From simplistic assurances of NEC to optimistic promises of NCW:

More pitfalls than promises?

By Wing Commander A C Chopra

To reduce the costs of conflict, mankind has incessantly pursued means to achieve quick decisive victories. In the past this was achieved by superior firepower. However, proliferation of modern weaponry and asymmetric methods has substantially reduced this differential with the costs of war reaching unacceptable proportions. To regain the decisive edge it is necessary to exploit the capabilities offered by Network Centric Warfare (NCW).

NCW demands information on all battle space entities. In a network centric environment, all platforms will need to communicate with each other. This necessitates the ability of each platform to transmit and receive information and the existence of common communication protocols.

While the prospects offered by it are promising, the path ahead is unlikely to be easy or straightforward. This paper visualises the promises of Network Centric Warfare and explores the hurdles in achieving the capability. In the process this paper reaches the conclusion that while most hurdles imposed by technology may be overcome, the hurdles imposed by humans in the network centric loop will eventually limit our aspirations from Network Centric Warfare.

"Look around. No 'good old-fashioned war' is in sight."
(John Arquilla and David Ronfeldt)[1]

"A vision without the means to execute is just a hallucination."
(Stephen Case, Founder of AOL)[2]

"Predicting the future is an enterprise with a very poor record unless predictions are so broad as to be useless for setting priorities"
(Col John Jogerst)[3]

The aim in all conflicts is to achieve quick decisive victories at minimal cost. In the past, the 'edge' enabling such a victory was usually provided by superior firepower and warfare centred on the niche capabilities of individual weapon platforms. Such form of warfare was 'platform centric'. The proliferation of modern weaponry and asymmetric techniques has reduced the decisive edge offered by platform centric warfare. This edge may be regained if synergy is generated on the battlefield by enhanced cooperation between weapon platforms. The military 'behaviour' that personifies such cooperative behaviour is referred to as Network Centric Warfare (NCW). NCW is characterised by geographically dispersed forces possessing high levels of situational awareness which is generated by linking them to each other and the exploitation of this advantage to generate high tempo on the battlefield.[4]

NCW promises to generate efficiency and synergy between fighting elements, increase tempo of operations, improve time sensitive targeting, reduce possibility of fratricide and increase flexibility in operations

The term NCW is a broad-based concept and may be viewed from different perspectives; therefore it is essential to clarify some issues surrounding the term. United States uses the term NCW, while the United Kingdom uses the term Network Enabled Capability (NEC) to essentially refer to the same basic underlying concept of waging war. However, the difference between the two is that the US is not budget limited, while UK tends to view the concept on a more cautionary note due to its resource limitations.[5] In this paper these terms will be used on a general basis, without the subtleties of either countries approach prejudicing the basic concept. In addition, terms such as Dominant Manoeuvre, Precision Engagement, Full Dimension Protection and Focussed Logistics etc — which have come to vogue and tend to unnecessarily obscure simpler concepts — will be deliberately avoided in this in order to clearly grasp the concepts of NCW.

In simple terms, NCW promises to compress Boyd's Observation-Orientation-Decision-Action (OODA) cycle such that friendly forces sustain high tempo of battlefield operations. It does this by providing force elements with large amounts of correlated information so as to develop high levels of shared situational awareness amongst them (Observation & Orientation). This increase in knowledge levels on the battlefield then permits informed decision making (Decision) and also generates a common understanding of the commander's intent among all fighting elements, so as to achieve effective cooperation between them (Action).[6] In addition to the compression of the OODA loop, NCW promises to garner advantage from enhanced information access to permit 'smarter' behaviour and efficient use of war fighting resources thus allowing faster and more flexible responses to emergent battlefield situations. It is not a new concept and may be broadly viewed as the emerging military response to the information age.[7]

However, the challenge lies in distinguishing the theories behind NCW from how it will actually be practiced, as the practical application of a concept may impact on the concept itself and the result may distort the original intent.[8] This is

As the tools of war increasingly become market-place commodities, who can make war — and how and when — is changing. Proliferation of modern weaponry and information technology has made war like a game of chess

An Iraqi rebel carrying a portable rocket launcher

an important aspect of the issue, because NEC concepts are still in their infancy and likely to evolve further. However, at this stage a few issues are clear. NCW promises to generate efficiency and synergy between fighting elements, increase tempo of operations, improve time sensitive targeting, reduce possibility of fratricide and increase flexibility in operations. It aims to achieve this by generating synergy from cooperation between war fighting elements and exploiting advantages from information superiority. While the intention appears to be clear, there are subtle problems in the path of achieving fully-fledged Network Centric Operations (NCO). Inherent in the path lie problems associated with network security, information overload, command and control structures, interoperability of equipment, bandwidth requirements, lack of appropriate doctrines and increasing erosion of traditional war fighting skills due to over reliance on the promises of nascent technology.

It is easy to fall prey to the promises offered by technology alone. Co-evolution of doctrine must follow; support of legacy systems for their life span needs to be ensured, migration costs need to be carefully apportioned and importantly interoperability within and with external coalitions needs to be maintained. The course of action to possessing a NCW capability must be carefully protracted such that NCW remains a process to achieve an end and not an end in itself. If this is to be realized then it is important to understand what NCW is all about, what it promises to achieve and the problems that may arise in the process of acquiring such a capability. This paper addresses these issues and determines that many technological and human factor hurdles exist on the route to gaining a NCW capability. While the technological hurdles may be eventually overcome human factors in the network will eventually limit our aspirations from NCW. To find out why, we need to determine why NEC is required and how it will affect future operations.

Warfare takes on the characteristics of its age.[9] In the wars of the past, massed armies faced each other over linear battlefields. The Napoleonic model (Corps-Division-Brigade-Regiment-

Battalion-Company-Platoon),[10] a highly institutionalised system, was suited to such warfare. Modern war has changed. The battle space is no longer linear. It has extended by virtue of the increase in number and variety of targets of interest and their dispersion.[11] The presence of weapons of 'effects' capable of reaching across long ranges complicates how battle is viewed and conducted. As the tools of war increasingly become market-place commodities, who can make war — and how and when — is changing.[12] Proliferation of modern weaponry and information technology has made war like a game of chess, where everyone has the same pieces and can see the same battle space. The winner is the one who can make the best use of his pieces.[13] This changing nature of war and its participants needs to be addressed because a stagnant military

While vast amounts of information were collected by the coalition they were unable to effectively analyse it to generate a coherent picture of the battlefield. The inability to do so resulted in fratricide, the second highest cause of coalition casualties

A US Army Bradley fighting vehicle destroyed by friendly fire during the Persian Gulf war

force, inflexibly resisting change in its means and methods of war fighting, is likely to be easily defeated by an innovative adversary.

While it is accepted that wars are inevitable, the increasing costs of war are not acceptable. Wars of attrition and exhaustion are no longer tolerated. Wars may be fought but they have to be fought more efficiently. As the ability to wage war is a function of the available 'means' and 'will'[14] and the differential in 'means' between adversaries diminishes, warfare predictably results in severe attrition on both sides. To avoid the costs of such attritional warfare, smarter techniques such as Effects Based Operations (EBO) constantly explore alternative means of defeating the enemy.[15] As the cause and effect nature of EBO are complex, EBO rely intensively on large amounts of diverse intelligence in an attempt to determine what may be targeted, the existence of accurate success indicators and the chain of cause and effect that reach back to the adversary's ability to wage war. The need to collect, analyse and disseminate intelligence to share knowledge for EBO thus naturally leads the path of evolution of warfare towards 'network-centricity', i.e. the ability to easily share information. This ability to share information by networking will form the essential backbone of NCW. However, this is just the first step and brings up the issue of what more can be offered by NCW. A quick look at some recent conflicts throws light on the subject.

During Op Desert Storm, the Air Tasking Order permitted de-confliction and orderly management of air targeting, but did not permit near real time targeting due to its inflexibility in responding to the changing battlefield. Similarly, while vast amounts of information were collected by the coalition they were unable to effectively analyse it to generate a coherent picture of the battlefield. The inability to do so resulted in fratricide, the second highest cause of coalition casualties.[16] Thus, Op Desert Storm did not witness any sustained information management and exploitation. On the other hand, during Op Enduring Freedom, data services, iridium satellite communications and web-based services such as email were key enablers in the conflict.[17] In the austere environment in Afghanistan the need to network and the advantages of such networking allowed the coalition forces to deal with fleeting targets.[18] The ability to 'see' the battle space allowed the Commander in Chief Central Command to run the war without a Joint Tasking Commander from 7,000 miles away in Tampa.[19] Thus, in sharp contrast to Op Desert Storm, Op Enduring Freedom witnessed the military exploiting the advantages of networking and sharing information between widely dispersed assets. A careful look at the two conflicts clearly brings out the emerging realisation of the value of sharing information. This issue of value is imbued in Metcalfe's Law.

