

Presentation by Trevor J Thomas,  
Managing Director, Business Communications Group and  
Editor-in-Chief, Australian Defence Business Review (ADBR) magazine to:

## NETWORK CENTRIC WARFARE 2004

Australian Defence Force Academy, Canberra, 24 November 2004

### A practical view on building Australia's NCW capability

**IQPC By-line:** Australia's top defence-industry commentator will ask both the hard questions and answer them, in terms of the infrastructure required to support a whole-of-government approach to effectively leveraging NCW by Australia's military commanders and executive government decision-makers. The presentation will begin with a review of the ability of Defence's own IT infrastructure to support the coming NCW model, and concludes with observations of the adequacy of connectivity across broader government in the task of ensuring that Defence's own investment in NCW can be made the most effective.

**Introduction:** Good afternoon ladies and gentleman. My name is Trevor J Thomas, and for those who are not already familiar with my ramblings, I am the Editor-in-Chief of Australian Defence Business Review (ADBR) magazine. This monthly publication covers the broad range of influences upon governmental decision-making in regard to what equipments and systems the Australian Defence Force will be funded to procure each year, and therefore, seeks to provide unique insights into how developments in the political environment impact upon the overall Defence function.

ADBR magazine is supported each month by an electronic newsletter, ADBR-Entrepreneur (ADBR-E), which specifically looks at how reforms to the military equipment procurement environment brought on by the Howard Government's decisions on the Malcolm Kinnaird's 2003 review of Defence Procurement are impacting on the defence business space, and in particular, what opportunities will be thrown up for the private sector to increasingly contribute to the efficiency with which the national Defence function is delivered on behalf of taxpayers.

Naturally, ADBR-E is also critically interested in how the Defence Materiel Organisation (DMO) is being restructured on its path to becoming a prescribed agency under the portents of the Financial Management and Accountability Act 1997, which is currently scheduled to occur on 1 July 2005. ADBR-E takes us into the field of regularly commenting upon the procurement performance of the Department of Defence in the science of Earned Value Management (EVM), that is, reporting on how current projects going through the acquisition system are meeting their contractual expectations in terms of Expenditure, Schedule and Capability. This work often takes us into the business of critically appraising initiatives of the DMO's CEO, Dr Stephen Gumley, however, we remain confident he views our contributions in parallel with his own quest, to make the

military procurement system more efficient and truer to the task of delivering new capability to warfighters in the most timely and cost-efficient manner that is possible.

For those of you who remain hungry for information on the defence-industry business space, even after digesting ADBR and ADBR-E, our organisation also publishes the weekly Defence Industry & Aerospace Report e-Newsletter, or DIAR.com as it is more widely known.

As I said earlier, our aim is to give readers the widest possible cut on what is happening in the defence-industry business space. DIAR.com does this in a weekly format which basically summarises - by headline and 4-7 line extract - all the key press releases, reports, speeches or other related documents released by key ministers and government departments most relevant to Australia's national defence, internal security and border protection functions. In addition to this, and uniquely in the Australian defence publishing environment, DIAR.com also covers all major industry press releases and other documents. In short, and as a 10-minute (maximum) read first up every Monday morning, a quick scan of DIAR.com either allows you to settle back into the business you had already planned to undertake that week, or alternatively, it changes your day and the week ends up running completely different to that which you had first planned!

## **1 - Sizing up to the NCW challenge**

So now that you better understand what it is that we do - and I'm conscious that I am the only thing between this august gathering and IQPC's sumptuous lunch - I will now try to hold your attention with some ground breaking insights into the age of Network Centric Warfare (NCW) that is apparently upon us, as just outlined by AVM Clarke, Gary Waters and company.

When I first accepted the offer to speak at this conference, I had in mind the delivery of a chilling repast as to what Australia's real technological capacity was to absorb all the barriers that might emerge in the not insubstantial challenge of moving to an NCW approach by our military. To provide some spice to that analysis, I thought to trawl you through the detail of the Auditor-General's recent report (No.5 of 2004/05) in regard to delivery of the Standard Defence Supply System (SDSS), or Joint Project 2077 as many others know it.

