Adapting the Military to Net-Centricity

P C Katoch

Networking is becoming more and more vital to business enterprises. Similarly, net-centricity, the enabler to net-centric warfare capabilities, is important to the military. More importantly, networking in the military is far more challenging than industry networking since the former is heavily dependent on wireless communications, with heavy demand for security, and requires robust resistance to hostile actions. Net-centric warfare is an information superiority enabled war-fighting concept that generates increased combat power by robust networking of sensors, decision-makers and shooters. Net-centric warfare allows the armed forces to evolve a confluence of weapons, sensors and decision-making, all of which ride on information superiority. Information advantage is achieved by the military through this approach to warfare designed to achieve multi-dimensional integration and synergy. Sharing of information enables a force to optimise the full potential of dominant manoeuvre, precision engagement, full dimensional protection and focussed logistics.

Net-centric warfare is the enabler that facilitates the shift from attrition style warfare to faster and more effective concepts of speed of command and precision/ synchronisation. In addition to technological improvements, net-centric warfare requires continued evolution of policy, strategy and concepts, organisational adjustments, doctrine, training to sustain development of information advantage and more importantly, a net-centric warfare culture. The basis of net-centric warfare is the premise that the power of a force grows proportionate to the extent of networking that is prevalent among the weapons, sensors and the command and control elements. The impact of net-centric warfare capabilities may be gauged from the fact that in Iraq in recent years, the US armed forces have had

Lieutenant General **P C Katoch** is Director General, Information Systems, Army HQ.
(N.B. The suggestions and views expressed in the article have been made by the author in his personal capacity and do not have any official endorsement.)

Net-centric warfare is the enabler that facilitates the shift from attrition style warfare to faster and more effective concepts of speed of command and precision/ synchronisation.

to deploy less than half of the ground forces and two-thirds of the air assets used in Desert Storm a decade plus ago.

The network war-fighter has to simultaneously focus on the physical, information and cognitive domains, plus the interactions among them. The physical domain is the traditional domain of warfare where physical weapons and units and communication networks that connect them reside. Elements of this domain are easiest to measure, and traditionally combat power is measured like this. All elements of the force must be robustly networked, achieving secure and seamless connectivity. Information domain is the domain where information lies. It facilitates communication of information among war-fighters and communication of command and control of the commanders. It must be protected to enable the generation of combat power in the face of enemy information attacks. The force must have the capability to collect, access and share information, improve its information position through fusion and analysis and achieve information advantage over the enemy. The cognitive domain is the domain of the mind of the war-fighter. Many battles are won or lost in this domain. All the intangibles like leadership, morale, unit cohesion, training experience, situational awareness, etc are elements of this domain. Here the commander's intent, doctrine, tactics, techniques and procedures reside. The force must develop and share high quality situational awareness, must have a shared knowledge of the commander's intent and must self-synchronise its operations. While command and control processes in net-centric warfare span the physical, information and cognitive domains, information systems are at the very heart of these. Support layers are available in the form of knowledge bearers, information bearers and data bearers.

Net-centric warfare operations exploit state-of-the-art science and technology to integrate widely dispersed human decision–makers, situating and targeting sensors, weapon platforms and field forces into a highly adaptive, comprehensive system of systems to achieve unprecedented mission effectiveness. For exploiting science and technology and to apply a technology-oriented framework, net-centric warfare should have the ingredients of surveillance, information, command and engagement grids. The surveillance

grid rapidly generates battlespace awareness and self-synchronisation. The information grid is a high performance network that provides the back plane for computing and communications. The basic level requirement for net-centric warfare is a high performance national information grid (which should be part of the global information grid) that provides a backbone for computing and communications across the spectrum. But this remains only a potential capability until we develop the appropriate software, capture the required data, have the organisational set-up, human resources and doctrines to exploit this capability. This is all the more vital when we are required to cope with asymmetric warfare situations, as was demonstrated during the 26/11 Mumbai terrorist attack. The command grid is principally the province of human decision-makers but it could include knowledge-based artificial intelligence and software applications that act as command advisers and are able to recommend courses of actions. The engagement grid exploits the awareness and translates it into increased combat potential. The sensor grid observes, the information grid orients, the command grid decides and the engagement grid acts. To achieve mission objectives, the grids must interact and exchange information. It, therefore, emerges that net-centric warfare is a multi-disciplinary process that can only be implemented by harnessing the available information and communication technologies. Implementation of such concept naturally lends itself to challenges that we need to overcome.

