NETWORK CENTRIC WARFARE

> Our existing hierarchical structure, created long before IT started making its impact, is unable to cope with our current and future requirements. We will be at a great disadvantage if we do not realize the value of networking as we move towards the next millennium. [1]
>
> - General VP Malik

INTRODUCTION

At the start of the new millenium we are driven to a new era of warfare. The emergence of Information Technology (IT) is changing the society at an extremely rapid pace. Naturally the fundamental changes happening all over would affect the very nature of war and how we fight them. In this information age we are in the midst of a Revolution in Military Affairs (RMA) which is being called as, "A fundamental shift from what we call platform centric warfare to something we call network centric warfare."

In the business world Information Technology is undergoing a fundamental shift from platform centric computing to network centric computing. Platform centric computing emerged with the widespread proliferation of Personal Computers (PC) in business and at home. However, with the explosive growth of internet, intranet and Local Area Networks personnel using these are well aware of Transmission Control Protocol/Internet Protocol (TCP/IP), Hypertext Mark Up Language (HTML), Web Browsers (such as Internet Explorer or Netscape Navigator), Search Engines (like Yahoo or Altavista) and JAVA Computing Architecture. These technologies combined with high volume, high speed data access and high speed data networking using hubs and routers have led to the emergence of network-centric computing. The business world is shifting towards network-centric operations which are characterized by information-intensive interactions between computational nodes on the network. Whether these interactions are focused on commerce, education or military operations, there is "value" which is derived from the content, quality and timeliness of information moving between nodes on the network. Network centric warfare would give the military the same advantages as is being accrued by the business world. [2]

In this information age it is already apparent that new levels of military effectiveness can be achieved by networking together disparate sensors, weapons and command and control systems. Rapid advances in information and related technologies allow military forces to detect, identify and track a far greater number of targets over a larger area for a longer time than ever before. Increasingly powerful information processing and communication systems offer the ability to distribute this data more quickly and effectively. The result is a dramatic improvement in the quality and quantity of information that modern military organization can collect, process and disseminate.

The integration of information technology into military forces is also changing the relationship between fire and maneuver. Networking long range sensors and weapons allows us to concentrate fire from dispersed platforms on a common set of targets. The US Navy, for example, has examined the "Ring of Fire", a concept for focusing dispersal naval fire over shore based targets. Networking thus allows the potential massing of effects without massing forces. It would also reduce vulnerability by denying an adversary the ability to target forces with his own long range strike systems, while increasing the tempo of military operation by reducing the delay between observation and action. [3]

In the information age time available for a commander to make a decision has been reduced considerably. It is ironic that on one hand information age gives vastly increased capabilities to collect and process data that makes it possible to make better and better decisions more and more quickly is-on the other hand-reducing the time available to make decisions.

WHAT IS NETWORK CENTRIC WARFARE

"Network Centric Warfare is to warfare what e-business is to business"

The term Network Centric Warfare (NCW), as yet, has not been universally accepted in the Defence Community nor Network Centric Concepts well understood. The term Network Centric Warfare was first introduced to a wide audience in 1998 in the seminal article "Network Centric Warfare : Its Origins and Future" [4] in Proceedings of the Naval Institute. There is an emerging understanding in the international defence community of the power of network centric operations. Distribution of large number of copies and downloading of the book "Network Centric Warfare" : Developing and Leveraging Information Superiority [5] has made the concept of NCW well known. The recent US DOD report on NCW gives a detailed account of what USA is thinking on this kind of warfare. [6]

Network Centric Warfare derives its power from the strong networking of a well informed but geographically dispersed force. The enabling elements are a high performance information grid, access to all appropriate information sources, weapons reach and maneuver with precision and speed of response, value adding Command and Control (C2) processing and integrated sensor grids coupled in time to shooters and C2 processes. Network-Centric Warfare is applicable to all levels of warfare, and contributes to the coalescence of strategy, operations and tactics. It is transparent to mission, force size, composition and geography. NCW is an approach to the conduct of warfare that derives its frontier from the effective linking or networking of the war fighting enterprise. It is characterised by the ability of geographically dispersed forces to create a high level of shared battle space awareness that can be exploited via self synchronization and other network- centric operations to active commander's intent.

Network Centric Warfare may be defined as information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability and a degree of self synchronization. In essence, NCW translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace. [7]

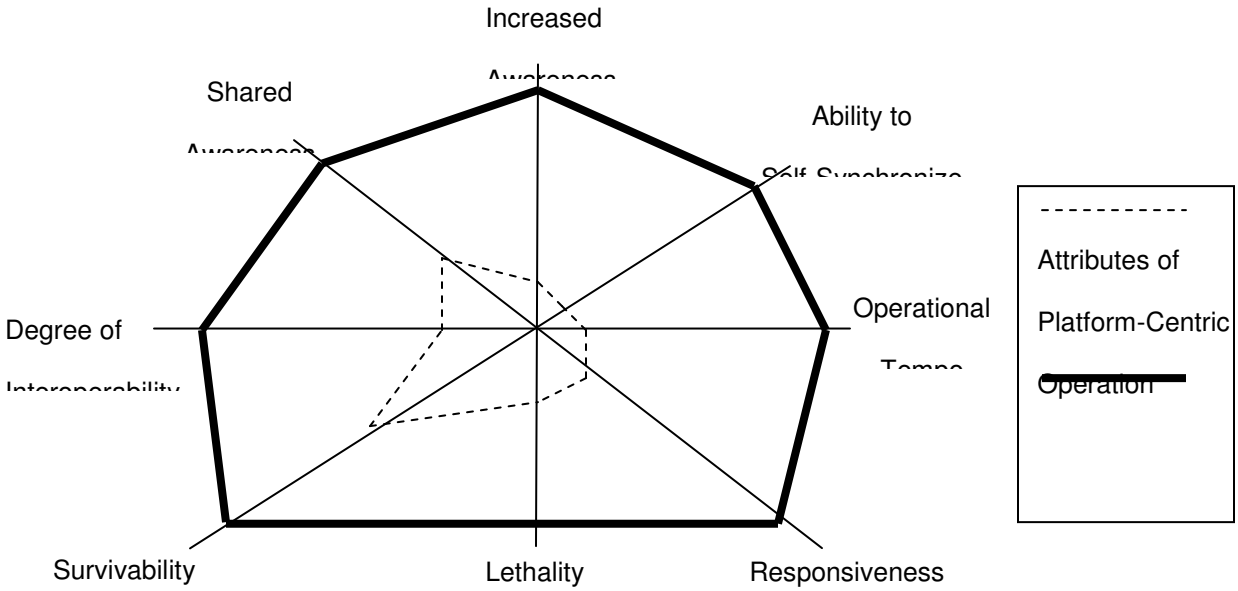


Figure 1 : Network Centric Warfare

Shooter or arrangement grids in the information network approach can help exploit the high levels of awareness that, in turn, generate increased combat power. This expansion in power can translate to massing of effects as opposed to the massing of forces, maximizing awesome joint combat strength. An information grid provides access for computing and communications but it also requires redundant, high data rate pipes that span the joint battle space. Another necessity is more effective integration of computation, communications and networking. [8]

Potential relationships between the proposed operational concepts of Joint Vision 2010, Information Superiority and Network Centric Warfare can be explored by examining operational architecture that effectively link sensors, command and control and shooters. Command and control elements and shooters suggest three potential building blocks : an information grid, a sensor grid and a shooter grid.