Whilst comprehensive in its analysis (we won't call it criticism), that report provides only one or two key elements of the broader range of requirements the ADF will have to overcome in heading towards effective NCW. In essence, if the fundamental IT systems underpinning the organisation's ability to keep track of its multitude of service personnel and civilians can't perform the basic task of adding up their leave entitlements, what chance do we have of harnessing information superiority to root out and neutralise suspected terrorists hiding in caves in foreign countries?

Clearly, and as recognised by Monday's announcements in regard to the 2003/04 Defence Annual Report, there remains a big job ahead of the organisation in not only addressing

financial records keeping, but also in data management across the broader organisation. The whole construct of data, its pyramid-like transformation into information and knowledge, and then distillation into wisdom is naturally at the heart of the concept of Network Centric Warfare.

In the past few months, and as I have read wider into the subject of the application of modern technology to the battlefield, I discovered the whole NCW construct appears to be built upon a series of quite bold assumptions, many of which appear to not have been substantially tested or proven before NCW proponents have moved on in taking the next leap of faith into the Network Centric world.

This has led me to look more critically at NCW concepts being proposed for Australia, so with your indulgence, I propose for the balance of this presentation to change my original plan of attack, and instead seek to put up for your considered examination some of these successive assumptions underpinning NCW. The tools for this analysis will not so much be computer modelling, wargaming, simulation or virtual reality centres, but the tried and tested 'snout' of a defence journalist with over fifteen years kicking around the fraternity on Russel Hill and the Parliament House.

## **2 - Information Superiority & Support Concept**

As a starting point, I might just draw some observations from the statements made so far this morning by our erstwhile friends in the Department. In this process, I am seeking to draw your attention to the collective use of NCW-speak (a term I have coined), compared to what you might think it means after pegging it back to what I was taught as the English language. Admittedly, that was a few years ago, however, you might again extend me your indulgences. Can we start with just a few key paragraphs from the little book outlining 'A Concept for Enabling Information Superiority & Support'.

**In summary, the key themes** contained in that publication would have us believe (ADBR's distillation):

.... The widespread use of information technology will inevitably lead to 'information superiority', a state of affairs in which our side would benefit from a far more detailed picture of the enemy than the enemy would be able to have of ours. From this position of superiority, our side would naturally come to understand the circumstances surrounding the battle long before the enemy could do the same, AND, aided by this 'cognitive' superiority, our side should then be able to devise tactical operations that could subsequently be unfolded at a significantly faster rate than the enemy's own reaction speed. This speed differential would succeed in confusing the enemy and paralysing his will to resist. Under such circumstances, our side would then be easily able to seize the initiative, dictate the course of military operations to the enemy, and thus end up destroying the enemy's forces in the substantive whole, and at minimum cost to us.

Now I might just leave that point summary up on the overhead for a minute so everyone can have a second take of the comprehensiveness of what is being proposed, and also, the accumulated assumptions contained in such a proposition.

If you believe what is being said, this new ability to wage war without having to worry any more about the uncertainty of battle my own father experienced as a bomber pilot in World War II might indeed, if true, constitute a revolution in military affairs. But, while all the consequences that NCW theory attributes to the use of information technology could occur in actual combat some of the time, I would suggest it is far from proven that even some of them could occur all of the time. Therefore, attempts by western militaries (and their supporting governments and taxpayers) to irreversibly restructure their defence forces around information technology before the natural limits of NCW assumptions have been explicitly ascertained, I would say, exposes the status of our national security to considerable risks.

In essence, and if said quickly, all the base assumptions and follow-on linkages and connections assumed in the paragraph cited above might lead readers to conclude the end result really is plausible. I fear not. On the basis of my readings, NCW theory has a tendency to assert, rather than argue, its revolutionary vision AND NCW proponents - with the force which so often characterises unquestionable convictions - have a similar penchant to brush aside quickly, and without further discussion, many points that may be legitimately raised in opposition to their claims.