Metcalfe's law observes that although the cost of deploying a network increases linearly with the number of nodes in the network, the potential value of a network increases as a function of the square of the number of nodes that are connected on the network. To understand this concept of value more clearly, take the example of present day communication networks and what they offer. These networks range from traditional mail, telephones, fax machines, email and the multimedia-based World Wide Web. If the services offered by each is scaled on the values of full duplexity, service reach, visual experience, timeliness of information transportation, availability, capability for multi-actor participation, audio experience and search facilities, it may be noted that in the order presented above, each network in sequence presents an increasing value to the user in terms of 'richness' of the interaction and a better understanding of the content of what is communicated. The understanding of this concept of value is fundamental to understanding the power of NCO.[20]

Having understood the relationship between value and networks, it is now pertinent to take a look at how such value from information flow may mitigate the effects of 'fog' and 'friction' in war. It may be recalled that 'fog of battle' is about the uncertainty associated with what is going on, while 'friction of war' is about the difficulty in translating the commander's intent into actions.[21] In one way or another, either one relates to

Even if the intelligence gathered is accurate and relevant but cannot be timely disseminated and received, it has no value in dynamic battle space. Networking will therefore provide the crucial link in insuring an information advantage by providing timely transportation of accurate and relevant knowledge at all levels within battle space

availability of information at all levels in war. For example, the lack of information on an adversary's order of battle (ORBAT), its movements and intentions can lead a Commander to take a wrong decision. Similarly, lack of knowledge on the information upon which a commander's decision is based can lead lower formations to take actions out of line with the commander's intent. Both fog and friction may be alleviated by ensuring the availability of accurate, relevant and timely information with all force elements by interconnecting them. This achievement of information advantage will be one of the first priorities of NCW.

The author believes that accuracy of any piece of information is related to the amount of 'surrounding' information that can be gathered and on the manner in which it can be co-related or fused into knowledge in order to build a more wholesome 'picture'. The larger the amount of information that can be gathered and fused, the greater the accuracy of the final 'picture'. Similarly, relevance of information is important and pertains to determining when a piece of information may be useful. Knowing when a piece of information is relevant depends on knowing the context of the battle space and the knowledge of the context of the battle space is a function of the amount of information available on it. So, firstly, it may be said that to develop an accurate and relevant picture of the battle space there is a need to continuously gather information and fuse it into knowledge. Secondly, relevance of information is related to the ability to retrieve the intelligence from the gathered information when it is required and also relates to the ability to extract intelligence from the knowledge base on the basis of the context of the battle.

However even if the intelligence gathered is accurate and relevant but cannot be timely disseminated and received, it has no value in dynamic battle space. Network Centricity (i.e. the capability of all force elements to communicate with each other) will ensure fast movement of such information. Networking will therefore provide the crucial link in insuring an information advantage by providing timely transportation of accurate and relevant knowledge at all levels within battle space. This information advantage provided by NEC will help reduce the Fog and Friction of War and thus enhance situational awareness amongst all war fighting elements.

To ensure enhanced situational awareness, in addition to possessing knowledge about the adversary's ORBAT and intentions, it is also necessary to possess knowledge of the disposition of friendly forces. Therefore, to supplement the information provided by sensors, friendly force elements will also need to provide information on their status, movements and intentions. This information will then need to be transported over the same network links. Thus, NEC links will provide the information for building a composite picture of all war fighting elements on both sides of the battle space.

While situational awareness of individual elements may increase, the true potential of NEC will be realised when collaborative planning enhances this to 'shared' situational awareness. Networking will provide this ability to plan in

a collaborative manner because it will allow sharing of information between all war fighting elements. Shared situational awareness will then fulfil the two crucial promises of NCW: 'self synchronisation' and 'swarming'. However, before these two concepts are addressed it is necessary to understand the impact of networking and shared situational awareness on existing command and control structures.

Command and Control (C^2) structures serve the purpose of ensuring that the commander's intention is transmitted to his fighting elements (through a plan or concept of operations) and coordination of these elements to ensure their efficient utilisation. Present C^2 structures are pyramidical. These are necessarily so because planning is done at higher echelons, where all relevant intelligence is available. Commanders at each subsequent echelon need to be concerned with only a subset of these operations for three reasons. Firstly, they may not possess enough information on the battle space outside their immediate concern. Secondly, there are limitations to the number of simultaneous engagements that any commander can pay adequate attention to. Thirdly, the available lines of communication dictate the extent of control that each commander may exercise. Similarly military staff functions like intelligence, operations, logistics etc,

While the commander at the highest echelon makes the plan, the middle tier of the C^2 structure ensures that his intentions are understood, plans are developed to coordinate action, performance is monitored and feedback is provided

Soldiers of 3rd Battalion, 187th Infantry Regiment of the 101st Airborne Division, head into urban warfare operations east of the former Saddam International Airport

allow commanders at each level to maintain a coherent grasp of the war.[22] Therefore, while the commander at the highest echelon makes the plan, the middle tier of the C^2 structure ensures that his intentions are understood, plans are developed to coordinate action, performance is monitored and feedback is provided.[23] The command tier between the higher echelons and the force elements therefore exist primarily as facilitators of the commander's intent and as managers of the large resources of personnel and material under the commanders.

However this centralised system of planning and management is a manifestation of the belief in the need for optimising and de-conflicting war fighting elements. This is because in order to maintain cohesion and a grasp on the rapid events on the battlefield, commanders need to restrict the behaviour of its fighting elements short of the chaos that may result. Such optimisation and de-confliction is at the expense of synergy because it generally entails restricting action by one war-fighting element in order to permit freedom of action to another. In addition, it may be said that centralised planning is antithetical to agility because it is slow to recognise and respond to changes, results in ill informed participants and places many constraints on behaviour.[24]

A good example of how optimisation and the need to de-conflict reduce war-fighting capability is exemplified by close air support. At present there exist essentially two methods of avoiding fratricide in the battlefield when the enemy is in close contact. If the target to be attacked is within the Fire Support Coordination Line[25] the attacking aircraft needs to be actively controlled by a Forward Air Controller or the attacking aircraft needs to follow pre-planned procedures to execute his attack. Both methods reduce the flexibility of the pilot to engage emergent targets and impose severe constraints on the employment of aircraft. In addition in most cases, the presence of friendly aircraft in the battlefield restricts the land forces in utilisation of its organic firepower. Thus optimisation and de-confliction necessitated by centralised command and control methods, while reducing chaos, circumvent efficient utilisation of the full potential of war fighting assets.

Such centralised systems of command and planning reside on one end of the spectrum. On the other end of the spectrum is an example of C^2 as exemplified by the famous Battle of Trafalgar in which Lord Nelson commanded and controlled the battle with just two statements. The first was *"England expects that every man will do his duty"* and the second was *"Close Action"*.[26] Between the existing institutionalised hierarchies based C^2 that relies on centralised command (and planning) and completely 'self-synchronised' force elements (as exemplified by Lord Nelson's forces) lies the path that NCW will probably take. As rigidly centralised control and total de-centralisation are equally self-defeating, risks and implications need to be balanced by focused leadership and coherent strategic choices.[27]

The commander's necessity to control force elements in order to coordinate their action towards a centralised plan is also done at the expense of maintaining tempo of operations. On the other hand, if operations were completely decentralised there remains the risk that a subordinate's action could result in unwanted escalation or inappropriate use of force.[28] A good compromise between the two methods of command and control lies in the concept of '*auftragstaktik*', i.e. 'mission command'. The concept of 'mission command' relies upon decentralised execution of the commander's intent (i.e. coherent towards the intent but with high levels of flexibility, permitting exploitation of emergent situations in a dynamic battle space). Forces following 'mission command', would therefore be able to coordinate the execution of a plan while maintaining high tempo of operations. The availability of shared situational awareness among all war fighting elements provided by NEC will ensure that the commander's intentions are understood, thus allowing these subordinate elements greater freedom of action and thus greater tempo of operations. Concurrently, NEC will provide the necessary links to allow commanders at all levels to exercise control over their force elements. NCW will therefore balance between the need to sustain adequate tempo of operations and the need to ensure that the commander's intentions stated or implied are not

violated. NCW will therefore also achieve 'mission command'.