Information Grid. The information grid provides the infrastructure for network centric computing and communications. This infrastructure provides the means to receive, process, transport, store and protect information for the joint and combined forces. This grid provides the necessary infrastructure for plug in and plug out of the sensors and shooters. This grid will exist in space, in both low and high earth orbat, in

the air at all attitudes on land and under sea. This is a physical permanent grid. It consists of both military and commercial communication capabilities and transmits multiple information types in multiple modes at multiple data rates. Voice, data and video can be transmitted via a point to point or direct broadcast. Another key capability of information grid is information protection. The combination of these capabilities enables the information grid to provide the war fighter with ensured high speed access to the information required to dominate across all levels of conflict.

The Sensor Grid. The sensor grid is composed of air, sea, ground, space and cyberspace based sensors. Sensor grid elements include dedicated sensors, sensors based on weapon platforms, sensors employed by individual soldiers and embedded logistic sensors. The sensors grid provides the Joint Force with a high degree of awareness of friendly forces, enemy forces and the environment across the battle space. The sensors are physical and when tasked to produce information about a target they are inter related. This grid then exists for the task only and is reformed for every mission.

Shooter Grid. The operational architecture of the shooter grid enables the Joint War fighter to plan and execute operations in a manner that achieves an overwhelming effect at precise places and time. The shooter grid is like the sensor grid, in that its parts are physical but the grid is only virtual. The shooters are tasked to create the necessary effect on the battlefield then dynamically retasked as necessary.

Cooperative Engagement Capability (CEC). The US Navy's Cooperative Engagement Capability (CEC) employs network-centric concepts to increase combat power. Traditionally, each ship's radar would build incoming missile tracks independently, on the basis of what it saw. The CEC architecture increases combat power by networking the censor, command and control, and shooters of a Battle Group's platforms to develop a sensor grid and an engagement grid. The mission specific sensor grid embedded in CEC generates a high level of battle space awareness by fusing data from the multiple sensor to create a consolidated high accuracy track unobtainable with stand alone sensor. Passing the track to all ships in the Group permits each ship to engage a target on the basis of what other ships see , thus extending the battlespace and engagement of the incoming targets in depth with multiple shooters with an increasing probability of kill. [9]

There are several key concepts in the definition of NCW that merit emphasis. They are :-

- **Geographically Dispersed Forces.** In the past due to limitations of Armed Forces to communicate, move and project forces, the forces needed to be co-located or in close proximity to the enemy. As a result a geographically dispersed forces was relatively weak and was unable to respond quickly or mount a concentrated attack. With the information age technologies available the approach is now based on massing of effects rather the massing of forces. As the range of sensors and weapons increase, our ability to move information rapidly improves and geographical constraints diminishes. To generate or concentrate forces it is no longer necessary to physically

concentrate forces. This in turn reduces risk because we can avoid presenting the enemy with attractive, high value targets. A sensor or a shooter can now be in a position to engage many different targets without having to move.

- **Knowledgeable Force.** Empowered by knowledge Armed Forces will be able to self-synchronize, operate with a small foot-print and be more effective when operating autonomously. A Knowledgeable force depends on a steady diet of timely , accurate information and the processing power tools and expertise necessary to put battlefield information into context and turn it into battlefield knowledge.

- **Effective Linking Among Entities in Battlefield.** Dispersed and distributed entities will generate synergy and responsibility and work can be dynamically re allocated to adopt to the situation.

However, there is a word of caution. There is no guarantee that simply hooking things up will make the results better. There is every possibility that the unintended consequences of wiring up the battlefield and hoping for the best will, in fact, degrade performance particularly if doctrines , organization, training and other key elements of the process are not changed to take advantage of the new configuration.

Battlefield Awareness. Battlefield Awareness results from the fusion of key elements of information which characterize the battlefield. The elements are primarily explicit information such as position of forces, geography and weather. This type of information needs little interpretation and usually can be communicated quickly and easily. The difficulty comes in placing the information in a large context and understanding its implications. Sensors are key contributors to battlefield awareness.

Battlefield knowledge. Battlefield knowledge consists of tacit information. It requires interpretations. While facts can be easily transferred, the underlying organizing logic can seldom be transferred quickly and easily. Examples of tacit information include capabilities and tactics of an adversary, local customs and intent. Battlefield knowledge workers play a key role in developing, processing and communicating tacit information. To develop battlefield knowledge, experience and intellectual capabilities of commanders and staff and decision aids, simulation aid, knowledge (expertise) located at distance and forms of Artificial Intelligence (AI) and expert systems are utilized. Warfare takes on the characteristics of its age. NCW is the military response to the opportunities created by the information age. Network Centric Operations are military operations that are enabled by the networking of the forces. Networking the force entails much more than providing connectivity among force components. It involves the development of distributed collaboration process designed to ensure that all pertinent available information is shared and that all appropriate assets can be brought into effect by commanders to employ dominate maneuver, precision engagement, full dimensional protection and focused logistics. Warfare takes place simultaneously in and among the physical , the information and the cognitive domains.

DOMAINS OF WARFARE

To understand what is different about NCW, as well as to understand the source of increased combat power associated with NCW, one has to simultaneously focus on the three domains of warfare and the interactions among them. These domains are, the physical domain, the information domain and the cognitive domain.

Physical Domain. The Physical domain is the traditional domain of warfare. It is the domain where strike, protect and maneuver take place across the environment of ground, sea, air and space. It is the domain where physical platforms and communication networks that connect them reside. Comparatively, the elements of this domain are the easiest to measure and consequently, combat power has traditionally been measured primarily in the domain.

Information Domain . The information domain is the domain where information lies. It is the domain where information is created, manipulated , and shared. It is the domain that facilitates the communication of information among warfighters. It is the domain where the command and control of modern military forces is communicated , where commander's intent is conveyed. Consequently, it is increasingly the information domain that must be protected and defended to enable a force to generate combat power in the face of offensive actions taken by an adversary. And , in the all-important battle for information superiority , the information domain is ground zero.

Cognitive Domain . The cognitive domain is the domain of the mind of the warfighter and the warfigher's supporting populace. Many battles and wars are won or lost in the cognitive domain. The intangibles of leadership, morale, unit cohesion, level of training and experience, situational awareness and public opinion are elements of this domain. This is the domain where commander's intent, doctrine, tactics, techniques, and procedures reside.

NCW Force Attributes and Capabilities. A warfare force that can conduct Network Centric Operations can be defined as having the following attributes and capabilities :-

Physical Domain.

- All elements of the force are robustly networked achieving secure and seamless connectivity.

Information Domain.

- The force has the capability to collect, share , access and protect information.

- The force has the capability to collaborate in the information domain, which enables a force to improve its information position through processes of correlation , fusion, and analysis.

- A force can achieve information advantage over an adversary in the Information Domain.

Cognitive Domain.

- The force has the capability to develop and share high-quality situational awareness.
- The force has the capability to develop a shared knowledge of commander's intent.
- The force has the capability to self-synchronize its operations.