Thankfully, and in the Australian contest, it is refreshing to witness the willingness of the Department of Defence to support forums such as these, so that the advantages and disadvantages of Network Centric Warfare, the integration of the undeniable qualities of information technology within the boundaries of more conventional, non-revolutionary forms of warfare, and a better understanding of the factors limiting the applicability of NCW theory to actual war might productively emerge.

So where am I going with my raising of this concept of 'factors that limit the applicability of NCW theory to actual war'? In essence, I see there is real merit in challenging early in the NCW adoption process the assumption that the widespread adoption of information technology alone will be able to produce the revolutionary advantages NCW theorists promise, because - as our own forces in Afghanistan and Iraq know - war is a bloody fight against ingenious and resourceful enemies, and a fight conducted by military forces whose behaviour is all too human.

By seeking to increasingly substitute the workings of information technology across the battlespace - as is the objective of NCW - for human control, there is a risk that in the quest to ensure our collective security, we might stumble as a result of blind faith being put in the omnipotence of such technologies, thus introducing new vulnerabilities that ultimately could undo our security.

### 3 - English as a second language to NCW-speak

The first issue I would draw your attention to as you listen to the presentations over this couple of days, and subsequently wade through the published information, is to reflect on the language that is NCW-speak. True, it sounds like English - it uses words like information, knowledge, understanding, and awareness - all words familiar to us from our first days in primary school. Yet I would caution you all that subtle differences in the interpretation of such language are at work. Let's just have a look at the forward to the IS&S Concept booklet [page (i)]:

"information superiority will require a secure infrastructure that allows information to be collected, analysed and distributed by the right people at the right time, providing friendly forces with an understanding of the situation that is superior to the adversary's."

The word I would like you to focus on is 'information'. My scribes dictionary (Pitman) tells me the word information means something else - 'intelligence given, instruction'. Somehow this is not what I think the IS&S concept is looking to communicate. I suspect, instead, its view of the word reflects essentially a computer professional's construct of information. That is, observations generally represented by the readings provided by some sensor device programmed to match statistical correspondence with certain energy levels. As such, what NCW talks about as 'information' is really only 'data'. This conclusion is supported in the IS&S Concept's next paragraph:

"This information will be drawn from a wide range of local, regional and global sources (particularly allied and coalition sources), including space-based capabilities, and will require tools to fuse, manage and process this information into intelligence."

Similarly, to the dutiful scribe the word 'knowledge' means - 'knowing; the result of knowing; mental apprehension'. Is this really what our friends in the NCW world mean? Again, I fear not. In NCW-speak, it is more likely that 'knowledge' is regarded as the discernment of patterns present in the information (read data?) one receives from sensors.

An itching snout journalist might further ask, are these differences in NCW-speak and common English the result of an inadvertent misreading of the dictionary, or - more concerning - a deliberate modification of meaning intended to serve the needs of NCW doctrine intended to justify the rule of information technology in future warfare, itself a developing construct where it is the ultimate combination of technology, not humans, that play the crucial role in securing the ultimate victory in combat? Too strong?

Let's move on, but in doing so, let us also be mindful of the 'Ps and Qs' of NCW-speak. I would say to you there appears to be a fundamental difference between the NCW usage of traditional English language when used to describe the key concepts of the quest to achieve situational awareness, and essentially, this difference reflects the degree to which the apprehending human mind is involved, if at all, in the process of generating and accumulating those critical insights which, ultimately, will be presented to humans further up decision chain as validated 'knowledge'. That is, of course, the 'knowledge'

upon which they will similarly be expected to distil wisdom in the process of making value-added decisions on our behalf in respect of national security and defence issues.