For exploiting science and technology and to apply a technology-oriented framework, net-centric warfare should have the ingredients of surveillance, information, command and engagement grids.

A shift from platform-centric to net-centric warfare implies a major change in terms of manoeuvre, mass, firepower and logistics. The latter's battlespace is flatter, synchronised,has fluid boundaries, compressed, open access to information, interactive and with coordinated data collection. The difference between network-centric and past operations is very clear. The latter process is largely centralised and sequential, with information passed through messages and with limited common situational awareness and ability to adapt in time. In sharp contrast to this process, the network infrastructure enables shared situational awareness and decentralised planning and execution, with potentially greater ability for rapid adaptation and improved speed of

command. Essentially, there is a paradigm shift in the battlefield. The erstwhile decision support system is transforming the decision assistance system, with increasing dominance of intelligence and computers to tackle the complexity of the system. In net-centric warfare, decision-makers, sensors and shooters work collaboratively and consistently, in response, to the dynamics of the battlespace, to achieve the commander's mission. However, we need to understand that net-centric warfare is not narrowly about technology, but broadly about an emerging military response to the information age and technology misapplied within an organisation only guarantees failure.

During the next decade, the focus of the military will continue to be on leveraging emerging technologies to integrate dispersed sensors, networks and weapon systems. The thrust areas for technology and implications on acquiring net-centric warfare capabilities are sensors, networks, weapons and integration. Sensors collect data directly and remotely, process it to produce knowledge using clustered computers and disseminate the processed knowledge to operators. Future trends include advanced platforms like high altitude, high endurance unmanned aerial vehicles (UAVs), intelligent unattended ground sensors and high resolution imaging satellites. There is a definite requirement of dedicated military satellites for comprehensive sub-metre resolution, capable of rapid launch, invulnerable to interception, and for precision engagement, including at the extreme periphery of the area of military operations. Superior technology networks assist soldiers to take better and quicker decisions. They assess information depending on the scale of embedded processing technology. Inter and intra-Service networks need designs with compatible and upgradeable algorithms, secure backbone and geographically dispersed and carefully positioned nodes with open system augmentations. Incorporating emerging networking technology capable of 'autonomous detection, reaction and restoration' mechanisms is needed. The immediate necessity is a stable communication network which will allow interoperability of the highest order amongst all the constituents of the war-fighting machinery. Such integration needs to be developed to a fully compatible networking environment between the Services. Modern weaponry is a prime churner of war-fighting innovation. Weapons are no longer simple munitions but have also become part of the system of sensors as they are guided onto their targets until they explode.

The realities of the information age continue to baffle some. It is not surprising that those who are beginning to understand the nature of the daunting challenge are not eager to take it on and would like the past to hold on for a bit longer. For

example, the custodians of legacy communication systems loathe changing and are continuing to resist demands for modernity under the ambiguous façade of 'information overload' despite adequate safeguards available to guard against this. Such an approach ignores the immediacy of the challenge and potential pay-offs. Transformation requires alterations in our concept of operations, doctrine, organisation, and force structure and, above all, in the psyche of the fighting man, including leadership. Associated changes in logistics, education, and training will also be required. These changes will have to be concurrent and on existing structures so as to bring about a graduated increment in net-centric warfare capabilities within the constraints of development and implementation time. A number of steps need to be taken. These include a phased shift in existing technology at the services level and horizontal fusion in the armed forces at a laid down hierarchical structure, bringing about a cultural change by aptitude-based selection procedures that will influence the attitudes, values and beliefs of future military leaders. Human resources development must be pursued vigorously ,with emphasis on making the man behind the weapon aware of the state of future wars and how to fight them.

Modern weaponry is a prime churner of war-fighting innovation. Weapons are no longer simple munitions but have also become part of the system of sensors as they are guided onto their targets until they explode.