The central hypothesis of NCW is that a force with these capabilities can increase combat power by :-

- Better synchronizing effects in the battlespace.
- Achieving greater speed of command.
- Increasing lethality, survivability and responsiveness.

Network Centric Operations to date has focused on the tactical and operational levels of warfare, but they impact all levels of military from the tactical to the strategic. At the operational level, Network Centric Operations provide commanders with capability to generate precise war fighting effects at an unprecedented operational tempo, creating conditions for the rapid lockout of adversary's courses of action.

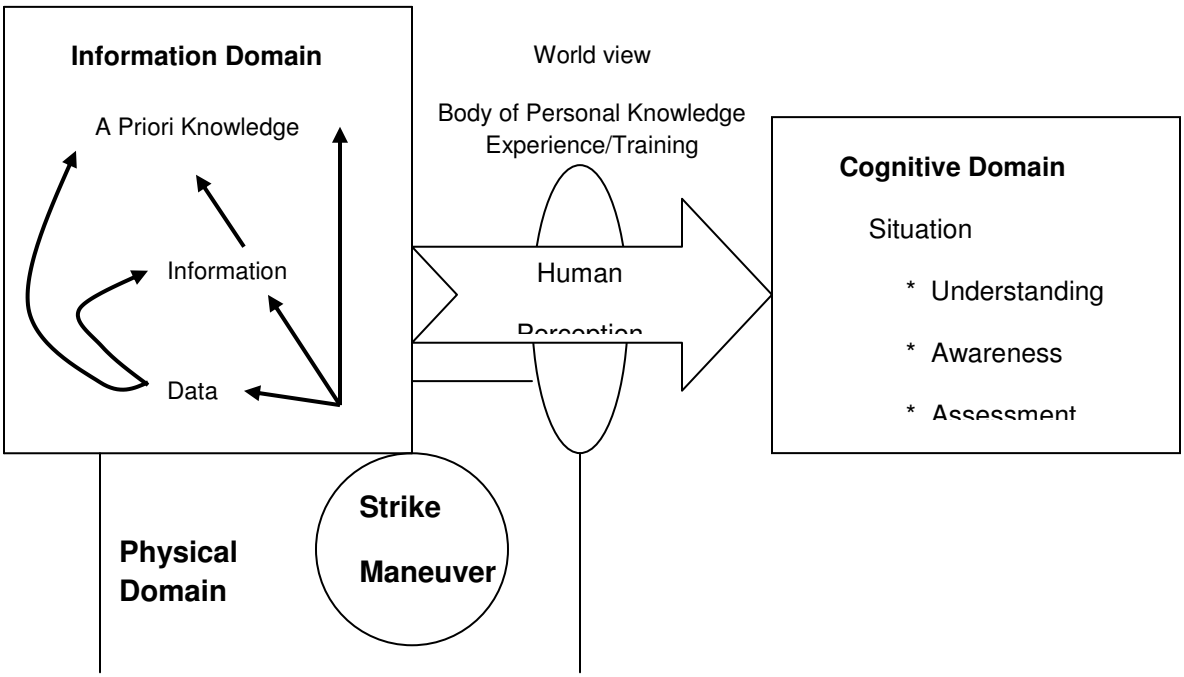
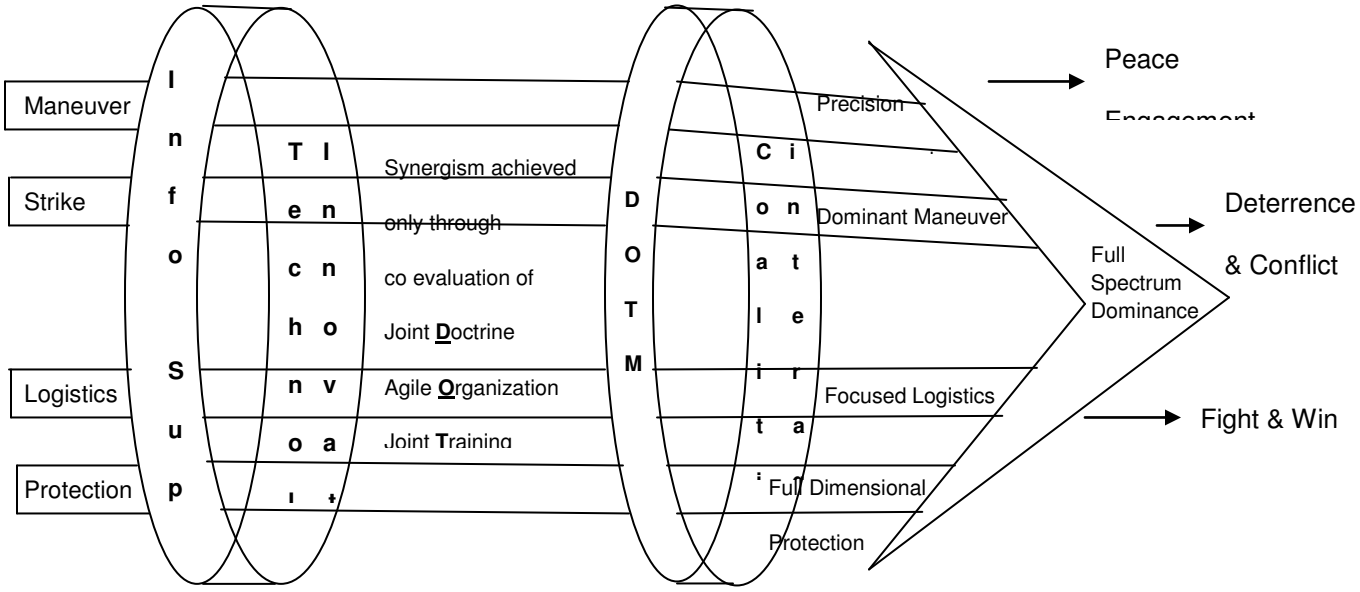


Figure 2 : Domains of Warfare

Joint Vision 2020, Information Superiority and NCW.

> In the future, war will not be waged by armies, but by groups whom today we call terrorist, guerillas, bandits and robbers but who will undoubtedly hit on more formal titles to describe themselves.
>
> - Martin Von Creveld, [10]

USA, the leading military power in the world has published a document Joint Vision 2020 which describes the ongoing transformation so that their Armed Forces become faster, more lethal and more precise in 2020. The overall goal of transformation is the creation of a force that is dominant across full spectrum of military operations. Realizing the potential of information revolution today's capabilities for maneuver, strike, logistic and protection will become dominate maneuver, precision engagement, focused logistics and full dimensional protection. Improved capabilities for joint C2 are key to achieving this goal. Attainting the goal will require steady infusion of new technology and modernization and replacement of equipment. The continuous development and proliferation of information technologies will substantially change the conduct of military operations. These changes in the information environment will make information superiority a key enabler of the transformation of the operational capabilities of the joint force and the evolution of joint command and control. The US Armed Forces will continue to rely on capacity for intellectual and technical innovation. [11]



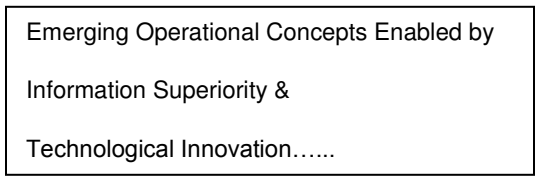


Figure 3 : JV 2020

Dominant Maneuver. [12] Dominant Maneuver is the ability of joint forces to gain positional advantage with decisive speed and overwhelming operational tempo in the achievement of assigned military tasks. Widely dispersed Joint air, land, sea, amphibious, special operations, and space forces, capable of scaling and massing force or forces and the effects of fires as required for either combat or noncombat operations, will secure advantage across the range of military operations through the application of information, deception, engagement, mobility, and counter-mobility capabilities.