#### 4 - NCW theory and the essential vision

Returning to the 'key themes' collectively presented earlier as encapsulating the NCW approach - as elicited from our reading of the IS&S Concept booklet - I would now like to distil some key assumptions this audience might want to hold in their minds as they listen to the balance of presentations at this conference. Whilst there's not time to debate these in detail in this address - it's useful to highlight them in the subsequent process of exposing obvious weaknesses in the NCW construct.

- **NCW proponents first assert that the networking of battlefield entities automatically produces shared information between those entities** - Well I can accept this when connectivity is achieved simply by sensors and the connection between them consists of data links, but would this remain valid once humans are included as entities within the battlespace? Reflecting upon our earlier observations of NCW's misrepresentation of the word 'information', what might be the impact on information superiority when two people in the value-adding chain are unable to agree as to the veracity of information they have communicated to each other? Might it be that information content initially shared between human entities in this example will not necessarily become shared with the wider battlespace audience? But do not NCW proponents assume all information becomes shared?
- **NCW proponents secondly assert that virtual collaboration between networked, battlespace entities transforms shared information into shared knowledge** - Yet, if 'information' means no more than identifiable patterns in the available information (data?), can it really be viewed as knowledge? This second assertion cyclically relies upon the first, and therefore does not add any value to the belief that collaboration would automatically generate shared knowledge. Is it that NCW theory inadvertently seek to create a dominant 'information domain' dominated by technology as a feeder into subservient 'human domain' populated by humans as natural consumers of the information domain in their quest to command understanding and decision making?
- **The third NCW assertion actually crosses over this boundary between the information domain and the cognitive domain, and enters the latter.** It proposes that shared situational awareness and shared understanding are made possible by shared knowledge through collaboration.
- **NCW proponents fourthly assert that the shared situational awareness and understanding made possible by shared knowledge can be transformed into synchronisation.** If we check the NCW-speak against the scribes dictionary, I suspect the word 'orchestration' would have been a better choice. Essentially, the effect of this assertion is that the combination of NCW outcomes automatically enables commanders to orchestrate their forces in order to maximise the concentration of firepower against key enemy assets discovered in the battlespace.

- **NCW proponents fifthly assert that by thus synchronising (orchestrating?) its actions**, a networked force will be able to generate increased combat power by significantly increasing the speed at which it make decisions and executes orders, as well as by significantly increasing lethality, survivability, and responsiveness.

Taken together, all of these collective assertions (others cite them as hypotheses?) seek to establish an unshakeable belief that networking, as well as the collaboration enabled by it, will produce a revolution in military affairs that will change the course of future warfare. The reason they stress a belief, rather than certainty, is that accepting their validity similarly requires a larger number of supplementary conditions to also be met.

Being sprinkled through the NCW literature, they are not easily identified. Most of these assertions (requiring further investigation to establish their validity), appear to be presented as 'challenges' requiring the balancing of warfighters' expectations or 'risks' (IS&S, page 20) that NCW proponents expect to overcome during the development of a NCW-dependent force. As such, further expenditures in the forms of Experimentation, Simulation & Modelling, and dare I say Rapid Prototyping, are required to prove they really are no more than simple impediments. So what are these supplementary conditions? The following are but a few:

- The hypothetical nature NCW doctrine means it will not work unless the fog and friction of war can be kept under control. [To expand, if things revert to chaos, will our side still be able to control the play of battle?];
- To realise the revolution in military affairs all assertions, especially the first about fog and friction must end up being true, otherwise the NCW construct might start to fall in on itself;
- One must accept that human individuality and/or frailty do not intrude into the process of information sharing - essentially their must be 'quiet confidence and trust' right up and down the system (IS&S, page8). [To expand - humans must be able to accept information received from other humans, whether factual or documentary; must be able to handle without confusion large quantities of information; must be able to accept the compromise understanding resulting from collaboration despite any doubts they may still entertain about that compromise; and must be able to follow action orders that issue from that understanding without any misgivings.];
- An enemy subjected to NCW operations (eg: through the transformation of shared understanding into commanders intent and then onto synchronised action) will be substantively paralysed, and by default, lose his ability to think independently (eg: continuing resistance will be minimal). [To expand, the proposition that networking translates into information superiority is manifestly true if, and only if, the enemy lays himself out to be observed];

