare (NCW) focuses on human behaviour within a networked environment. Therefore, the implementation of NCW must look beyond the acquisition of technical enablers to individual and organisational behaviour emphasising the importance of the ‘networker’ over the ‘network’. The paper reports on a study spanning over two years with the aim of providing insights of what contemporary trends in warfighting, primarily NCW, mean for Australian Defence Force (ADF) personnel - how they will operate, make decisions, and interact with others. The research involved in depth interviews with a representative sample (over one hundred interviews) of the defence personnel who had been deployed in the Middle East. More specifically, this paper focuses on how people gather and share information in high uncertainty and high tempo environments. The research data clearly indicates that the willingness to collaborate and the interconnectedness of robust human networks were the necessary ingredients for building up situational awareness, achieving agility and, ultimately, securing successful mission outcomes.

1. Introduction

In the foreword to *The Implementation of Network-Centric Warfare (2005)*, the Director of the US Force Transformation stated that warfare is about human behaviour, in a context of organised violence, directed toward political ends. In the same vein, network-centric warfare (NCW) is about human behaviour within a networked environment. “The network” is a noun representing information technology, and can only be an enabler. “To network” is the verb, the human behaviour, the action, and the main focus. Therefore, implementation of NCW must look beyond the acquisition of technical enablers and capabilities to individual and organisational behaviour, such as organisational structure, processes, tactics, education and training, and the way choices and decisions are made.

Similarly, in his recent speech on Australia’s Defence Capabilities Priorities, Lieutenant General David Hurley highlighted an interesting point on NCW arising from a workshop that CDG conducted in early August 2005 on the human dimension of NCW—the emergence of the importance of the ‘networker’ over the ‘network’, and thus the introduction of the concepts of ‘Networker Centric Warfare’ and the ‘Networker at War’”. General Hurley further stated “Nothing brand new here but...the possibility it offers to transfer our consideration of capability from technology-centric to people-centric warrants further work” (Hurley, 2005).

Recent literature (Alberts & Hayes 2003; Alberts, 2005; *The Implementation of Network-Centric Warfare*, 2005) and discussions on NCW refer to four tenets, all-starting with the concept of a robustly networked force:

- A robustly networked force leads to increased information sharing.
- Increased information sharing enhances not only the quality of information but encourages collaboration and increases shared awareness.
- Increased collaboration and shared awareness enables self-synchronisation.
- All of that together dramatically improves mission effectiveness and ability.

These four tenets serve to define a value chain that links the full spectrum of material and non-material investments to operational effectiveness and agility. These are important NCW principles; however, one major element appears to be neglected from these, the human element. Although the human is the key element, the focus seems to be on hardware, bandwidth, and electronics. Even assuming that the information flows freely between and across all force elements, the challenge remains as to how human beings share, absorb, and understand the available information, and subsequently make decisions based on that information.

2. Research study and methods

The aim of DSTO research study *The Human Dimension of Future Warfighting* was to investigate, from an ADF perspective, the human dimension of NCW. Three key research questions were posed:

1. How do ADF personnel make sense of an NCW environment?
2. How does that understanding affect their behaviours?
3. What are the implications of this with respect to the ADF's planned transition to a seamless NCW force?

This final question opened the way for a range of issues to be explored including the ADF's preparation and training regimes, command and control arrangements and interoperability with other nations.

The study began with a review of the literature concerning NCW and future warfighting. Thereafter, the researchers undertook a series of in-depth interviews with ADF personnel returned from deployment to the Middle Eastern Area of Operation (MEAO) since the Coalition invasion of Iraq in March 2003. The interviews were conducted with a purposive but representative sample of ADF personnel with MEAO experience. The interview schedule was largely based on future-warfighting issues prevalent in the current NCW literature. In total a hundred interviews were conducted which were recorded, transcribed and coded. A qualitative software package, NVivo, was used to analyse the data.

Although each of the interviewee related their own experiences, there were a number of common themes emerging. This paper focuses on one of these themes and addresses how people gather and share, information as well as the issues concerning information management in high uncertainty and high tempo environments.

3. Information gathering and sharing

Whether by design or necessity, humans tend to collaborate to achieve set goals. Looking back in history, many significant developments resulted from group activity and sharing of know-how. In fact, this sharing of information and knowledge, and the willingness to cooperate, are the key elements for innovation and advancement. Warfare is no different from other endeavours.