NCW capabilities will support the conduct of dominant maneuver by enabling :-

* Adaptive and concurrent planning.

* Coordination of widely dispersed units.

* Gathering of timely feedback on the status, location, and activities of subordinate units.

* Anticipation of the course of events leading to mission accomplishment.

Precision Engagement. Precision Engagement is the ability of joint forces to locate, survey, discern, and track objectives or targets ; select, organize, and use the correct systems; generate desired effects; assess results; and reengage with decisive speed and overwhelming operational tempo as required, throughout the full range of military operations.

Simply put, precision engagement is effects-based engagement that is relevant to all types of operations. Its success depends on in depth analysis to identify and locate critical nodes and targets. The pivotal characteristic of precision engagement is the

linking of sensors, delivery systems, and effects. NCW concepts and capabilities effectively network sensors, command and control, and shooters to engage with precision across the depth and breadth of the battlespace.

The concept of precision engagement extends beyond precisely striking a target with explosive ordnance. Network Centric Warfare capabilities will enhance the capability of the Joint force commander to understand the situation, determine the effects desired, select a course of action and the forces to execute it, accurately assess the effects of that action, and reengage as necessary while minimizing collateral damage.

Focused Logistics. Focused Logistics is the ability to provide the Joint force the right personnel, equipment, and supplies in the right place, at the right time, and in the right quantity, across the full range of military operations. This will be made possible through a real-time, web-based information system providing total asset visibility as part of a common relevant operational picture, effectively linking the operator and logistician across services and support agencies. Through transformational innovations to organizations and processes, focused logistics will provide the Joint warfighter with support for all functions.

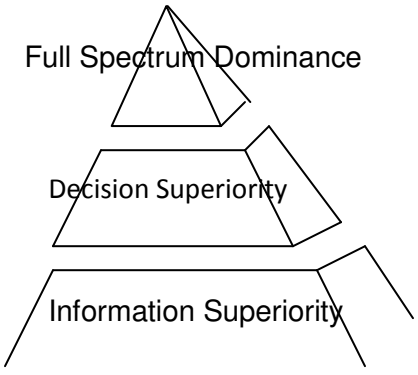
Focused logistics will effectively link all logistics functions and units through advanced information systems that integrate real-time total asset visibility with a common operational picture. These systems will incorporate enhanced decision-support tools that will improve analysis, planning, and anticipation of warfighter requirements. They will also provide a more seamless connection to the commercial sector to take advantage of applicable advanced business practices and commercial economies.

Full Dimensional Protection. Full Dimensional Protection is the ability of the Joint force to protect its personnel and other assets required to decisively execute assigned tasks. Full dimensional protection is achieved through the tailored selection and application of multilayered active and passive measures, within the domains of air, land, sea, space, and information across the range of military operations with an acceptable level of risk.

The capability for full dimensional protection incorporates a complete array of both combat and noncombat actions in offensive and defensive operations, enabled by information superiority. There is a critical need for protection of the information content and systems vital for operational success, including increased vigilance in counterintelligence and information security.

Global Information Grid (GIG). Joint Vision 2020 highlights the importance of U.S., Allied, and coalition forces achieving dramatically improved capabilities for operating in the information domain. The concept for achieving this capability to operate in the information domain is the GIG. It is described in Joint Vision 2020 as "…the globally interconnected, end to end set of information capabilities, associated processes, and people to manage and provide information on demand to warfighters, policy makers, and support personnel ".

The role of the GIG in enabling NCW, Information Superiority and ultimately full spectrum dominance is given in figure 4.



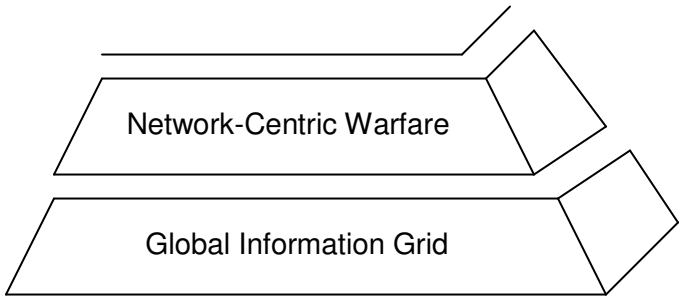


Figure 4 : The GIG as an Enabler

Army Vision on NCW.

The theory behind NCW is that by linking sensor networks, Command and Control (C2) networks we can achieve efficiencies in all military operations from the synergy that would be derived by simultaneously sharing information in a common operating environment. NCW emphasizes the following :-

* Timely relevant, accurate and precise information is required to automatically engage targets expeditiously with the most effective weapons and forces available.

* Using networked Intelligence, Surveillance and Reconnaissance(ISR) capabilities and predetermined decision criteria to support automated responses from the "network" to threats against individual platforms.

* Importance of situational awareness for both targeting and decision making.

* Value of information sharing, collaboration, synchronization, improved interoperability within the information domain.

* Information superiority and victory on the battlefield will be dependent on technological solutions that will help acquire, process, exploit dominate and protect information.

Some examples are :-

* Collaborative and simultaneous planning and execution among widely dispersed commanders and staff saves planning and travel time, allowing commanders to focus on information collection, decision making, and execution.

* Enroute mission planning and rehearsal among dispersed force elements prior to deployment, enroute, and in theatre.
* Command and Control on the move allows commanders the freedom to move to critical points on the battlefield.

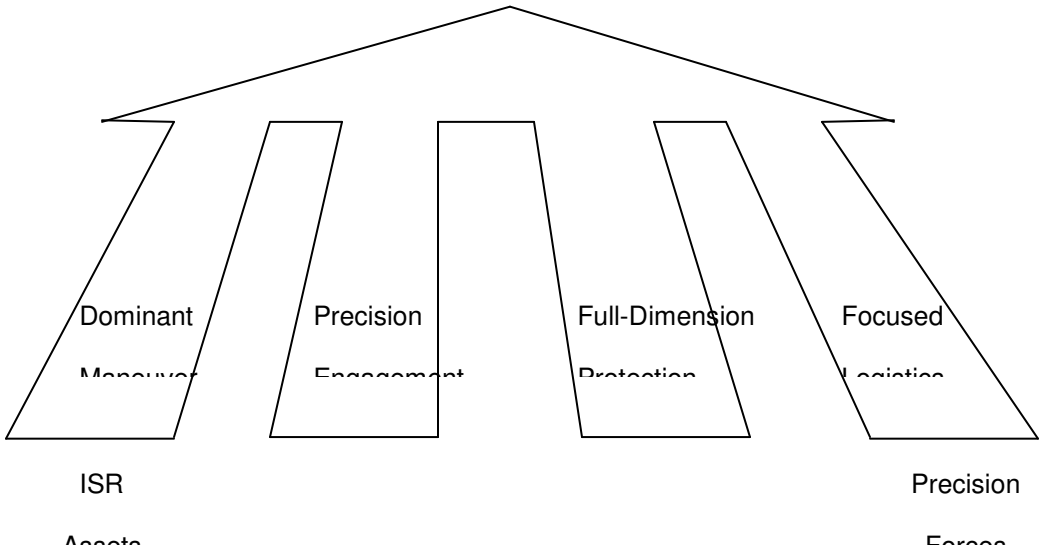
* Split-based operations reduces the number of staff and support personnel required to be deployed to theatre thus reducing the associated Tactical Operations Center footprint.