With that in mind, it is time to take a look at an important capability that NCW promises to provide —'self-synchronisation'. This is the ability of all force elements to synchronise their actions to the commander's intentions through shared situational awareness and action, with such speed and agility so as to negate the adversary's initiative.[29] It is a process by which each individual war-fighting element operates such that its actions are coordinated with all others and remains directed towards the commander's intent. Self-synchronisation needs three essential elements, firstly all force elements must have a common understanding of the context of the battle through a common operational picture and secondly they must be aware of the commander's intention and lastly the force elements must possess good training to utilise the knowledge from the first two in order to execute their actions synchronously to the overall campaign objective. Networking of force elements to share their picture of the battle space and easy flow of information between them and the commander will set the stage for such synchronous action. If proper training and doctrine is in place NEC will achieve the goal of providing such self-synchronisation.

To better understand the concept of self-synchronisation let us return to the example of the game of chess. In a networked environment, all friendly pieces will know the position of all other pieces on the board and will also be aware of what the player (commander) wants to achieve. With this knowledge they will then independently execute all necessary steps required to achieve the end state (defeat of the other side), flexibly responding to the adversary's actions and synchronising their actions towards their common objective (the commander's intent). The knowledge of the position and intent of all other pieces allows them to assist each other in a synergistic fashion. In theory, if the pieces are well trained and well knitted together by a sound doctrine, further intervention by the commander (player) would not be necessary till the other side is defeated. This synchronisation in action may only be disturbed when information on the each other's actions and its implications are not available to all war fighting elements. Networking will provide these crucial information links to permit 'self-synchronisation' to take place. Going back to the example of close air support, in a network-centric environment, self-synchronisation between land-based elements and the aircraft would permit the land forces to continue action while the aircraft engages targets more proactively within the same battle space with minimal restraints. The 'common' understanding of the context of the battle and each others 'intent' would permit all elements to behave in what may externally appear as chaos, but subtle coordination not externally visible would tie these actions to make a coherent whole.

If self-synchronisation is to take place, some changes in the existing command structures will be necessary. Self-synchronisation requires 'true' empowerment of the subordinate force elements.[30] Some predict that this need will flatten command and control structures; others argue that this will not be necessary. While it is necessary to understand that some changes will need to take place, their exact nature is however not important at this stage and will be discussed later in this paper.

In addition to promising self-synchronisation, NEC also promises the ability of force elements to 'Swarm'. Swarming behaviour may be explained as the convergence of geographically dispersed decentralised units on a common objective or problem and then re-dispersal for future action — a complex collective behaviour by individuals following simple rules.[31] As opposed to prolonged engagements swarming entails sustained 'pulsing', i.e. sustained 'hit & run' attacks creating running battles of attrition. This ability to flexibly concentrate firepower in time and space could then lead to creation of decisive conditions in multiple situations in battle space. Common examples of swarming behaviour are activities by smart mobs and terrorists. Some examples of swarming in history include the Battle of Arsuf in which Saladin successfully employed swarming techniques

to attack the crusaders, and the behaviour of Somalian militia and civilians in Mogadishu in 1993.[32] An example of accidental swarming action is exemplified by US airborne operations during the landings at Normandy, in which the troops parachuted into Normandy in disarray but accidental formation of ad-hoc groups allowed them to confuse the Germans with their hit and run tactics, till such time that they managed to organise themselves.[33] Similar swarming action, but deliberately executed, will be possible in network centric environments because NEC will provide a high degree of shared awareness amongst all participating force elements through a 'common operational picture'.

Importantly, this ability to swarm as envisaged by NCW also addresses problems with respect to concentration of force in war. The ability to share a common battle space picture and commonly understand the commander's intent will allow widely dispersed forces to pre-emptively initiate swarming behaviour to concentrate their mass (firepower) at any point in the battlefield. Thus, the need to mobilise large forces to cover large areas will not be necessary in network centric environments. The ability to swarm, coupled with standoff weaponry, will therefore change the manner in which concentration of force is generated on the battlefield. It will permit massing of effects rather than massing of forces on the

The need to mobilise large forces to cover large areas will not be necessary in network centric environments

US troops in northern Kuwait

battlefield. Additionally, the ability to generate concentration of force in battle space with widely dispersed forces also generates economy in effort as a lesser density of forces are required in any given size of battle space. Also, present day trends indicate that in order to gain greater mobility for manoeuvre, war-fighting elements are getting more and more dispersed on the battlefield. These will need to communicate through networks in order to maintain coherent action.[34] In fact, it is this trend that reinforces the author's belief that the final goal of NCW is to gain ability to swarm. This aspect will therefore be revisited later in the paper.

Another important capability provided by NEC will be the ability to attack time sensitive targets.[35] While stationary targets, especially high value strategic target systems may be identified by sustained surveillance and successfully attacked, time sensitive targets pose an ongoing dilemma for targeting. NEC will offer the ability to quickly spot, identify and determine the value of a target, thereby permitting it to be timely attacked. This ability will be one of the main value, adding characteristics provided by NCW.

This ability to attack time-sensitive targets exists because collaborative planning (as opposed to centralised planning) permits more agility in operations as well as better utilisation of resources. This is because collaborative planning by widely dispersed forces will allow them to self-assess the best methods for engaging such targets. In addition, flexibility in responses available through the larger subset of opportunities made available by NEC increases the options available to commanders in responding to emergent situations on the battlefield. This ability to operate flexibly in turn enhances the responsiveness of all force elements.

Therefore, NEC will provide the ability to timely share knowledge to enhance the understanding the context of the battle and the commander's intentions. It will permit smaller formations to exhibit unprecedented cooperative behaviour through self-synchronisation and swarming to engage numerically superior forces. It will increase flexibility, agility and responsiveness in action through collaborative planning and enhance the efficiency in utilisation of resources. Lastly, NCW will provide solutions for time sensitive targeting. In short, it will permit efficient operations in a controlled state of chaos.

The author believes that to meet all these promises, NCW will require an infrastructure based upon six critical capabilities:

- A large network with extensive bandwidth to connect all battle space entities
- A large number of sensors to collect information
- Technology to convert collected information to knowledge
- Technology to present the knowledge to all force elements in context of the battle in an easily understood form
- C^2 structures and doctrines to exploit the capabilities of self-synchronisation and swarming
- High training status amongst all force elements to actually execute cooperative behaviour as envisaged by self-synchronisation and swarming.

It may be noticed that out of the six capabilities mentioned above, the first four involve technology and the last two concern human factors. At first glance, it appears that all these requirements could be easily met — at least those concerning technology alone. However, it is easy to be complacent by over relying on the ability of technology to provide all the answers, for even the best of technology has its limitations. Most importantly, advantages provided solely by technology are at best temporary.[36] A closer look at the technological requirements and the human factors is therefore necessary to determine the first hurdles on the path to achieving NCW capabilities.

The first difficulty that comes to mind is the issue of communication between all elements associated with the network. In platform centric warfare, each weapon platform provided a niche capability of its own. The sum total of all the capabilities provided by the platforms determined the overall capability of the forces. There was little interaction between all these platforms.

The need for each weapon platform to transmit and receive poses two problems: firstly, that any transmitting platform can be detected. Therefore while NCW proposes to reduce the battlefield footprint, the presence of a large number of non-stealthy elements in the battlefield will achieve just the opposite. Secondly, the need to transmit and receive information between each force element will require these platforms to carry additional equipment to do so. On fighter aircraft at one end of the spectrum and the foot soldier on the other, the ability to carry such equipment will be at the cost of reducing their effective payload for war fighting. While some platforms may be made larger in size to do so at the expense of increasing their battlefield footprint, others such as the foot soldier cannot.[37] Therefore the core necessity for force elements to communicate in the envisaged ubiquitous networked environment opposes the need for stealth and reduces the effective payload carried by all force elements.