The research data clearly indicates that the willingness to collaborate and the interconnectedness of robust human networks were some of the necessary ingredients for building up situational awareness, achieving agility and, ultimately, securing successful mission outcomes. This person to person networking allowed for the linking of ideas and resources, seeking and sharing information and, overall, it played an important role in almost every aspect of deployment. It can be easily said that there is nothing new about personal networking. However, as the complexity of circumstances increases and as the environment of uncertainty prevails, the need for informal networking seems to increase. Networking was seen by many of the study participants as a conscious alternative to often obstructive or protracted bureaucracy or processes. Networking not only expanded each person's matrix of connections but it often eliminated the passing on of responsibilities and frequently led to decentralised and speedier decision making.

3.3 Trust and information sharing and gathering

Many factors underpin cooperation between individuals and groups in work settings. During the interview program, our participants were asked to identify those that were critical to Australian-US cooperation. One of the most frequently mentioned factors was "trust".

An important outcome of networking is trust building, a characteristic that was identified by most study participants as an essential factor for any future operations and information sharing. People spoke about trust as the glue that kept human networks and interconnections aligned and was also seen as an underlying foundation for collaboration:

...rapport and trust, especially trust, is completely essential.

...you also very quickly build up a rapport with people, and if you can build up a rapport very quickly and get to know them and they get to trust you and you trust them, it becomes a lot easier.

...it was in our best interest both professionally, socially and militarily to mix as much as we could. I think we were much better off for doing so.

Trust may be associated with pragmatic characteristics such as communication, openness, commitment, and transparency (i.e. competence-based trust), or it may be equated with traditional qualities such as integrity, truthfulness, a proven track record, and not ridiculing others if they do not know something (i.e. benevolence-based trust)(Cross & Parker, 2004):

When you task someone to do a job, you have to know - well, you have to trust that he can do the job and the job gets done properly...you'd also follow up to see that it is, but, yeah, if you can't trust people in an environment like that, it's a very sad environment.

We trusted each other implicitly in everything and that was a good feeling. You knew that if you could not make a deadline or you could not be in a place at a certain time you knew that your offsider would be there to help you out and to do it. So, that was without even saying anything, you just knew that they would be there to back you up. The feeling of trust was awesome. I think trust or teamwork was probably the first one...

Trust is one of these commodities that cannot be taken for granted. It requires time and effort to cultivate, and as one of our interviewees put it, *trust - very hard to build up, and very easy to destroy*. Interpersonal trust is elusive; however, developing relationships on a personal and professional level helped generate trust. Often, rank, position, service or force affiliation, and perceived expectations created barriers that prevented the development of trust and subsequently, the sharing of information.

Almost all our interviewees said that breaking those barriers and establishing a personal connection was crucial for a productive relationship and trust building. Discovering non-work related commonalities allowed them to relate to each other on more than an instrumental basis. Socialising was perceived as a vehicle for developing wider networks, and therefore it enabled people to get to know each other. Getting to know each other and establishing rapport were seen as vital steps in building a team, building external relationships, and in achieving set goals. As team-members got to know each other they become aware of each other's strengths and weaknesses, what they could or could not do, their expertise and experience. People used various ways and means to develop these connections and networks and they all pointed out that it paid dividends in promoting interpersonal trust and paved a way for subsequent information and resource sharing:

I mean, even with the little bit of rapport that we had, the results were astounding - the things they were willing to do for us, just so we would give them a stuffed koala! ... The socialisation did contribute a lot to the success of our mission.

...you take time out of your really incredibly hectic day to sort of spend some time with them and just sit down quietly and just sort of talk about the work and whatever else. And you have things set up for them, you know, little things like you make up a little name plate made out of paper. Just sort of say, "You're a part of this team here. We value you". And when parcels come in you share the goodies around. You don't hoard it. These are very small examples. But together they build that jigsaw of trust and responsibility.

So I'd go up and have a chat with them and then I'd find out more of what they did. So when the boss would come up and say, "Look, you know, we need to know - find out about this and this", "Yeah, I know this guy", and it was networking a lot of it, and although at the start you wouldn't know why they would be important to you, but as the job progressed on...