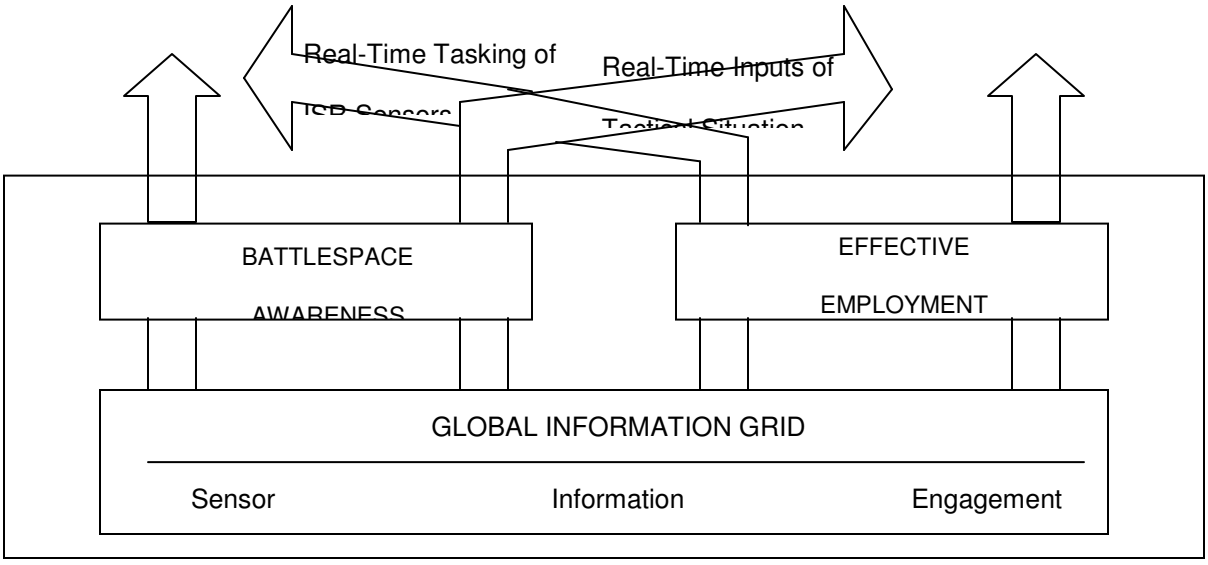
* Virtual support services support deployed forces from centers of knowledge across the country.

* Distance learning and Knowledge Centers provide warfighters access to education, training and knowledge.

* Integrated and layered Intelligence, Surveillance and Reconnaissance (ISR) allows commanders, staffs and analysts worldwide to collaborate in the development of real time combat information and near real time, predictive intelligence products for the warfighter.

New Concepts To Achieve
Operational Dominance





The Concept of Information Superiority as Described in US Joint Warfighting Science and Technology Plan

Organisation for Network Warfare. Information networks will enable soldiers at the lowest levels to know as much as the most senior commanders about the combat situation throughout an entire theatre of operation. The result of this information networking will be a decentralization of command authority with individual war fighters empowered as never before. It would offer unprecedented opportunities for initiative and independent operations by individuals and small units. Some suggest that the ultimate combat organization as a network of distributed systems with individuals nodes exchanging information laterally and acting independently in pursuit of common system goals – an organization essentially freed from centralized authority altogether. [13]

But these types of organizations are unlikely. Emerging information technologies in fact reverse the trend forwards centralization and relative reduction in command authority.

Terrorism and Netwar.

Terrorism seems to be evolving in the directions of violent networked organization. Islamic fundamental organizations like Hamas and the Bin Laden network consist of groups organized in loosely interconnected semi independent cells that have no single hierarchy. All the recent terrorist groups like Osama Bin Laden led Arab Afghan movement, Islamic Group (IG) of Egypt and Armed Islamic Group (GIA) share the principles of networked organization-relatively flat hierarchies, decentralization and delegation of decision making authority and loose lateral ties among dispersed groups and individuals. For example Bin Laden led terrorist organization Arab Afghans are part of a complex network of relatively autonomous groups that are financed from private sources forming “a kind of international terrorist ‘Internet’ ”. Osama Bin Laden used his

wealth and organizational skill to support and direct a multinational alliance of Islamic extremists. At the heart of the alliance is his own inner core group known as Al-Qaeda (the base), which sometimes conducts missions on its own, but more often in conjunction with other groups or elements in the alliance. Bin Laden specifies that holy war against the USA and the West will be fought by irregular, light and highly mobile forces using guerrilla tactics. A study with inputs from various researchers, "Special Report : Al-Qaeda" in Janes Intelligence Review, [14] provides an extensive analysis of Al-Qaeda's organizational structure, history and activities. The analysis views Al-Qaeda as a kind of "Conglomerate" with both formal vertical and informal horizontal elements, making it a partial hybrid of hierarchical and network forms of organization.

Use of IT by Terrorists. Information Technology (IT) is an enabling factor for networked groups. Terrorists use IT to coordinate and support their activities. The greater the degree of organizational networking in a terrorist group, the higher the likelihood that IT is used to support the network's decision making. Recent advances in IT facilitate networked terrorist organizations because information flows are becoming cheaper, more secure and more versatile. According to reporters who visited Bin Laden ; headquarters in a remote mountainous area of Afghanistan, the terrorist financier has compilers, communication equipment and a large numbers of disks for data storage. Egyptian 'Afghan' computer experts are said to have helped devise a communications network that relies on world wide web, e-mail and electronic bulletin board so that the extremist can exchange information without running a major risk of being intercepted by counter terrorism officially.

ORGANIZATIONAL IMPLICATIONS

> We must build forces that draw upon the revolutionary advances in the technology of war….one that relies more heavily on stealth, precision weaponry and information technology
>
> - George W Bush, Commander In Chief of US Armed Forces, 25 May 2001

The information revolution challenges the design of many institutions. It disrupts and erodes the hierarchies around which institutions are normally designed. Military, traditionally, is an institution which field armed forces. The form that all institutions normally take is the hierarchy. Military in particular depend heavily on hierarchy. The classic example of an ancient force who were organized more like a network than a hierarchy is perhaps the greatest warrior of all-the Chenghis Khan and the Mongols. A relatively minor military power, the combined forces of North Vietnaum and the Viet Cong that fought and defeated a great power, the USA, operated in many respects more like a network than an institution. In recent times the international terrorists, guerilla insurgents, drug smuggling cartels, ethnic factions as well as racial and tribal

gangs-------are all organized like networks. Although their leadership may well be hierarchical. These organizations are innovative, flexible, exhibit shared goal, focus on core competencies and are difficult to counter. Creativity is enhanced because individuals are not bound by doctrine and are free to innovate or experiment with new techniques. Perhaps the reason that military institutions are having difficulty in Low Intensity Conflicts is because they are not meant to be fought by institutions. The lesson is institution can be defeated by networks. It may take networks to counter networks.