- Successful NCW operations require information assurance. Essentially, each item in an information system can be tracked back to its origin and validated, there is no opportunity for outsiders to tamper in the system by modifying/deleting records and/or introducing false information. [To expand, does the unchallenged acceptance of this assumption risk over-estimating our own peoples' capacity to deal with contradictory information, whilst similarly underestimating the enemy's ability for mischief].
- Does NCW really revolutionise warfare? I would argue the NCW model does not see us getting involved in a truly two-sided contest of warfare, one which is subsequently full of surprising moves by the enemy. Instead, it envisages us standing-off at some safe distance and surgically destroying largely helpless enemy forces at will. [To expand, do we not envisage strikes being easily defeated by the enemy creatively hiding from the attackers eye? By not challenging this assumption, are we not underestimating the power of an enemy that resorts to deception and evasion?]

Whilst I grant you that certain of the above qualities may be present in a first-rate NCW system at any one time, realistically, it is more likely that many (and perhaps all) of these qualities may in fact be missing from an NCW system, not because agencies did not try to create them, but because they are not physically attainable - either technologically or within the sort of Budgets that most western governments (other than the US) are generally willing to provide these days.

Essentially, and in my view, NCW doctrine (as well as elements of the IS&S Concept paper) essentially take it on faith that none of these so called challenges, balancing items (or risks) will prove, at the final raising of an NCW-dependent military force, to have been intractable. Why? Well let's look at it in reverse. Should our faith in NCW be eventually betrayed by reality, might not the great expenditures involved in attempting to transform the current force into an NCW-dependent force before each of these supplementary conditions was tested and proven, be subsequently proved to have been wasted?

If you accept the above, it doesn't take much more for the cynical journalist to start thinking - as one recent prominent NCW writer (Kaufman) has - "the doctrine of NCW is the embodiment of that consuming need for self-justification. By taking the proposition that information technology would enable us to fight our enemies in a totally different way than we have ever fought them before, the proponents are no longer under any obligation to justify their doctrine in terms of military advantage because those advantages are already presupposed in the new definition of what war is."

## **5 - What NCW is asking the ADF to achieve**

In the discussion above, I have looked to share with you a number of areas that collective writers suggest advocates of NCW tend to ignore. To the extent these observation have also clicked with you as deniable assumptions that NCW theory makes about war, then

perhaps you might also entertain such observation may turn out to be the very things that limit its applicability.

Effective NCW is said in the IS&S Concept paper (page 15) to have the effect of delivering 'the right information, in the right form, at the right place and time needed for concurrent planning and execution of operations'. In essence, this would set the ADF up to position itself in the right place at the right time, neutralise the enemy, and then leave more or less as soon as the neutralisation job is done. Use of the word 'right' suggests that we are more interested in countering the true actions of the enemy, not what we happen to think might be his true actions.

To achieve the latter, the future ADF must be able to surveil and reconnoiter enemy activity, quickly decide what to do in a consequence of what has been learned, attain and appropriate force posture at the appropriate time, execute the job as fast as possible without losing too much of the force, and then quickly move onto the next job. Yet, to the extent that an enemy is able to deceive us concerning his true operational intentions, we may end up - by virtue of these operations - being in the wrong place at the wrong time, with all the associated down-side effects. [In short, NCW faces limits to the extent we subsequently become exposed to enemy deception. To the extent an enemy is cleverer than we thought, or the future ADF's ability to collect information is no match for his ingenuity, would not an NCW-dependent force be left looking for alternative strategies?]