Since trust was built upon close personal relationships, events that disrupted these relationships (for instance, personnel rotation) undermined the benefits to interoperability that trust provided. As illustrated in the following account, such events brought about periods of trust-rebuilding:

We didn't want to upset our host nation, if you like, so any dealings we had were just very formal until - and once they get to know someone they sort of only want to deal with that particular person, because that was the person that they trust. But when - if you've been rotated or something well then - the next person has to sort of build up that rapport again.

This resonates with other research examining the impact of personnel rotation. For example, Warne, Ali and Pascoe (2003) argue that the rotation of Headquarters staff brought about by posting cycles impedes the development and maintenance of Headquarters corporate knowledge.

3.3 Relationships and information sharing

In the literature review on the network centric warrior, Warne et al, (2004) point out that information sharing lies at the core of NCW. Information sharing enhances quality of information and shared situational understanding. Atkinson and Moffat (2005) further state that sharing of information is based on trust developed through social interaction, shared values, and beliefs. A human is a node in such interactions and a link is a bond that people develop which is based on mutual trust. Therefore, a significant component of a person's information environment consists of the relationships he or she can tap into for various informational needs. Sharing of information has a behavioural component and the emphasis is usually on one-to-one networking initiative and effort. It requires time and space (physical, cognitive and social) to develop the sense of safety and trust that is needed for information sharing. These informal networks usually developed in order to produce 'action' where formal processes were not agile enough for it to occur. The Australian contingent, very early in their deployment, realised that unless they fostered a good relationship, particularly with the Americans, they could not assume that the necessary information would be made available to them:

Without the trust and interaction, on a social level, where they were happy to have a joke with us and establish something like what we would call "mateship", where they were happy [to] respond to any requests we might make, it would have been much more difficult.

It is still about building a relationship, I think, because to get something out of someone that they do not necessarily want to give up, then it is all about them knowing and trust and liking and thinking there is going to be a mutual benefit out of it.

Conversely, it was also pointed out that a lack of networking skills was detrimental to effective operations:

There are so many military people that miss opportunities to either get the job done or to be able to achieve things, because they don't know how to ask in either the right tone or the right words to communicate with the person they need help from. And they aren't either humble enough or aren't assertive enough to ask and it really depends on who you're asking and what you're asking for, and a timeliness of when you're asking for it. And you've got to give that person a reason why they should help you. So, you've got to look at their position and what their needs are. So, take yourself out of your shoes, there's no military training for that. In the military we tend to go, "This is what I want and now you will give it to me". That doesn't work.

The issue of sharing classified information across national boundaries was a problem not only for the Australians but also for other coalition members. Therefore, the benefits of robust connectivity and access to a wide spectrum of databases were often bound by goodwill and personal relationships.

3.4 Coalition access to information

The lack of easy access to information for coalition partners was an issue for most of our interviewees and often they pointed out that their operational effectiveness, and at times their safety, was compromised as a result of that:

...at the least it's got to be releasable in Australia, Great Britain, Canada, but this affects an area where the Bangladeshi's are working with the Danes and the Poles, so it's got to be releasable to them too. There's no point in having this intelligence if we can't tell the folks that it affects...

This lack of formal sharing of information and transparency was also recognised by the US commanders. Rear Admiral Thomas Zelibor at the Technet International 2005 Conference in Washington in May 2005 pointed out that network centric warfare is at a crossroads. That crossroads is satisfying the need to know, the need to share, and the right to know in a culture that always has hesitated to reveal too much to too many. Sharing of knowledge is necessary if all entities are to work together as a team, he said, and that applies not just to inter-service communications; it's also necessary to keep international allies in the loop. "Recent history has shown us that when America finds itself in a street fight, England and Australia are with us like our older brothers when we were young kids, and I contend that they have a right to know, and we need to make sure that we keep them in the loop on all our decision-making processes. Ultimately, it is leadership and culture that will determine the success of network centric warfare at the strategic level" (Zelibor, 2005). The recently announced upgrade of Australia's security clearance with the US should hopefully address this issue (The Australian, 2005).

4 Information sharing and technological infrastructure

As pointed out earlier, trust is an essential underlying element to successful information sharing. However, another critical factor for information sharing and exchange is the presence of effective and appropriately robust, secure communication channels. The interview data suggests that the availability of reliable communication networks varied quite considerably throughout deployments.