There are serious implications of the proposed Network centric concept for the organizational structure. Should military be organized as a true network in which self-synchronization, synergy and speed of action replace the traditional hierarchy characterized by deliberate planning, experience and command and control ? Will this new system prove effective across the entire spectrum of conflict ? Without a well developed Concept of Operation (a plan) it will be impossible for the network centric commander to provide anything other than very general statistic analysis. Today there is a school of thought that technologically superior networked organization endowed with a blinding speed should replace hierarchical command system that are not sufficiently "responsive" to compete in the information age.

Hierarchical Organisation. One of the advantages of hierarchy is its standardization. It facilitates a certain predictability allowing an organization to assimilate large number of new personnel to remain effective with high turnover in the event of casualties. Unit structure is predictable and repetitive allowing interchangeability and facilitating task organization of groups of units. Knowledge, technique and experiences gained from past endeavours is retained by the senior personnel and passed to the lower echelons of the organization often in an informal manner.

Authority for independent action can be delegated in the organization but responsibility cannot . A Commander is always held responsible for the outcome regardless of whether a flawed decision was his own or that of his subordinates. The commander furnishes subordinates with guidance in the form of Rules of Engagement (ROE), tactical decision aids, administrative procedure etc. As the organization grows and commander's ability to supervise is impaired by geography , communication or sheer numbers, additional layers are inserted in the organization. These additional layers enable communication and processing of vast quantities of information but the opportunity for a disconnect between the intent of the commander and the action of the trigger-puller increases proportionally. Thus from the commander's perspective it is advantageous to have the fewest layers and the flattest organization possible.

The operational chain of command insulates the operators from the higher degree of uncertainty that often prevails at the highest level of organization. Not all the instructions that starts at the top are passed to the lowest levels of the organization. The personnel who man the intermediate echelons, experienced operators themselves, may detect flaws or potential problems and either modify the plan or recommended an alternate course of action. This optimizes the lowest functional

levels allowing for their concentration on daily operations while centralized longer range planning is conducted by dedicated staff at a higher echelon.

However, when not properly managed a hierarchy can become overly regimented, notoriously slow and cumbersome. Operational, functional and contingency plans are laboriously prepared, chopped and reshaped up and down the chain in an effort to purge errors and minimize risk prior to execution. Poor lateral communication within the organization worsens the situation.

Nerworked Organisation. The information revolution is favouring and strengthing network froms of organization often giving them an advantage over hierarchical organization. Unlike hierarchical organizations, networked organizations offer decentralized control orientation that makes better use of information technology. In a networked organization, the information gathering process will be more equally distributed and more information will be available more rapidly to all levels of command. Commanders will share rather than control information, resulting in faster decision making at all levels of Command.

Problem of Network Organisation. While a networked organization may be ideal for sharing information gathering it may not be the best model for military commanders when dealing with tough decisions in combat. Unlike their business counterparts, military commanders must really make life and death decision and put subordinate at risk. In a networked organization, who among the collaborators will make these decisions ? War requires commanders not collaborators. Thus decision making may be more a hierarchical function than information gathering. Some type of hierarchical organization is required to support the decision making process.

Combination of Both Forms. Networked form of organization in not about technology. Current improvements in communications technology have enhanced the performance of both hierarchical and network organizations but in neither case does technology dictate structure. There is a danger in advocating emphasis on concept of speed and precision as panacea. Before we trade off our command structure and abandon the enduring flexibility and redundancy it has traditionally provided we must consider our new course carefully. Due to multi-mission nature of today's weapon and sensor systems the hierarchy must continue to exist at the operational level and above. No other system of human interaction has the proven ability to prioritize the configuration and distribution of resources in military application. At the tactical level the most prudent course of action is to continue the evolution of military processes through careful application of commercially available technology to localized task specific networks.

DICHOTOMIES

Access/Security Trade off. If shared battlefield awareness can provide a critical and decisive advantage opponents will find that the data infrastructure and the data

themselves make exceedingly valuable targets. There is a dilemma between easy access and robust security. Networks are supposed to have a seamless quality. Once in the network one can see almost everything. An adversary who has gained access will be able to steal, change or destroy critical information freely and swiftly. By contrast within a traditional hierarchical organization an opponent that impersonates an infantry soldier would have great difficulty discovering essential information simply because his rank would restrict access. The very nature of non-hierarchical information system means that the penetration of one point of defence could provide access to enormous amounts of information or even unleash havoc throughout the information system.

Insurgency/Guerilla Warfare. The insurgent forces using terrorism as a tactic require relatively little information , most of them not even time sensitive. They can plant bombs, lay mines and set ambushes without knowing when they will actually launch attacks and often without concern about collateral damage. Conventional forces fighting them need quite precision information in order to locate and defeat them. Even more information is needed if collateral damage which often alienate the general population is to be avoided. This information can be exceptionally difficult to obtain and keep up to date. In these situations the more conventional force often finds it advantageous to adopt its tactics in order to reduce its dependence on information.

Time. One of the fundamental changes which NCW espouses as central to its increased efficiency and effectiveness is speed of command. While it may be intuitively obvious that being able to act before your adversary is important, does faster command equal better command ? Will future commanders measure their success not on what they accomplish, but how quickly ? Will potential preoccupation with speed lead to shortcuts and poor decisions made quickly ? We must avoid being sucked into the belief that more data, over faster networks can be intelligently engineered to reduce the complexities of decision making and reduce the OODA Loop. Nor will it reduce the importance of experience and judgment. Numerous studies over the past years have suggested that experts in various fields use intuition as the basis for decision making rather than the formal analytical model. Taken to extreme, preoccupation with speed of command could add an additional element of friction to the conflict equation, the enemy does not have time to react and we end up reacting to our own action.

Bandwidth Dilemma. Gordon Moore, co founder of Intel had predicted that performance of computers would double every 18 months which remains true till date. However, in Network Centric Computing computer is the network and this makes the communication the key. Moore's law is no longer the driving force of progress in information technology, instead it is the bandwidth. Bandwidth is the capacity of an information channel to transmit bits without errors in the presence of noise. Bandwidth is now doubling every year. Though Optical Fiber Cable has immense capacity of bandwidth expansion wireless bandwidth capacity will have fundamental limits which will adversely affect mobile users. In planning and conducting network centric operations warfighters will need to have an insight and understanding into the bandwidth costs of their activities. The broad dictum that a video conference link costs a

headquarters 16 telephone links indicates that trade off will need to be made when choosing interconnections on the nets.