While NCW proposes to reduce the battlefield footprint, the presence of a large number of non-stealthy elements in the battlefield will achieve just the opposite

The next concern regarding the network is the issue of standardisation and interoperability. At present there exists a large number of legacy platforms that communicates on propriety protocols, and a majority that do not communicate with each other at all. In order to be interoperable, all platforms in a network centric environment will need to possess the capability of utilising a single secure communication protocol. Therefore the first step would be the need for all platforms to migrate towards such a protocol. This cannot be easily achieved and would also be expensive. The only viable option would be to accept the inability of older equipment to be interoperable while a contentious effort is made to ensure that all future systems meet the standards set for network centric systems. But, do such standards exist? If set timelines (approximately 2015 for UK)[38] are to be met to achieve a NEC, such standards need to be developed immediately. As the industries providing the weapon platforms are not run by the defence forces, this need to meet future standards must be communicated to them at the earliest. In addition as a large number of the weapon platforms come from different sources within the industry, the industry must agree to the decided standards and must be involved in its development from the start.[39] Such cooperative behaviour within the defence industries is unlikely to be initiated by it, as most industries rely on propriety achievements to develop a competitive edge in the defence market. Therefore, while it may be realised that interoperability is crucial, divergent interests will oppose coherent solutions to the problem.

In addition to the issue of meeting standards, interoperability has extra complications with respect to security of the standardised protocols. For example, in order to permit the industry to develop weapons and weapon platforms that meet the NCW standards, the MoD will need to release the details of such protocols to them. This could create problems on the issue of security of such information. On the other hand, if the protocols were released after weapon systems were chosen, it would unnecessarily delay acquisition of the platforms until such time that they met the set standards. This would in turn increase the cost of the platforms. Lastly, the release of standards to a select few to ensure security would also reduce the purchase options of the MoD.

The issue regarding interoperability does not end here. Even if all force elements are designed to be interoperable within a country, will they be interoperable in a coalition environment? For example, when the US DoD SIPRNet (a military form of the internet) was brought online it excluded its allies, thus forcing the US to develop a 'fix' called the Coalition Wide Area Network

A US Air Force Defence Support Programme (DSP) satellite being launched aboard a Titan IV B rocket in February 2004

In 1999 the US had $100 billion invested in space and in the next decade 1,000 satellites are expected to be launched into space. The costs for launching these was estimated to exceed half a trillion dollars

(CWAN).[40] Sub-optimised networking solutions can hardly be categorised as war wining. The answer to this lies on the ability of coalition partners to determine the need to develop standardised protocols for networking and sharing development processes, such that likely coalition partners meet interoperability standards from the very beginning. This is not likely to be an easy path as every country may prefer to keep certain niche capabilities to itself and may not 'fully trust' other partners.[41] This lack of trust is natural, as security standards for the network will need to meet stringent criteria, which all coalition members cannot afford. Sharing of information may then be restricted to the lowest common denominator defined by security issues. Therefore, coalition interoperability is likely to be a major hurdle in achieving a NCW capability.

In addition, the constant drive by defence industries to maintain a competitive edge has led to failure of interoperability between weapon systems within a country itself. While the development of technology within the military domain two decades ago led to technological advancement in the commercial sector, this process has now been reversed. The realisation of the need for maintaining interoperable standards within the commercial sector has permitted a larger improvement in technology available to it compared with the military domain. Defence industries therefore have no option but to revert to commercial practices on the issue and

will perhaps have no choice but to embrace commercial standards to maintain interoperability. In fact, most of the interoperability existing today has been imposed by the increasing use of commercial off-the-shelf software.[42] The reluctance of the military industry to increasingly rely on commercial hardware and software to maintain interoperability is likely to slow down the process of shifting towards network centricity. Alternatively the use of commercial standards to meet interoperability requirements is likely to pose security problems. This issue will however be dealt with later in the paper.

The next problem with attempting to set up a ubiquitous networked environment is the question of how such a network will physically exist. While short range communications between force elements may be easily achieved, long range communication with major network nodes or intelligence processing sites will need to rely extensively on satellite systems. The need for obtaining access to the information on each and every individually dispersed force element will also require support of the battle space from a large number of satellites.[43] As the transponders that may be fitted on a given satellite are limited, the number of satellites required for this task will be substantial. The problem is additionally complicated by the fact that such satellite systems will have to be geo-synchronous to provide good coverage or the number of satellites required would increase. If the intention is to possess NCW capabilities all over the globe, this number would increase even more. Therefore it is probable that NCW capabilities may only be achieved in geographically limited areas due to limitations imposed by the number of satellite systems available for completing the links required by the network.

The need for satellites also increases the costs of building such networks. In 1999 the US had $100 billion invested in space and in the next decade 1,000 satellites are expected to be launched into space. The costs for launching these was estimated to exceed half a trillion dollars.[44] These satellites are meant for a multitude of tasks from meteorology to relaying TV channels, and by themselves do not constitute the satellites needed for NCW. If the intention is to provide a NEC on a global scale, the estimated bill for providing the satellite coverage envisaged may be extrapolated from these figures to get an idea of the magnitude of costs involved. It may not be possible to meet such budgetary requirements, even for a country like USA. Thus, budget considerations will also constrain NCW capabilities. On the other hand, in a budget limited military force, the costs of continued investment in NEC technology would probably be at the expense of reduction in training, essential force levels or all-round capability. Therefore, while NEC may result in a leaner force with latent capability, it would probably be at the expense of losing traditional fighting skills and realistic training levels or result in restricted niche capabilities. The requirement to avoid these problems would then further increase the costs of building and sustaining a network centric force.

Another 'hidden' area that could increase costs is the need to protect the network. While all other forms of network nodes may be protected in some way or the other on the surface of the earth, protection of satellites is another matter. As the capability to wage a network centric war is heavily reliant on the use of satellites, they will become the 'centre of gravity' of the NEC and a lucrative target of choice. This vulnerability of satellite systems will thus pose an additional problem on sustaining the NEC.

In addition to the problems of long-range connectivity and the over reliance on satellites, there is the need for transporting large amounts of information on the network. This brings up the question of the availability of adequate bandwidth, i.e. the amount of information that can be transmitted at any one time. The increasing ability of sensors to transmit intelligence through video and the increasing demand for information in a visually appealing format whether it is for intelligence or video conferencing will place a heavy demand on bandwidth and a network centric force will therefore always use up whatever bandwidth is available.[45] As the number of force elements increase, this demand would increase exponentially. In fact, the lack of sufficient

bandwidth and its allocation was one of the major problems in communication during Op Enduring Freedom.[46] In the Global 2000 war game the available bandwidth was quickly saturated and caused the technical performance of the network to deteriorate.[47] Similar problems were faced in a NCW simulation exercise 'Millennium Challenge 2002', during which the US Defence Information Systems Agency conducted tests to determine bandwidth requirements and discovered that the small simulation network connecting 30,000 platforms was running at 48 megabits per second. (This is a long call, as present battlefield information systems communicate at only small fractions of this value.) The network therefore had to be adjusted to reduce this need to 10 megabits per second.[48] A medium scale operation could easily involve more than 10 times this amount, giving an idea of the amount of bandwidth that may be needed to satisfy a basic NCW capability. In the high frequency bands this bandwidth may be eventually realised, but achieving this requirement in the presently cluttered V/UHF bands is likely to pose problems. For example, while optical fibre can provide 100 Mbps connections between MoD and PJHQ, and satellite communications can provide 8 Mbps to JTFHQ, the bandwidth down to the lowest sub-unit relying on such V/UHF bands reduces to about 8 Kbps[49] — a figure not likely to provide impressive NCW capabilities.

During Op Enduring Freedom, despite the availability of Hellfire missiles on Predator UAVs (to reduce the sensor to shooter time gap) the problem of target identification still posed sufficient problems to negate the advantages of such systems

In addition, assuming that the physical structure of the network could be set up and that sufficient bandwidth existed to transport the collated intelligence, there would still be a problem with respect to putting the information into context so as to translate it into meaningful knowledge.[50] This will not be an easy task and as vast amounts of information are continuously gathered from the battlefield, the complexity of this task will exponentially increase. Knowledge representation methods will also need to be developed to store the context of the gathered information. Additionally techniques of depicting this information to force elements in forms appropriate to the context of the battle at their level will also need to be done. How will all this be achieved? As the nature of information needed at any given instant in the battlefield will continuously vary, the permutations and combinations of such representation techniques will put an enormous strain on the computing subsystems of the network. The time delays caused by this issue are likely to reduce the real time capability of the network, negating its very purpose.