Apart from the lack of secure communication links, another problem that the Australian contingent had to overcome was the issue of incompatible technology. This was seen as a considerable impediment for information gathering and sharing particularly with the coalition partners.

Technologically they could not talk to each other because they were not compatible ...

The pressures of keeping up situational awareness means that access to information should be constant. Some units felt disadvantaged because, due to technological deficiencies or outdated equipment and the lack of adequate bandwidth, they struggled to keep on top of up-to-date

information. Because of these limitations they were unable to understand much beyond their own picture of the battlespace.

Instead of talking on a radio you're doing it on chat. The problem with that is that the Americans do everything on chat and ... we cannot be on chat all the time.

What I meant was that you had to type something, send it out, save it on a floppy disk, give it to one guy, send that out. Put it on another floppy disk and send it out again, or have two people - two or three people duplicating the same information.

In addition, due to the lack of connectivity and thus access to information, staff had to walk quite a distance to other units where they could get the required information. Taking into account often extreme weather conditions and the time required to cover the distance, these people felt considerably disadvantaged:

...there was no connectivity ... there were no lines, there was nothing, right? So my guys to get intelligence updates had to walk across physically several times a day in very hot weather, above everything else, and ask the Americans to tell them.

So, whilst it's a small distance it's actually a long way to go every time you want information. It sounds funny but it is, you know - because you've got to go in through a series of barriers, gates and fences and tents... if you go in and you talk to someone and then potentially get the information you need and you've got to walk all the way back down.

5 Information management

NCW is about deriving combat power from distributed interacting entities with significantly improved access to information (Alberts et al, 1999). This can only occur through effective information sharing. Information sharing succeeds when the right information is provided to the right people at the right time and place. Effective sharing of information requires an information management policy and data management strategies.

Information management (IM) is typically defined as “the planning, budgeting, manipulating, and controlling of information throughout its lifecycle” (Office of Management and Budget, 2000). It may be understood as “a set of intentional activities which maximise the value of information in support of the objectives of the enterprise” (Linderman et al, 2005). These activities control information, from creation, through dissemination and use, to final disposal. Many of these activities are also referred to as: data management, records management, content management.

The purpose of an information management strategy or plan is to improve participants' ability to find the data they need and to understand that data when they receive it. Data and information must be visible, accessible, understandable, trusted, interoperable, and made available in response to user needs. Moreover, the individuals or units must be able to obtain all the data/information needed and be able to retrieve that information repeatedly for verification (Renner, 2005).

Our interviewees were very critical of information management practices during some deployments as illustrated by the following quote:

Unfortunately there was no data base and there was no information. So, you know, that was one of my biggest bugbears was there was no really useable data base. I had to develop my own data base over there just to store my information and to be able to see it.

This led to frustration and difficulties in the verification of information. Many of the interviewees said that once they saw a presentation or a report at some of the briefings it was almost impossible to find it again and go over the details, unless they were able save it on their own database system. Taking into account that the network-centric environment is characterised by a large number of participants and a plethora of information, the need for management of all information resources is crucial as overall advantage and agility over the adversary will come from readily available information and knowledge.

Renner (2005) describes an effective IM for a network-centric environment as having the four key elements:

- A body that exercises authority over data, i.e. what data must be collected and made available, how it should be represented and stored, quality/accuracy of data or information, how it will be validated and maintained.
- Shared information spaces – collection of data/information intended to suit the needs of different groups of information consumers. The defining aspects of the information space are data content and governance processes: who posts what to the information space, validation of who can be a consumer of the available information, and how the data should be organised.
- Common vocabularies – shared understanding of terms used and what the data means, for instance, simple dictionaries to keep consistency and aid understanding.
- Implementation infrastructure – information systems operated by data/information producers and consumers, i.e. interoperability.

Since NCW places an additional demand on information storage and retrieval, it is of paramount importance that the information needs of various consumers will be addressed and the policies are in place long before operations begin.

6 Summary

It is generally believed that the human aspect of current and future warfare is the least understood and researched domain of NCW. In recent years, there seems to have been a shift in emphasis from “the network” indicating the information technology, to a “networker” or “to network” representing the human behaviour, the action, which should be the main focus.