Decision Making. Technocrats argue that advances in automated decision making technologies will replace the human in the loop enabling the order of magnitude increase in speed of command. There is a proposal to remove the commander from the loop when conducting precision fire by permitting artificial intelligence to make the combat decisions while the commander serves as over rider. The solution overlooks the probability that a thinking opponent is trying to deceive the commander. The commander has traditionally relied on experience and intuition to shape his course of action. Artificial Intelligence and decision templates have no such intuition, nor do they possess much capacity for initiative to exploit a developing opportunity. Technology promises much – the paperless office, the perfect intelligence picture, the rapid destruction of enemy forces, the Collapse of Civilian morals –but it rarely delivers. [15] But it raises the following questions :-

* Who inputs data and in what form ? If the information acquired does not fit the designed format is it discounted or do we "trim the feet to fit the shoes" ?

* If more automation is employed to reduce the processing of data and speed up the decision cycle, will certain actions or alternatives be automatically filled out or discounted due to their implausibility or irrationality ? Will the network centric commander of tomorrow dismiss the idea of a German offensive through the Ardennes much like his French counterpart of 1940 ? We must recognize that data and information do not equal knowledge.

* If sensors and shooters are tied together to enable us to scan the battlefield, sift for targets, prioritize and strike then automatically who will be responsible? Will unit commanders have weapon release authority or will they simply be the pawns on a command centre chessboard.

Self Synchronization. One of the fundamental principle of successful transformation to network centric operation is self synchronization. By empowering troops via the common operational picture they will be able to act more quickly and decisively to enhance both the speed and continuity of operations. This also implies a decentralization of control downward what has been termed decentralized empowerment – and a flattening of hierarchies. Self synchronization has the following hurdles to overcome. [16]

* Can we actually improve the creation and implementation of mission statements, commander's intent and Rules of Engagement so that ambiguities will be removed, empowering forces to act on their information with little direction ?

* Will senior military and political leaders be able to provide subordinates their missions, guidance/ROE, intent and cut them loose ?

CNN Effect. In a world which has been shrunk by CNN effect where individual tactical engagements can have strategic and therefore political implications the temptation for interference from above may prove to be too great. Will it be possible to carryout a company or Infantry Battalion level operation in a sensitive place like Hazrat-Bal shrine in full media glare without any interference from top ?

Fog of War. Will we recognize information dominance when we see it or will commanders wait in search of better or more complete information ? Will we lift the fog of war as advertised or make it thicker as more and more information arrives faster and faster, overwhelming commanders with too much noise to discern the signal. Friction- chance, luck, uncertainties, uncontrollable passions and irrationality - is constant in war and the very nature of interaction is bound to make it unpredictable. We must not underestimate the role of intangible factors in war and search for linear answers to the non linear battlefield of future.

Information/Knowledge collected and culled through a sophisticated system cannot provide perfect knowledge and unless specifically designed will fail to convey a discrete list of information required to make timely, accurate decisions. This is especially true under the chaotic, stressful and time sensitive conditions (fog and friction) that permeate warfare. The Vincennes shoot down of the Iran Air Flight 655 is a good example of sensory overload.

Technology. Technology is supposed to serve the users needs. Field positions are frequently selected to accommodate technology rather than for advantages of the terrain. Often the best combined arms solution will not be able to employ the full parameters of the new system's capabilities. For example the new artillery that outranges forward observer's ability to observe and body armour that protects a soldier but is too heavy to fight in. The FM tactical radio that can transmit and receive for a distance of 30 Km over open ground cannot communicate two blocks away in a city full of high-rise buildings.

How the infostructure and C2 architecture adapt to the threat of asymmetric warfare has to be seen. In 1999 USA could not accomplish information dominance in their war with technologically unsophisticated Serbians. US failure to gain information dominance in Kosovo makes one question whether information superiority, to the extent envisioned, is probable or even possible due to the fog and friction of war. [17] An unsophisticated adversary in Serbia destroyed numerous UAVs with dumb weapons, deceived satellites through use of decoys and camouflage and overcame the destruction of their LOC by employing landmines and cellular phones.

RECENT EXAMPLES

Afghanistan. In Afghanistan the US military was able to deploy and operate a constellation of sensor systems. This constellation included photographic and electronic intelligence satellites, E-3 Airborne Warning and Control System (AWACS) aircraft Joint STARS, the RC-135 Rivet Joint electronic intelligence collectors, P-3 Orion aircraft, Predators and the new long-range, high-altitude RQ-4A Global Hawk UAV, along with stalwarts such as the EA-6B Prowler, S-3B Viking and F-14 and F-16 fighters with targeting pods.

The use of multiple sensors allowed for increased refinement of ISR information. Satellite imagery would suggest a search area for the Joint STARS, the results of which would be used to key a Predator UAV that provided targeting quality pictures to strike platforms. UAVs also have the advantage of extended loiter times over the battlefield.

The vast array of sensors was tied together with communications linked that permitted an unprecedented connectivity not only between sensors and shooters but between decision makers to shooters as well. Officers in the Combined Air Operations Center (CAOC) at Prince Sultan airbase in Saudi Arabia watched live video feed from Predators over Kunduz or Kandahar. B-52s could target their weapons based on information that developed while they were in flight, allowing them to provide close support to forces on the ground. Special Operations units routinely provided real-time targeting information to fighters and bombers overhead via laser rangefinders, GPS receivers and secure communications channels. The Predator supplying pictures to the CAOC was, at the same time, feeding that same information to AC-130 gun-ships operating in Afghanistan. “In the war itself, what has changed is a real strong appreciation of the value of ISR and the real-time value of being able to target rapidly”.[18]

Resistance to Change. Armed Forces across the world have understood the need to transform to meet the demands of information age warfare. However, significant organizational barriers to the adoption of new technology, doctrine and organizations exist. The services are reluctant to take measures that are disruptive of service culture such as shifting away from traditional platforms and towards new weapon systems, concepts and organizations.

The US Navy began exploring concepts that would replace large platforms with a network of smaller and less vulnerable systems. The concept of STREETFIGHTER-a family of small platforms designed to gain and sustain access to the littoral region in the face of a strong resistance was examined. They were also exploring the use of fast catamarans to deploy and sustain amphibious forces.