Coupled to the issue of resolving intelligence to knowledge and presenting it to the network users is the problem of 'understanding' the presented information. It is common knowledge that given the same 'picture' of the situation, different individuals perceive and absorb what they see in a different manner.[51] Therefore the crucial and basic assumption, that it will be possible to develop a 'common operating picture' and 'shared awareness' is not likely to be correct. As NCW proposes to garner synergy from 'shared situational awareness' and 'shared awareness' of the commander's 'intent', the very lack of commonality in what is 'shared' within the minds of people is likely to subvert the intentions of NCW. Worse still, human decision-making alters under stress.[52] How will commonality in thought exist when war itself is stressful? The problem of generating a common understanding is enhanced in coalition environments, where military and civilian personnel of varying cultural, ethnic and religious backgrounds need to work collectively. In a paper written on the Exercise Bridge to Global 99 at the Naval War College USA, one of the lessons

learnt was that global situational awareness was a myth: assuming that such situational awareness exists could be hazardous.[53] At this stage even if it is assumed that the hurdles relating to technology are overcome, it becomes apparent that the real problem areas appear where the network interfaces with humans.

As one of the important objectives of NCW is to provide the capability to attack time sensitive targets, the next foreseeable problem is the question of how such intelligence may be quickly retrieved for action. During Op Enduring Freedom, despite the availability of Hellfire missiles on Predator UAVs (to reduce the sensor to shooter time gap) the problem of target identification still posed sufficient problems to negate the advantages of such systems. Although the rules of engagement in Afghanistan were perhaps more relaxed as may be expected in other conflicts[54] (as the case was in Op Telic), the unavailability of sufficient intelligence feeds to permit real time target identification restricted full exploitation of the available capability for time sensitive targeting. Therefore lack of capability in putting context to the intelligence and representation of the knowledge to the force elements so that they may take informed decisions is likely to reduce what may be expected from NCW.

Alternatively, the human mind is capable of assimilating a limited amount of disjointed information at a time. Therefore, simple representation of information (for example, the JTIDS air picture) will not be sufficient for commanders. As information is available on every force element (friendly or otherwise) the amount of information reaching commanders will be substantially higher than what is available at present. As long as intelligence is translated to knowledge and means exist to present it to commanders in an easily understood format, its sustained availability is likely to assist decision-making in the battlefield. However, as a consequence of slippage in meeting of timeframes for putting context to the information and as information continues to steadily flow in, the next problem that is likely to surface is that of information overload. This would result in commanders being engulfed in large quantities of incoherent information on which they would be expected to take decisions. Additionally, increasing information may reduce uncertainty due to lack of information, but it also increases the decision maker's uncertainty, as alternatives become difficult to single out.[55]

Traditionally, humans confront lack of precise information with heuristic responses and 'rules of thumb' behaviour allows us to handle uncertainty by taking intuitive decisions that reach back into the sub conscious centres of our brains for solutions. Simultaneously the amount of information that the human mind can scan is about seven words per second and process this information at a rate of one every 25 milli-seconds. Therefore, while there are advantages of collecting and organising large amounts of information, constraints on the information 'bandwidth' of the human mind and its traditional way of handling uncertainty impose fundamental limits on a human's ability to guide events in war[56] and lastly, as Macintosh states, "More information does not make for better decisions".[57]

The other end of this problem is that, as more and more information becomes available to commanders they will always want more information before taking a decision.[58] Therefore tools to assist commanders in utilising the vast quantities of information will need to exist before NEC may be gainfully employed. But do such tools exist today? More importantly, the author believes that as commanders increasingly rely on large amounts of information to take decisions their capability to take decisions in uncertain environments will slowly erode. Fast, agile and responsive action by commanders occurs when they rely on their intuition and experience. Over-reliance on information systems for decision-making will reduce this ability and probably be more counter-productive. Similarly if a soldier used to a network centric environment were to lose connectivity, his loss of situational awareness would be a lot higher than that of a soldier not used to it.[59] This could have serious connotations on the battlefield. Therefore, it appears that irrespective of what solutions technology may

US Air Force E-3D AWACS aircraft

Assuming that modern computational power can take on the burden of putting the information together and make a composite 'picture' of the situation, the 'picture' may itself be too complex to understand

offer, the presence of humans in the network centric loop are likely to impose limitations on what may be expected from network centric technology. Alternatively, the persistence of high technology and over reliance on it will eventually corrode the traditional war fighting capability of humans.

In order to exploit opportunities of time-sensitive targeting, self-synchronisation and swarming as offered by NCW, it will be necessary that the decision making process is speeded up. The current hierarchical command and control system is probably not suited to meet this need, because it relies upon a vertical chain consisting of many layers between the commander and the force elements executing his actions on the battlefield. Therefore, while the capabilities to collect, analyse, contextualise and disseminate intelligence exist to help commanders take better decisions, the lack of proper C^2 structures to exploit the capability will negate it. Alternatively, access to information

about every battle space element at higher command echelons may lead them to micro-manage the tactical level battlefield, thereby reducing the flexibility and agility of these war-fighting elements.[60] This problem of C^2 may be resolved only if proper doctrines exist on the subject. But, do such doctrines exist? The lack of doctrines for exploitation of NCW will limit its utility. Therefore, a major challenge will be the adaptation of the decision component to the new requirements of speed and tempo on the battlefield and achieving a balance between extreme centralisation or decentralisation.[61] Once again, the humans in the loop and their interaction with each other appear as the limiting factor.

Similar to the issue of command and control, is the problem of lack of doctrines and training on how self-synchronisation (or swarming for that matter) may take place. At the tactical level, not only is it important that doctrines exist to define the nature of the command relationships vertically and laterally, but it is equally important that all force elements are trained to respond cooperatively. It is important to recall here that self-synchronisation relies upon a common understanding of the commander's intent as well as the disposition and intent of all peer force elements. Pitfalls in sharing a common understanding of the commander's intent have already been mentioned earlier, but even if such an understanding exists, how are these force elements to 'realise' their part in a dynamic battlefield without being commanded to enact their 'subsets' of the plan? This may take place only if these force elements have extensively trained together before with the network centric equipment. Such high levels of training status may not be easily achieved. The inability to synchronise actions and confusion about a commander's intent could then have catastrophic consequences in a network centric environment.[62] To avoid such problems, training standards and operating procedures will need to be in place before attempts are made to use such technology on the battlefield. Therefore, it may be seen that promises made by technology will not bear fruit unless efforts are simultaneously made to address the issues of doctrine and training. Training takes time to catch up and in the meantime new equipment would be a burden to use.[63] Rather than developing the technology and then developing the doctrine, it is be necessary for them to co-evolve. The central issue in training is that of C^2. The fact that C^2 structures have been more or less static for a long time suggests that inherent inertia to transform is likely to be a cause for concern in achieving NCW capabilities. In the Global '98 War Game, existing command structures were identified as the single most difficult obstacle to achieving NCW capabilities.[64] This aspect was noticed again in the Global War Game 2001, when in the absence of extensive indoctrination and training, personnel were unable to make the transition easily to networked environments.[65] These human limitations will therefore need to be addressed along with improvements in technology.

Perhaps over and above all the hurdles mentioned above, as access to data increases, information security challenges will grow exponentially and security of the network will become crucial.[66] As the entire management, control and execution of the battle plan is based on the accessibility of the network, its availability and robustness will need to be of high order. Over reliance on the network would be analogous to 'putting all the eggs in one basket'. As information warfare techniques proliferate, the protection of the network will become increasingly difficult. The magnitude of the security problem may be realised by the fact that 95% of present military communications relies upon commercial communication networks.[67] The loss of any existing terminal with the force elements could pose a significant risk to the security of the entire network or the loss of a network node due to enemy action could result in loss of effective control over a large segment of the war fighting elements.[68] Alternatively, disconnection from the knowledge databanks could have more catastrophic results, with commanders losing situational awareness at a rapid rate.

From this viewpoint of computer network security at present only *SOLARIS 8* from Sun Microsystems is certified to operate at the high level of functionality and assurance specified by US NSA and DoD.[69] In spite of this, a large number of military systems worldwide continue to use Microsoft Windows NT Server, which is commonly known to have serious security holes.