- The research data clearly indicates that willingness to collaborate and the interconnectedness of robust human networks were necessary ingredients for building up situational awareness, resource and information sharing, achieving agility and, ultimately, securing successful mission outcomes. Trust was seen as the glue that kept human networks and interconnections aligned and was also seen as an underlying foundation for collaboration
- The issue of sharing classified information across national boundaries was a problem for coalition members. Furthermore, the benefits of robust connectivity were largely dependant on goodwill and on fostering personal relationships.
- The availability of secure communication networks varied quite considerably throughout deployments. Furthermore, incompatible technology was seen as an impediment for information gathering and sharing.

- The lack of information management policies led to frustration and difficulties in access and verification of information.
- Better recognition needs to be given to the role of informal networks in operational situations and joint exercises and training whether at the Service or coalition level. International exchange programs would pave the way to relationship and trust building amongst the warriors who may, in the future, find themselves working together.

Further research should be undertaken into the potential application of electronic techniques for supporting relationship building and social interaction (e.g. virtual communities) as a means of encouraging the development of informal links and relationships between personnel from across the ADF and, possibly, appropriate international forces as well.

Combat power, to a large degree depends on the availability of information which is easily accessible, trusted, visible, interoperable and made available in response to user's needs. There is a need for information management policies that will ensure the authority over data/information, access rights, vocabulary/nomenclature standards, and technological interoperability.

7 Bibliography

Alberts, J. Gartzstka, and F. Stein, (1999) *Network Centric Warfare: Developing and Leveraging, Information Superiority*, 2nd ed., CCRP Publication Series.http://www.dodccrp.org/publications/pdf/Alberts_NCW.pdf

Alberts, David & Hayes, Richard (2003) *Power to the Edge*, CCRP Publication Series, http://www.dodccrp.org/publications/pdf/Alberts_Power.pdf

Alberts, David (March 2005), *Network centric warfare panel*, National Press Club, Washington, <http://www.af.mil/news/story.asp?storyID=123010127>

Atkinson, Simon Reay and James Moffat. (2005) *The Agile Organization*. Washington, DC: CCRP Publication Series.

The Australian, 5 Sep 2005

Cross & Parker,(2004) “*The hidden power of social networks*” Harvard Business School Publishing Corporation, Boston.

Hurley, D. (2005) “*Australia’s Defence Capabilities Priorities-Lieutenant General David Hurley*”, ASPI Series Lunch Address, Thursday, 11 August 2005, Boathouse, Canberra.

Linderman, J. Brichacek, S. Haines, D. Ouellet, B. Siegel, G. Chase, and J. O’May (2005), “A Reference Model for Information Management to Support Coalition Information Sharing Needs”, in *Proc. 10th Int. Command and Control Research and Technology Symposium (ICCRTS)*, McLean, VA, June 2005.

Office of Management and Budget, *Circular A-130: Management of Information Resources*, Nov. 2000. <http://www.whitehouse.gov/omb/circulars/a130/a130trans4.pdf>

Renner, Scott (2005) *Net-Centric Information Management*, The MITRE Corporation, sar@mitre.org <http://www.dodccrp.org/events/2005/10th/CD/papers/348.pdf>

The Implementation of Network-Centric Warfare (January 5, 2005), Force Transformation, Office of the Secretary of Defense, 1000 Defense Pentagon, Washington, DC 20301-1000, http://www.ofc.osd.mil/library/library_files/document_387_NCW_Book_LowRes.pdf

Warne, L. Ali, I. Pascoe, C. (2003) *"Social Learning and Knowledge Management - A Journey through the Australian Defence Organisation: the final report of the Enterprise Social Learning Architectures Task"*, DSTO RR 0257 AR 012 854, Defence Systems Analysis Division, DSTO Information Sciences Laboratories, South Australia.

Warne, Leoni. Ali, Irena, Bopping, Derek, Hart, Dennis Pascoe, Celina (2004) *"The network centric warrior: the human dimension of network centric warfare"*, DSTO Report CR-0373, AR-013-158, DSTO Information Science Laboratory, Edinburgh, SA.

Zelibor, Thomas(17 May, 2005), "Networkcentric warfare streamlines the warfighting process at the operational level" Rear Adm. Thomas Zelibor, the director of global operations for U.S. Strategic Command Navy, Technet International 2005 Conference, Washington, May 17, 2005. American Forces Information Service, News articles http://www.defenselink.mil/news/May2005/20050518_1208.html