Since war, I am told, is a dynamic game - it cannot be assumed that the enemy will not try to evade our attack, whilst similarly looking to target our own attack assets for destruction. Can we therefore practically retain the assumption as suggested by information superiority, that an enemy will simply sit there passively awaiting to be destroyed by ground-based forces or stand-off weapons? If the enemy were to react in some unanticipated way to our attempts to destroy him, to what extent would this then diminish the military utility of our information gathering capability? Would we risk an NCW-dependent force collapsing? [In short, NCW faces limits by an enemy's resort to evasion whilst under attack.]

NCW proponents further assert that increasing the extent to which the force is networked must always return significant improvements in our capability to conduct war, because networking significantly increases force cohesion. Those of you of the naval persuasion will understand how difficult a task this is when considering the challenge involved in matching a group of people (essentially strangers) with a ship, and then having to fashion the two into a fully integrated ships crew and potent naval combatant. You will also perhaps understand how the average proficiency of each member of that crew might rapidly collapse if by catastrophic occurrence (eg: say an enemy strike), the size of that crew was reduced beyond some minimum number. [In short, the cohesiveness claimed under NCW is limited by the robustness of the human character.]

The rise of NCW has similarly been helped by a view that automation will not only deliver more effective warfighting capability, but also - by replacing man with machines - significant savings will accrue to governments without a significant loss of overall

military effectiveness. The utility of automated machines for any given function depends critically on the probability that the creator's vision of what may happen sufficiently coincides with what actually happens, a probability that for many functions may admittedly be high, but for others is also likely to be small.

Since man is better equipped to react intelligently to unforeseen circumstances than machines, replacing him by an automated machine would make sense only where the effect of the fog of war can be expected to be minimal. The debate between automation and the utilisation of man therefore, is decided by the extent to which one could expect to predict the operational environment. It appears this leans more towards automation when one believes oneself able to predict that environment, and towards man otherwise. [In short, NCW is limited by its assumptions about the extent to which humans can be replaced by machines. Essentially, one might automate all those tasks the performance of which would not be unduly effected by the vagaries of war.]

## **6 - Pegging back the NCW roadmap**

The above discussion has sought to illustrate some of the deniable NCW assumptions which - I submit - concern the often forgotten fact that war is a real contest between an unpredictable enemy and an imperfect self, not some mathematical exercise between stereotyped forces consummated via computer simulation. To the extent the discussion continues to focus more on the latter, and less on the former, I suggest our current approach to the adoption of NCW in the ADF risks us embracing two substantive failings - underestimating our enemy, and overestimating ourselves.

### ***Under-estimating the enemy:***

NCW proponents flirt with the deniable assumption that the enemy will not have the ingenuity to deceive us. The exact extent to which operational effectiveness can be increased as a result of available information content being increased depends upon the enemy's ability to hide his plan of action from us. To the extent that we have nothing to monitor or target, how are we to progress the course of the war?

To validate the claim of delivery of revolutionary advantages from information technology, NCW proponents have necessarily had to assume a perfectly predictable enemy. Conversely, allowing for a deceptive enemy forces NCW proponents to lower exaggerated expectations about the military value of information, and perhaps also call for additional expenditures on non-NCW military capability to make up the resultant gap.

Second, NCW proponents similarly embrace the deniable assumption that the enemy does not have the agility to force us into a dynamic encounter. The extent to which we can sustain our ability to monitor, target and attack an enemy depends upon what the said enemy does when first attacked. If such enemy is continually able to break off the engagement and resort to evasion tactics, NCW assumptions about the certainty of outcome of information enabled engagements is brought into question, again raising doubts about the validity of continuing investments in information technology against

more traditional military capability that is able to curtail an enemy's ability to evade successful engagement (eg: bunker penetrating bomb).

***Over-estimating ourselves:***

We have already spoken about NCW's deniable assumption that our human character does not play a significant role in the conduct of war. Ignoring the fact that we are, after all, only human, can lead to considerable misunderstandings in the current debate about the military utility of information technology. NCW proponents rely on the proposition that the networking of collaborative entities in a battlespace leads to common situational awareness, which in turn leads to self-synchronisation in action, and thus to a high rate of change in the tactical situation. Surely, the degree to which any of these events would actually occur depends upon the degree to which they are consistent with the nature of the entities connected by the network?