As the number of applications across the network increases, the complexity of the task of providing security to these applications and the data they access will be a difficult time consuming task. In addition to plugging security holes in software, the need to ensure that real time security of network traffic is not compromised could lead to delays within the network. For example, during Ex-Strong Resolve 2002 (a major NATO exercise) security checks on a simple application like instant messaging resulted in delays of six to eight seconds for each message.[70] Such penalties for maintaining security may actually negate the tempo building effects of NEC. Alternatively, instead of becoming the war winning formula to regain the 'edge' in battle space, if improperly protected NEC could become its Achilles Heel.

Probably the biggest hurdle in achieving a NCW capability would be the limitations imposed on its use in the transition period. At one benign end of the segment this could imply that some force elements would not have access to the kind of information that other force elements have.[71] It could also suggest that their lack of 'connectivity' effectively removes them from the chain of force elements with which they could possibly collude or self synchronise (i.e. they would be left out of the 'game'). However, the transition period could also have a darker side. It may be recalled that in a network centric environment all friendly force elements must be aware of each other's disposition and intentions. Lack of connectivity within the network centric environment could then easily result in fratricide as the lack of information on any element would cause it to be classified as the enemy. As connectivity in a network centric environment is 'assumed' the probability of fratricide when connectivity is lost is higher in a network centric environment than otherwise.[72] Thus elite digitised forces such as the US Force XXI would probably have to operate in isolation, negating the very intentions of networking. Thus while experimentation continues, actual operations will need to be conducted on the basis of the least common denominator within the forces.[73]

The ability to wage network centric warfare would depend upon two broadly defined areas: firstly the 'Physical' portion consisting of the physical network connecting all war—fighting elements, its networking protocols, databanks, algorithms to manage knowledge and display systems to interface the knowledge to the force elements; and secondly the 'Behavioural' portion that concerns issues like command and control, dealing with information overload, collaborative decision making, self-synchronisation and swarming etc. The author believes, as explained in the paper above, that at sometime in the future the aspects concerning the availability of the physical portion of network centric capability will not be a problem and that the major obstacles reside in the behavioural portion. Now, some proponents of NCW believe that NCW itself is not about the ability to network, but how networking will alter our behaviour in future combat. In the words of Admiral Cebrowski, NCW is less deterministic and more emergent and has less focused on the physical than on the behavioural.[74] With this premise greater attention will need to be paid towards the behavioural portion of NCW as compared to the technological aspects, i.e. the limitations imposed by the human factor in network centric operations.

The largest subset of the hurdles surrounding the 'behavioural' aspects of NCW revolve around translation of intelligence to knowledge and the assimilation of this knowledge by the force elements so that they can take faster decisions. A look at the investment areas needed for NCW, as stated in the US DoD Report to the Congress on NCW, highlights this concern. In the report, out of the nine major areas needing investment, five revolve around this issue. Some that shed light on the areas of concern are 'sense making processing', 'visualisation', 'estimation and inference engines', 'automated learning' and 'information representation technologies'. [75] It does appear to look as if the technology providing the connectivity will not be a problem area, but the 'human factor' in the network-centricity that will probably need to be the focus of attention.

To understand why, let us take a look at the OODA loop. The process of observation is a continuous process.

As long as information is required, the process continues, the time taken for this process being fixed and decided by the kind of observation platform used (i.e. satellite, radio, humans etc). Similarly, the process of action is more or less a function of the mobility of the force elements and to some extent of their organic firepower. For most battlefield entities, both these values are also more or less invariant. That leaves us with orientation and decision. These may be speeded up but as it may have been noticed, both concern the human in the network centric loop.

Orientation is achieved when all pieces of information translate to an understanding of the situation, i.e. all pieces of information fit together as a jigsaw and sense can be made out of the information as a 'whole'. Assuming that modern computational power can take on the burden of putting the information together and make a composite 'picture' of the situation, the 'picture' may itself be too complex to understand. For example, take the case of fusion of the radar pictures from various ships in a battle group with AWACS to build a composite air picture. While the 'picture' may be complete in all respects the sheer amount of information on the screen could clutter it up to make it useless. Then again the immense amount of information of the screen would make it impossible for a watch officer to coherently answer a simple question as 'Can you tell me what's going on in the air'. Alternatively, even if a complex 'picture' is understood, can a decision that accurately balances the considerations of all aspects of the picture be taken in a timely fashion to exploit the information advantage? The author believes that human limitations of knowledge assimilation and human inability to pay cognizance to a large number of factors before taking a decision will be a serious impediment. Therefore in the aspirations of NCW, there will be an upper limit to the advantages that may be garnered from network centricity and these limitations will be imposed by the presence of humans in the loop.[76]

Having studied the promises and pitfalls of NCW, it is therefore time to review the situation and capabilities existing at present. This is necessary for finding solutions as to how the defence forces should adapt themselves in the near future. As mentioned earlier, the first step could be the development of a concept of what we expect to do with network centric operations before we start creating information architectures.[77] This will pay due cognizance to the behavioural/human factor aspects of NCW in time, lest technology leads us up a blind alley. The process will then chart out the 'art of the possible' to find a middle path between the optimistic promises of NCW and the simplistic assurances of NEC.

To reiterate, there is a need to acknowledge the fact that the drive towards network centricity is an emergent military response to the information age. The process of networking all sources of information is a process that will continue. Demands on information technology to meet the world's knowledge processing requirements will continuously increase and information technology will not fail to provide solutions. However, as determined above in the paper, the limitations imposed by the humans will need closer attention. As a consequence when addressing the question of data fusion and presentation, it will be more important to determine how the human element will interpret presented information than how it needs to be fused to knowledge in the first place. It will be more important to study aspects of training that could improve our ability to develop a 'common' understanding of concepts rather than to study how the capability to chat on computers may be provided to tank crews. Similarly, command and control relationships will need to be addressed to determine how the advantages of network centricity may be exploited. Ultimately, the success of NCW will depend not upon technology but upon how the war fighter will exploit the information advantage it provides.[78]

A careful look at the aspirations of NCW indicate a strong desire for gaining the ability to increase the battle tempo to limits that make it appear as chaotic to the enemy. Perhaps to even operate so fast that the battle is over before the enemy can react and no friendly forces are lost. But technology has its limitations and costs. There is no flaw in the military drive towards embracing

the rewards offered by information technology, but in the exuberance to achieve quick fix solutions the crucial areas may be overlooked until it is too late. When large-scale changes are required to the core techniques of waging war, investment in flawed principles could have drastic consequences. Thus, while many believe that doctrine and training must co-evolve in the drive towards network centricity, perhaps it would be better if endeavours in these areas were actually in the lead.

Finally, in the drive to fight clean and efficient battles, we must not lose sight of the enemy. In the present security environment, it is improbable that any two nations of great military capability will face each other. If NCW is not likely to provide any substantial advantages against enemies who are measurably inferior in capability,[79] then the belief that NCW will make a great difference, which is based upon theorising that our information technology vulnerabilities are mirrored by our enemies, will prove to be false.[80] Therefore it is essential to ensure that NCW remains a natural course of evolution for the military and not an end in itself.

Bibliography

Books

Alberts DS, Hayes RE (2003), Power to the Edge: Command and Control in the Information Age (USA: DOD COMMAND AND CONTROL RESEARCH PROGRAM PUBLICATIONS)

Alberts DS, Garstka JJ, Stein FP (2000), Network Centric Warfare: Developing and Leveraging information Superiority, 2nd Edition, (USA: DOD COMMAND AND CONTROL RESEARCH PROGRAM PUBLICATIONS)

Antal, J A (1999), Battleshock XXI, in Bateman III R L, Ed, Digital War: A View From the Front Lines (NOVATO, USA: PRESIDIO PRESS), pp 53-79

Arquilla J, Ronfeldt D (1997), A New Epoch and Spectrum of Conflict, in John Arquilla and David Ronfeldt, Eds, In Athena's Camp, (SANTA MONICA CALIFORNIA USA: RAND PUBLICATIONS)

Bateman, III R L (1999), Pandora's Box, in Bateman III R L, Ed, Digital War: A View From the Front Lines, (NOVATO, USA: PRESIDIO PRESS), pp 1-52

Bolger, D P (1999), The Electric Pawn: Prospects for the Light Forces on the Digitised Battlefield, in Bateman III R L, Ed, Digital War: A View From the Front Lines, (NOVATO, USA: PRESIDIO PRESS), pp 53-79

Britten S M (2001), Directing War From Home, in Martel W C, Ed, The Technological Arsenal: Emerging Defence Capabilities, (WASHINGTON, USA: SIMITHSONIAN INSTITUTION PRESS)

Department of Defense Report to Congress (2001), Network Centric Wafare, (27 July 2001), JSCSC Library Ref 355.402 Accession No J14669.