For effective implementation, it should be very obvious that a number of imperatives will have to be taken up at the national level. All security related organisations must work in synergy on various aspects, leading to the implementation of net-centricity if we are to achieve the common goal of national security. These changes have to be driven from the top national leadership, as has been the case in most developed countries. In the United States, inter-Services rivalries were capped from the very top through an Act of Congress instituting the Department of Transformations for formulating a roadmap, and the Joint Forces Command was created. The German Chief of Defence Staff oversees transformation of the armed forces in accordance with the Berlin Decree. In China, it is Jiang Zemin himself who does this and its implementation is coordinated and overseen by the Central Military Commission. The Chief of General Staff of the People's Liberation Army spearheaded the blueprint of change. We need to study organisational interoperability models and adopt what

suits us. In the United Kingdom, the Chief of Defence Staff was thrust down the throat of the military after eighteen years of dithering and bickering by the Services.

If India is to graduate beyond being a regional power , our national focus should include establishment of a joint force networked for net-centric warfare. All our future accretions must be designed as 'net-ready' and interoperable. Emphasis must be placed upon indigenous research and self-reliance, to ensure security and redundancy in our system. We must develop net-centric warfare related concepts and capabilities in models and simulations too. Setting realistic and quantifiable goals, developing an implementation plan to achieve these and in so doing, being able to measure the progress made is essential. An immediate goal must be the availability of a networked joint force as a test-bed that can experiment with the concepts and capabilities of net-centric warfare. Our expertise in information technology must be exploited to create an interface between the defence forces and industry, with profitable pay-offs for both to foster self-reliance.

All commanders and the men they command will be the focus of transformation and the man behind the machine will continue to be the nerve centre. Net-centric warfare requires technology, but ultimately relies on people and organisations. Net-centric warfare demands a new set of skills and competencies from information age warriors that includes understanding of system capabilities in the battlespace and the ability, initiative and innovativeness to employ them for best effects, ability to interpret and make decisions on incomplete data, or when flooded with data overload, ability to operate in flatter organisational hierarchies, capability to deal with lethality / accuracy of new technology and adaptability and flexibility to cope with change. Enhanced education and intellectual standards for both soldiers and officers need to be catered for in a focussed manner. Aspects of network-centricity must be systematically worked up from basic stages of training to all the way up in a progressive fashion. Exercises will need to focus more on gaining experience and familiarity with utilising the network medium for interaction. The main challenge will be to train soldiers to work in small teams, develop common methodologies and joint staff procedures. Developing and harnessing of the existing training establishments of the Services for network-centric training should be looked into since leaders will need to function in an environment of increased speed of command, self-synchronisation and these operational imperatives will impact on the entire command process, including dispersion of authority. This requires attitudinal change. Operating with flexibility and speed, within the commander's intent,

requires a paradigm shift in tradition and culture. It needs decentralisation of authority based on trust, empowerment and confidence in the decision-makers – a very difficult proposition in the rigid hierarchical military gripped with the fear of slipping empires.

Net-centric warfare involves corroborating and sharing of information to ensure that in combined operations, appropriate assets can be quickly brought to bear upon the required target. This requires the creation of a more dynamic and responsive organisation. Net-centric warfare presupposes the abandonment of the classical hierarchical command and control system. Horizontal fusion of information calls for sharing of information by all components in the organisation in real-time that requires communication networks, connecting all the links simultaneously. For this to be realised at the tri-Services level, net-centric warfare will have to be forged on suitably integrated organisations, new technology, joint concepts, doctrines, joint training and joint communications architecture. Important issues that the Services need to examine are a jointly evolved communication architecture, joint / integrated organisations, joint concepts and a joint doctrine for net-centric warfare, induction of new technology, network-enabled platforms, attitudinal change to accommodate the concept of net-centric warfare and adapting the military leadership to accommodate the changing nature of war.

The architectural model for net-centric warfare must consist of a 'network of networks' with inherent redundancy. It must ensure seamless networking of all components, allowing the top leadership to access all information with regard to military, economic and diplomatic capabilities of the enemy. A functional, robust, secure and redundant network with unlimited bandwidth should provide military inputs. The firewalls, protocols and gateways of this functional network must ensure the flow of only genuine and relevant data, to avoid information overload. Once the operational picture is painted simultaneously to strategic decision-makers, the architecture must allow seamless interaction through a decision network to arrive at an optimal decision. At the operational level, the architecture must be designed to network the organisation in a manner similar to that at the strategic level. At the tactical level, the architecture must ensure seamless machine-to-machine integration of all manned and unmanned platforms and weapons. A highly reliable application network at this level is desired to establish situational awareness down to the lowest commander or the pilot of the aircraft to determine the whereabouts of his troops and identify enemy locations.