One might further accept the degree of common understanding attainable in a community of collaborating humans is strongly affected by the balance between the persuasive power of the community, and the degree of individuality demonstrated by its members. Humans being what they are, one should not expect them to easily discard their predispositions in favour of the community view. So before accepting NCW propositions outright and proceeding to acquire information technologies needed to network the force, might not a larger priority be developing a command and control system capable of efficiently manage the collaboration process?

In a similar fashion, increasing the size of the network might not necessarily lead to individuals that could react in a synchronised fashion to a common situational awareness, even if one emerged from a set collaboration. Could not it be argued the extent of self-synchronisation is more directly related to the proficiency with which members of the defence community are able to execute their part of the total task and that, in turn, depends upon: the size of the subject community, and the proficiency its members had before joining the community.

For a community the size of the ADF, one might consider the high degree of synchronisation required to satisfy the NCW outcome similarly requires a very high degree of pre-existing efficiency. In such a case, and contrary to the NCW order of battle, spending on recruiting and training systems to yield such individuals might rate a higher priority than the actual acquisition of information technology itself [Aren't there shades of SDSS in such observations?].

This leads me to a second deniable NCW assumption, that humans are infinitely perfectible. In reality, human proficiency is the result of the interplay between learning and forgetting. Learning involves both training as well as an individual's response to that training; the former is measured by the amount of time spent in training, the latter by the strength of the learning process that characterises the individual.

Yet I think we all know that the amount of time members of the military spend in realistic training is relatively small - meaning the level of proficiency is bound to be quite limited no matter how strong the learning ability. So whilst NCW proponents might argue the contrary, is it not more likely common situational awareness will not lead automatically to synchronised action because humans are not sufficiently perfectible? Further, and at this level of interaction in the data/information/knowledge/wisdom pyramid, there are obvious dangers in the extent to which humans can be substituted by machines in the pursuit of perfection.

## 7 - Summary and Conclusions

So my friends, I think we are now able to view the NCW proposition a little more clearer, and see it not as the final victory of technology over war, but for what it really is - just another new technology whose military value is strictly bounded by the realities of war. Such realities mandate that we should not assume our enemies are imperfect, nor that our own forces are perfect, as such assumptions risk increasing the vulnerability of our military posture. Accordingly, we should be careful to ensure the pursuit of the NCW vision is similarly matched by the procurement of sufficient traditional military capacity to ensure significant insurance against the possibility of all the NCW theory turning out to be wrong.

So despite all the hype about 'shock and awe' and the dawn of the new revolution in military affairs, I put it to you that what is being presented as the NCW roadmap can only be effectively advanced if its successive assumptions are exposed and put to the test of true or false. In the sum of it, this is not necessarily new.

What is new in much of the NCW literature is that old habits (of wisdom) appear to have been forgotten as people seem irresistibly attracted - like us all to 'Australian Idol' - to things that glisten but carry very little intrinsic value. The fact that we have all been drawn to this conference today to debate the issues gives me some confidence we are not just defaulting into a singular debate over the choice between Casey or Anthony, when in fact the real game and choice is John Farnham and Olivia Newton-John. Or has the real winner yet to materialise?

Towards the end of the IS&S Concept paper (page 26), it is stated that "commanders and staff must retain those elements of professionalism that endow them with a level of scepticism based on their understanding of an adversary's capabilities and the limitations of their own systems." I hope this presentation has gone some ways to achieving that directive. Ladies and Gentleman. NCW is an all encompassing subject, and I thank you for your patient attention.

**Acknowledgement:** ADBR's appreciation of the global Network Centric Warfare debate has been singularly expanded by the writings of Alfred Kaufman. See *'Curbing Innovation: How Command Technology Limits Network Centric Warfare'*, Argos Press, Canberra 2004 (Australia) ISBN 0 9580238 4 0