Edwards, Sean J A (2000), Swarming on the Battlefield: Past, Present and Future, (WASHINTON DC USA: RAND PUBLICATIONS)

Leonhard, R R (1998), The Principles of War in the Information Age, (NOVATO, USA: PRESIDO PRESS)

Macintosh, J P (1998), Connectivity: The Space, Tempo, and Exploitation of Risk in the Information Age, in Alan D Campen and Douglas H Dearth, Eds, Cyberwar 2.0: Myths, Mysteries and Reality,(VIRGINIA, USA: ARMED FORCES COMMUNICATIONS AND ELECTRONICS ASSOCIATION INTERNATIONAL PRESS), pp323-346

McClure, W B (2001), Computers and Controlling War, in Martel W C, Ed, The Technological Arsenal: Emerging Defence Capabilities, (WASHINGTON, USA: SIMITHSONIAN INSTITUTION PRESS)

Moffat, James (2003), Complexity Theory and Network Centric Warfare, (USA: DOD COMMAND AND CONTROL RESEARCH PROGRAM PUBLICATIONS)

Newell C R (1991), The Framework of Operational Art,(NEW YORK ,USA: ROUTLEDGE)

O'Hanlon M (2000), Technological Change and the Future of Warfare, (WASHINGTON DC, USA: BROOKINGS INSTITUTION PRESS)

Peartree C E, Allard C K, O'Berry C (1997), Information Superiority, in Daniel Goure and Christopher M.Szara, eds, Air and Space power in the New Millennium, (WASHINGTON DC: USA, The Centre for Strategic and International Studies), pp117-131

Smith, EA (2002), Effects Based Operations: Applying Network Centric Warfare in Peace, Crisis, and War, (USA:

DOD COMMAND AND CONTROL RESEARCH PROGRAM PUBLICATIONS)

Tyrrell, Patrick (1998), Cyberwar: The Role of Allies and Coalition Partners, in Alan D Campen and Douglas H Dearth, Eds, Cyberwar 2.0: Myths, Mysteries and Reality, (VIRGINIA, USA: ARMED FORCES COMMUNICATIONS AND ELECTRONICS ASSOCIATION INTERNATIONAL PRESS), pp 367-380

Articles

Ackerman, RK (March 2002), Technology Empowers Information Operations in Afghanistan, Signal (March 2002), pp 17-20

Ackerman, RK (April 2002), Afghanistan is Only the Tip of the Network Centric Iceberg, Signal (April 2002), pp 45-47

Ash, Lawrence N Cdr (2000), Fighting for Network Centric Warfare, Proceedings(August 2000), pp 74 – 76

Barnett, Thomas PM (1999), The Seven Deadly Sins of Network Centric Warfare, Proceedings (January 1999), pp 36-39

Berry, Sharon (2002), Collaborative Tool Buddy-Lists Coalition Partners, Signal (May 2002), pp 57-59

Bowdish, RG Cdr & Woodyard, Bruce Cdr (1999), A Naval Concepts-Base Vision for Space, Proceedings (Jan 1999), pp 50-53

Cebrowski AK Vice Admiral, Gartska JJ (1998), Network-Centric Warfare: Its Origins and Future, Proceedings (USNI), pp 28-35

Gagnon, Greg Capt (2002), Network-Centric Special Operations — Exploring New Operational Paradigms, Air & Space Power Chronicles, pp 1-10

Jogerst, John Col, USAF (2002), What's so Special about Special Operations? Lessons from the War in Afghanistan, Aerospace Power Journal (Summer 2002), pp 1-4

Kolenda, Christopher D Major (2003), Transforming how we fight, Naval War College Review (Spring 2003) Vol LVI, No2, pp 100-121

Kurth, Rolf Lt (2003), Networked Enabled Capability — The Future is Now, The Naval Riveiw (November 2003) Volume 91 No 4, pp 313-322

Ladymon, JM(2001), Network-Centric Warfare and Its Function in the realm of Interoperability, Acquisition Review Quarterly (Summer 2001), pp 111-120

McKendrick, Joseph (2002), Diverse Groups share Information Assurance Quandaries, Signal (August 2002), pp 41-44

Mitchell, Paul T Dr (2003), Small Navies and Network-Centric Warfare, Naval War College Revie, (Spring 2003) Vol LVI No 2, pp 83-99

ML (2002), Facing the Challenges of The New Millennium, Signal (July 2002) pp 51-54

Nagy, Paul Cdr (2001), Network-Centric Warfare Isn't New, Proceedings (September 2001), pp 44-46

Podlesney, Robert (1999), Infrastructure Networks Are Key Vulnerabilities, Proceedings (February1999), pp 51-53

Smi, Edward Dr (2001), Network Centric Warfare: Where's the Beef?, Naval War College Review Winter 2001, Vol. LIV, No. 1

Toomey, Christopher J (2003-4), Army Digitisation: Making it Ready for Prime Time, Parameters Winter 2003-04 BOL XXXIII No 4, pp 40-53

Watman, Kenneth Dr (2001), Global 2000, Naval War College Review (Spring 2001) Vol LIV No 2, pp 75-88

Zimm, Alan D Cdr(Retd) (1999), Human-Centric Warfare, Proceedings (May 1999), pp 28-31

Research papers

Hatter, SD Lt Col (2000), Self Synchronisation: Splendid Promise or Dangerous Delusion, Department of Joint Military Operations, (NEWPORT (USA): NAVAL WAR COLLEGE), Available Online at http://stinet.dtic.mil/cgi-bin/fulcrum_main.pl?database=ft_u2&searchid=10772833116239&keyfieldvalue=ADA381665&filename=%2Ffulcrum%2Fdata%2FTR_fulltext%2Fdoc%2FADA381665.pdf Accessed 29 Sep 2003

Keuhlen, DT Capt, Bryant OL Lt Col, Young KK Lt Col (2002), The Common Operational Picture in Joint Vision 2020: A Less Layered Cake, Joint Forces Staff College, Joint and Combined Warfare School Class 02-2S (28 May 2002), Available Online at http://www.jfsc.ndu.edu/current_students/documents_policies/documents/jca_cca_awsp/common.doc Accessed 22 Sep 2003

Richard, CA Cdr (2000), Network Centric Warfare and the Bandwidth Limited Platform: Beyond the Engagement, Department of Joint Military Operations, (NEWPORT (USA): NAVAL WAR COLLEGE)

Available Online at http://stinet.dtic.mil/cgi-bin/fulcrum_main.pl?database=ft_u2&searchid=107753917929259&keyfieldvalue=ADA382111&filename=%2Ffulcrum%2Fdata%2FTR_fulltext%2Fdoc%2FADA382111.pdf Accessed 27 Oct 2003

Slais, TA Jr Lt Cdr (1999), Some Principles of Network Centric Warfare: A Look at How Network Centric Warfare Applies to the Principles of War, Department of Joint Military Operations, (NEWPORT (USA): NAVAL WAR COLLEGE)
Available Online at http://stinet.dtic.mil/cgi-bin/fulcrum_main.pl?database=ft_u2&searchid=10772080374814&keyfieldvalue=ADA363055&filename=%2Ffulcrum%2Fdata%2FTR_fulltext%2Fdoc%2FADA363055.pdf Accessed 27 Oct 2003

Washington, JC Cdr (May 2001), Network Centric Warfare and Command and Control: Rethinking Organisational Architecture, Department of Joint Military Operations, (NEWPORT (USA): NAVAL WAR COLLEGE) Available Online at http://stinet.dtic.mil/cgi-bin/fulcrum_main.pl?database=ft_u2&searchid=10772075011311&keyfieldvalue=ADA393553&filename=%2Ffulcrum%2Fdata%2FTR_fulltext%2Fdoc%2FADA393553.pdf Accessed 27 Oct 2003

Zimmerman, JD Lt Cdr (2002), Command and Control in a Network Centric Environment, Department of Joint Military Operations, (NEWPORT (USA): NAVAL WAR COLLEGE)
Available Online at http://stinet.dtic.mil/cgi-bin/fulcrum_main.pl?database=ft_u2&searchid=10772078473488&keyfieldvalue=ADA389764&filename=%2Ffulcrum%2Fdata%2FTR_fulltext%2Fdoc%2FADA389764.pdf Accessed 27 Oct 2003