A major technical challenge in adaptation is that while the Services are modernising their respective networks with suitable gateways for limited integration at appropriate levels, existing communication networks do not allow the desired level of interoperability.

A major technical challenge in adaptation is that while the Services are modernising their respective networks with suitable gateways for limited integration at appropriate levels, existing communication networks do not allow the desired level of interoperability. The Defence Communication Network (DCN) is being fielded as a tri-Services strategic communication network for implementation of the command control communication, computers, intelligence, information (C4I2) concepts. Development of this needs to bear in mind various operational settings derived through strategy and operational tri-Service war-gaming. A multi-disciplinary project like implementing net-centric warfare demands addressing some critical issues at the inception stage. It is essential that a coherent framework for a 'Joint Services Enterprise Information Architecture' is defined which would support seamless flow of information across the battlefield, from the lowest echelons to the strategic level, but on a need to know basis. This should encompass the System Architecture, the Technical Architecture and the Operational Architecture. The System Architecture implies what is wired to what. The Technical Architecture indicates how interfaces are defined and the Operational Architecture implies how data flows. The technological challenge is how to integrate the desired information and to speed up and optimise information sharing among systems that were not originally designed to talk to one another. The organisational challenge is in determining how to adopt new practices that cut across organisational boundaries and harness collective expertise.

Communications infrastructure is the key to net-centric warfare. As per Metcalfe's Law governing network-centric computing, the power of a network is the square of the number of nodes in the network. This power can only be harnessed if matching mobile communications, with the requisite bandwidth, are provided to integrate the nodes to the network in time and space. Lack of communications / interim arrangements should not hijack networking. Bandwidth is important. The US forecasts 1 GB per sec requirement of bandwidth for a single combat

team by 2010-12. We need to examine use of commercial satellites for military communications with adequate security superimposed, as is being done by the developing countries. Lack of bandwidth on wireless media for mobile operations is one of the most complex technological challenges to net-centric warfare. A potential aid is the use of computer software to compress signals to ensure least consumption of space in the frequency spectrum. Higher capacity software defined radios that have the ability to transmit large volumes of information in lesser bandwidth than traditional radios are worth considering. The Services must continue to leverage commercial technology to determine alternate solutions to solve the bandwidth problem.

Lack of bandwidth on wireless media for mobile operations is one of the most complex technological challenges to net-centric warfare.

In the face of transmission impairments such as solar flares, bad weather and hostile jamming, networks must continue to function. If a signal cannot penetrate a rain shower or is blotted out by an enemy barrage jammer, then the link is broken. This would render the net-centric warfare model non-functional. Platforms must be able to specifically address and access other platforms or systems in a net-centric warfare environment, coping with a fluid network topology as platforms enter and leave an area of operations frequently. The answer lies in establishing "Plug and Play Connectivity". The future demands deployment of a large number of sensors over vast frontages that need complex application of data fusion. It would also demand management of various communication links, using diverse protocols across the frequency spectrum. Communication concentration, data management and fusion remain critical. The big challenge is to design an application with advanced artificial intelligence capability to detect and track legitimate targets. Collection, collation, interpretation and dissemination of information in near real-time can achieve information superiority. Data capture and their processing, including data fusion, hold the answer to this force multiplier. Capability to wage cyber war by denying information to the enemy while launching active attacks on enemy networks and databases would give the power of information dominance. These are evolving capabilities and it takes years of silent toil to achieve credible capability. Our neighbourhood is making giant strides in these fronts. Compare this to the remarks made by the president of the Cyber Society of India during an international seminar at Delhi in April 2009, stating that at the national level we have neither a proper organisation nor a policy for cyber security.

Inherent in network warfare is the potential for compromise. The more data you share, the greater the chance of compromise. There may be some virtue in keeping some elements on the net, and retaining tight hierarchical control of certain critical need-to-know elements. The level of active and passive security measures that are instituted will dictate success levels in future battles. We need to be alive to 'net forces' in our neighbourhood and microwave weapons being developed. Significantly, the US cyber warfare strategy is of "offence being the best form of defence". We should design own operating systems, create redundancy of networks and significantly enhance our chip manufacturing capabilities. Passive measures would include deception, disinformation, dispersion, nuclear, biological, chemical (NBC), electromagnetic pulse and high-pressure microwave hardening, etc. Such hardening is undoubtedly very expensive if one was to go for retro-fitment but if introduced *ab-initio*, the costs would go up marginally.