These ideas have drawn fire from officers who see them as a threat to existing surface ship programmes. STREETFIGHTER represents a challenge to US Navy’s current approach to force structure which emphasizes a relatively large number of large, highly capable ships. Rather than conducting rigorous analysis of the benefits and limitations

of such platforms, the idea is coming under fire. Vice Admiral Dan Murphy, the commander of the sixth fleet in his remarkably blunt criticism said, "It is a wild idea. There is nothing behind it. There is no analysis. You know, Vice Admiral Cebrowski dreamed up a bumper sticker, but what in fact he is talking about, to go into littorals to get into tough situation, to fight your own way through and deliver power is exactly what we are doing". One Admiral said, " If the next major naval better is fought in New ports Narragansett Bay, Streetfighters will be decisive". [19]

INDIAN SCERARIO

Indian Armed Forces are like dinosaurs, not able to move with times. American and British Special Forces were roaming behind enemy lines and illuminating targets by laser designators for the Air Force to destroy targets in Afghanistan not too far from our North Western borders. We are following the 1945 version of the concept when Air Force officers called Forward Air Controllers (FAC) move ahead of the army and call in a strike ahead of the advancing troops. What happens when there is no front line and we go in for "hot pursuit" ? The laser designated counter terrorist strike is not the magic bullet, but the failure to induct it along with a dozen other capabilities is symptomatic of an alarming doctrinal, tactical and technological obsolescence. [20]

Ask any of army's formation commanders about battlefield transparency and one can almost predict the expletives that may come from them. In an article in Indian Express on 08 April 2002 [21] Lt Gen Vijay Oberoi (Retd) the recently retired Vice Chief of the Army Staff urged for procurement of sensors of various types like thermal, infrared, acoustic and image intensification devices, radars, Unmanned Aerial Vehicles and tethered balloons. Army urgently requires direct firing heavy caliber weapons for precision shooting at targets across LOC, light and more lethal automatic weapons, light weight rocket launchers, specialized grenades of various categories, body armour, armour protected light vehicles, modern binoculars and compasses, sniper rifles and light weight radio sets and communication equipment.

CONCLUSION

The conjunction of sensors, weapons and C2 processes in NCW will undoubtedly improve our ability to conduct conventional warfare more efficiently and jointly. However, claims of eliminating risk, casualties and friction from war are utopian. NCW utility in a Military Operations Other Than War (MOOTW) environment is also suspect. The revolutionary possibilities of network centric operations will not be new technologies but how we integrate them in a synergistic relationship so that they shape, and are shaped by doctrine, operational concepts and organizational adaptation. Older forms of warfare are likely to persist alongside the new. Speed will be critical to success but numbers and endurance will also count.

In order to take advantage of new technologies of the future we need to be fully engaged now, looking not only for answers but also critically assessing our ideas, concepts, organization and the fundamental tenets of our military culture. Successful

adoption of NCW requires a cultural change. It cannot be achieved without widespread discussion, debate, experimentation and ultimately broad acceptance.

BIBLOGRAPHY

1. COAS, Batcheet No 3, Oct 98.

2. Fred P Stein, Observations on the Emergence of Network Centric Warfare, Network Centric Warfare Information Paper available at www.dtic.mil/jcs/j6/education/warfare.html. Also see www.dodccrp.org/steinncw.html.

3 Capt James R FitzSimonds, The Cultural Challenge of Information Technology, Naval War College Review, Summer 1998, p 9-21.

4. V Adm Arthur K Cebrowski, USN and John J Gastka, Network Centric Warfare : Its Origin and Future, Proceedings of the Naval Institute 124 : 1 (Jan 1998), P 28-35.

5. David S Albert, John J Garstka and Frederick P Stein, Network Centric Warfare : Developing and Leveraging Information Superiority, 2nd edition (Rev), Washington DC, CCRP Press, 1999, available at www.dodccrp.org/publicat.html.

6. Network Centric Warfare, Department of Defense Report to Congress, 27 Jul 2001 is available in www.c3i.osd.mil/ncw.

7. Information Superiority : Making the Joint Vision, available at www.c3i.osd.mil/ncw/ info superiority/.

8. Arthur K Cebrowski, ibid.

9. Group Captain Peter Layton, Network Centric Warfare : A Place in Our Future, Aerospace Centre Paper Number 74, available at www.defence.gov.au/Aerospace Centre/ Aerospace Center.html.

10. Martin Von Creveld, The Transformation of War, New York : The Free Press, 1991.

11. Joint Vision 2020. Available at www.dtic.mil/JV2020. Also see Enabling Joint Vision, available at www.dtic.mil/jcs/j6/Enabling JV.pdf.

12. NCW, DOD Report to Congress, ibid.

13. David S Albert et al, ibid.

14. Special Report : Al-Qaeda, Janes Intelligence Review, August 2001, pp 42-51.

15. Jacob W Kipp and Lt Col Lester W Gran, The Fog and Friction of Technology, Military Review, Sep – Oct 2001.

16. FitzSymonds, ibid.

17. Timothey L Thomas, Kosovo and the Current Myth of Information Superiority, Parameters, Spring 2000, P 14.

18. Daniel Goure, Briefings : Intelligence, Surveillance and Reconnaissance, Janes Defence weekly, 27 Feb 2002, pp25-26. also available at www.janes.com.

19. Thomas a Mankhen, Transforming the US Armed Forces, Rhetoric or Reality ? Naval War College Review, Summer 2001.

20. Raja Menon, We Can, But Don't, Outlook, 11 Feb 2002. p12. Also see Raja Menon, Bumblings at the Border, Times of India, 14 Feb 2002.

21. Lt Gen Vijay Oberoi, Army Modernisation : It's Time to Dust off The Rust, Indian Express, Chandigarh, 08 Apr 2002, p9.

RECOMMENDED READING

1. Thomas PM Barnett, The Seven Deadly Sins of Network Centric Warfare, US Naval Institute Proceedings, Vol 125, No 1, Jannuary 1999.

2. George Kasten, Building a Beehive : Observation on the Transition to Network-Centric Operations, Naval War College Review, Autumn 2000, available at www.nwc.navy.mil/Press/Review/2000/autumn.

3. Admiral Paul Reason and Davia G Freymann, "New Port Report Number 13 : Sailing New Seas" , Naval War College Press, available at www.nwc.navy.mil/press/npaper/np13.

4. John Arquila and David Ronfeldt, In Athena's Camp : Preparing for Conflict in the Information Age, Chapter 2, Rand, Santa Monica.

5. Lt Gen C Norman Wood, Network Crucial Key to Information Superiority, Signal, July 1997.

6. John J Garstka, Network Centric Warfare : An Overview of Emerging Theory, PHALANX, December 2000. available at www.mors.org/publications/phalanx/Dec00/.

7. Commander William K Lescher, USN, Network Centric : Is it Worth a Risk, USN Institute Proceedings, 1999 Publised in USI Digest Vol III, No 5 Sep 2000-Feb 2001.

8. Timothey L Thomas, Human Network Attacks, Mil Review, Sep - Oct 99.

9. Captain George Kaster, Building a Beehive – Observations on the Transition to Network Centric Operations, Naval War College Review, Autumn 2000.

10. Edward A Smith, Network Centric Warfare, What's the Point ? Naval War College Review, Winter 2001.

11. Captain Rober C Rubel, War Gaming Network Centric Warfare, Naval War College Review, Spring 2001.

12. Capt John W Bodner and 2/Lt Rebeeca Dengler, The Emergence of a Command Network, Naval War College Review, Autum 1996.

13. Lt Col Frank J Caravella, Achieving Sensor-to Shooter Synergy, Military Review, Nov-Dec 2000.

14. Jenkins, James T, Use Technology, BUT DON'T TRUST IT, US Naval Institute Proceedings, August 1998, pp 68-70.

15. Cdr William K Lescher, Network Centric : Is it Worth the risk ? US Naval Institute Proceedings, Vol 125, No 7 (July 1999) pp 58-63.

16. Cdr Alan D Zimm, Human Centric Warfare, US Naval Institute Proceedings, Vol 125 No 3 (May 1999), p 28-31.

Published in Pinnacle September 2001 issue.