Online reports & seminar papers

Adkins M, Kruse J, Younger R (2002), Ubiquitous Computing: Omnipresent Technology in Support of Network Centric Warfare, Proceedings of the 35th Hawaii International Conference on System Sciences-2002, pp 1-9, Available Online at http://csdl.computer.org/comp/proceedings/hicss/2002/1435/01/14350040.pdf Accessed 29 Sep 03

Brehmer, Berndt Prof & Sundin, Claes Col, Command and Control in Network-Centric Warfare, The Swedish National Defence College, Department of Operational Studies. Available Online at http://www.militaryscience.org/public/media/publications/Brehmer&%20Sundin(2000_45f).PDF Accessed on 29 Sep 03

Borgu, Aldo (2003), The Challenges and Limitations of 'Network Centric Warfare' — The Initial views of a Sceptic, A presentation to the Network Centric Warfare: Improving ADF capabilities through Network Enabled Operations Conference, Wednesday 17 Sept 2003, Australian Strategic Policy Institute, Available online at http://www.aspi.org.au/pdf/ncw_ab.pdf, Accessed 01 Nov 2003

Chartie, Chris (2003), Swarming, Networked Enabled C4ISR and U.S Military Transformation, Conference Proceedings — Swarming: Networked Enabled C4ISR, 13-14 Jan 2003", Revised 25 Jun 2003, Section B pp 1-15 Available Online http://140.185.43.25/Swarming/Swarming_Conference_Proceedings.pdf Accessed 29 Sep 2003
Edwards, Sean (2003), Military History of Swarming, Conference Proceedings — Swarming: Networked Enabled C4ISR, 13-14 Jan 2003", Revised 25 Jun 2003, Section C pp1-18 Available Online at http://140.185.43.25/Swarming/Swarming_Conference_Proceedings.pdf Accessed 29 Sep 2003

Honan JT, Allen B, Hamilton (2003), Riding the Whirlwind: C^2 of Swarms using the Public Safety Model, Conference Proceedings — Swarming: Networked Enabled C4ISR, 13-14 Jan 2003, Section C pp 41-51 Available Online at http://140.185.43.25/Swarming/Swarming_Conference_Proceedings.pdf Accessed 29 Sep 2003

Kiszely, JP Lt Gen (2003), Networked Enabled Capability — The Human Dimension, Paper — Proceedings of NEC — The Human Dimension, A symposium on Network Enabled Capability at The Defence Academy Shrivenham on 26-27 Nov 2003.

Money, AL (Assistant Scretary of Defence (C^3I) (2003), Report on Network Centric Warfare: Sense of the Report, Available online at http://www.defenselink.mil/nii/NCW/ncw_sense.pdf, Accessed 01 Nov 2003

NEC Outline Concept Part 1 (2003), Dstl/IMD/SOS/500/2 Issue 2.0 dated 02 May 2003, Available at JSCSC Intranet

Norwegian Battle Lab & Experimentation (NOBEL), White Paper : Common Operating Picture (CODS), http://www.lencods.com/Downloads/CODS-WP.pdf, Accessed 04 Nov 2003

Rafferty, P Lt Col (2003), Tactical Networked Enabled Capability — The Human Challenge, Presentation — Proceedings of NEC — The Human Dimension, A symposium on Network Enabled Capability at The Defence Academy Shrivenham on 26-27 Nov 2003.

Seymour, Robert & Sands, DG & Grisogono, Anne-Marrie & Unewisse, Mark & Vaughan, Jon, Application of Network Centric Warfare Concepts to Land-Air System — an experimentation approach, Land Operations Division, Defence Science and

Technology Organisation, Salibury South Australia. Available Online at http://citeseer.nj.nec.com/rd/95848840%2C461198%2C1%2C0.25%2CDownload/http://citeseer.nj.nec.com/cache/papers/cs/23093/http:zSzzSzwww.dodccrp.orgzSz6thICCRTSzSzCdzSzTrackszSzPaperszSzTrack2zSz049_tr2.pdf/application-of-network-centric.pdf Accessed 29 Sep 2003

The Joint Staff, C4 Systems Directorate, Information Superiority Division (J6Q), Enabling the Joint Vision, Pentagon, Washington DC, May 2000, Available Online at http://www.dtic.mil/jcs/j6/enablingjv.pdf Accessed 29 Sep 2003

Wells, Linton Dr (2003), Opening Remarks, Conference Proceedings — Swarming: Networked Enabled C4ISR, 13-14 Jan 2003, Revised 25 Jun 2003, Section A, pp 1-3, Available Online at http://140.185.43.25/Swarming/Swarming_Conference_Proceedings.pdf Accessed 29 Sep 2003

Notes

1 Arquilla & Ronfeldt (1997), p 1
2 Wells (2003), p 1
3 Jogerst (2002), p 1
4 Alberts,Garstka,Stein (2000), p 90-91
5 Borgu (2003), p 4, 5
6 Gagnon (2002), p 2
7 Alberts,Garstka,Stein (2000), p 88
8 Borgu (2003), p 2
9 Money (2001), p 4
10 Washington (2001), p 4
11 Alberts,Garstka,Stein (2000), p 62
12 Cebrowski & Garstka (1998), p 29
13 Alberts,Garstka,Stein (2000), p 64
14 Smith (2002), p 25
15 Smith (2002), p 46
16 Keuhlen, Bryant, Young (2002), p 7, 8
17 Ackerman (Mar 2002), p 19
18 Ackerman (Apr 2002), p 46
19 Keuhlen, Bryant,Young (2002), p 8
20 Alberts,Garstka,Stein (2000), p 250-261
21 Alberts,Garstka,Stein (2000), p 72
22 Alberts, Hayes (2003), p 38
23 Ibid (2003), p 41
24 Ibid (2003), p 63
25 A Fire Support Coordination line is a line drawn on a map, close to the battlefront, depicting the forward edge of the land commander's activity. Any air activity within the boundaries of this line, need to be approved by and coordinated with the land commander.
26 Zimmerman (2002), p 1
27 Peartree (1997), p 121
28 Zimmerman (2002), p 9
29 Slais (1999), p 9
30 Hatter (2000), p 13
31 Chartier (2003), p 1, 2
32 Edwards (2003), p 2, 3
33 Honan, Allen, Hamilton (2003), p 42
34 Leonhard (1998), p-120/121
35 Alberts,Garstka,Stein (2000), p 58
36 Edwards (2000), p 75
37 Bolger (1999), p 123
38 NEC Outline Concept UK, p 5
39 Ash (2000), p 74
40 Ladymon (2001), p 114
41 Kiszely (2003), p 5
42 Patrick (1998), p 377
43 Ackerman (2002), p 18
44 Bowdish & Woodyard (1999), p 52
45 Richard (2000), p 20
46 Ackerman (2002), p 18
47 Watman (2001), p 81
48 ML (2002), p 53
49 Rafferty (2003), Slide 23
50 The Joint Staff, C4 Systems Directorate (2000), p 12
51 Kolenda (2003), p 100
52 Zimm (1999), p 30
53 Hess & Entin & Hess & Hutchins & Kemple & Kleinman & Hocevar & Serfaty (1999), p 12
54 This is the author's opinion and is based on the fact that media presence was minimal in Afghanistan.
55 Brehmer & Sundin
56 McClure (2001), p 222
57 Macintosh (1998), p 326
58 Borgu (2003), p 3
59 Antal (1999), p 54-79
60 Kiszely (2003), p 3
61 NOBEL White Paper, p 4
62 Hatter (2000), p 11
63 Bateman (1999), p 6-8
64 Washington (2001), p 1
65 Adkins, Kruse, Younger (2002), p 7
66 McKendrick (2002), p-41
67 Peartree (1997), p 124
68 Podlesny (1999), p 52
69 McKendrick (2002), p 42
70 Berry (2002), p 57
71 Kurth (2003), p 320
72 Toomey (2003-04), p 45

73 Mitchell (2003), p 89
74 Moffat (2003), p 45
75 DoD Report to Congress on NCW (2001), p 10 15
76 The ideas expressed in the two paragraphs above are the author's
77 Smi (2001), p 1
78 Nagy (2001), p 44
79 Seymour, Sands, Grisogono, Unewisse, Vaughan, Baumgart, p11
80 Barnett (1999), p 38