Not everyone understands the difference between cyber security and information assurance. Cyber security is only one part of information assurance. We need to expand on the base of cyber security to ensure full-fledged information assurance. Implementation of net-centric warfare will exponentially increase the number of information sources and the volume of information flow. Without measures to mediate this volume, information overload will occur much more than in the past. Increased information complexity can cause loss of situational awareness or unmanageable increase in mental workload. Of particular concern will be how to clarify, filter, and synthesise enormous amounts of information generated by net-centric warfare sensors to take critical decisions under time pressure and uncertainty. Automation can aid, in that it can quickly sort, filter and optimise a set of multi-objective functions.

Logistics nodes should be located in suitable geographical areas, with an automated inventory control mechanism. They should be self-contained and nuclear hardened plug and play modules to cater for sustenance of forces in an environment of precision strikes. Maintenance of high-end information technology equipment will necessitate major restructuring through a maintenance philosophy suiting a net-centric force. The dangers of micro-management are evident in the net-centric warfare concept. Commanders influencing two levels down and learning to practise information sufficiency rather than seeking infomation overload, can minimise this. Higher level commanders should be focussing on future moves of the force and not be sidetracked by the demands of the moment to interfere with the lower level handling of current activities by subordinates. A major tenet of net-centric warfare is that its

implementation can leverage significantly use of commercial products to reduce costs. Maximum use should be made of commercially available-off-the-shelf (COTS) hardware and software with the military funding development of unique software, and customisation that can use information more efficiently than COTS products. In order to achieve fast track modernisation of our armed forces in the field of technology, we need to take initiatives in development and accelerating own operating systems, global positioning system (GPS) and geographic information system (GIS), with standard protocols for data exchange. It is also essential that we develop our own chip technology and lay down guidelines and rules for cryptography, cyber warfare and policies on information assurance to protect our networks and databases.

A major tenet of net-centric warfare is that its implementation can leverage significantly, use of commercial products to reduce costs.

Concerted efforts have to be made at all levels to conceptualise, define, induct, implement and operate the new systems in a defined period of time. This is vital so as to be able to contain and limit obsolescence, cost escalation and depletion of carefully created expertise and continuity. Industry support can only be expected or sustained if projects are executed professionally in a time-bound manner. Therefore, the procurement cycle needs to be shortened. For meaningful and time-bound adoption of net-centric warfare in the armed forces, a number of measures need to be instituted. We need to formulate a suitable joint net-centric warfare doctrine at the national level, providing an evolving strategic vision of 'full spectrum dominance'. This doctrine should pave the way for de-conflicting actions to achieve united national efforts for net-centric warfare.

Fast paced technological developments have ushered a revolution in military affairs, ramifications of which have manifested into the inescapable requirements of militaries being net-centric warfare capable. In the Indian context, it is extremely important for the military to be net-centric warfare capable to meet future challenges not only in the battlefield but also for a variety of tasks they perform on the mainland that require near a real-time response to minimise damage. Towards this end, it is extremely important that the new military doctrine is joint and addresses the issues of interoperability and move of required data within the Services without impediments. It would also be prudent to aim for second generation net-centric warfare where effect-based operations (EBOs) would be the order of the day. This implies a shift in how we

A net-centric warfare capable military entails that the surveillance grid resources at the national level be integrated into networks, creating a viable surveillance grid.

look at network-centric operations; from a focus on 'networks' and an emphasis on faster targeting and more efficient attrition attained by taking the man out of the loop, to a focus on 'networking,' both social and physical connectivity, and an emphasis on using EBOs not only to deal with, but to exploit, the complexity of the security environment to be attained by knowing where man belongs in the loop and using the network to support him.

A net-centric warfare capable military also entails that the surveillance grid resources at the national level be integrated into networks, creating a viable surveillance grid. This, in turn, should provide the necessary inputs to designated firepower resources to react in a viable time-frame to neutralise the threat. We must accelerate indigenous research and development (R&D) to acquire critical technology, and to innovate and absorb the same is a must. We need to create joint organisations to achieve synergy and seamless interoperability, build a robust information and communications technological infrastructure effectively managing the transformation, and increase the technical threshold of users.

In the future, we may well be part of a multinational operation in a net-centric warfare environment. It is imperative that adequate technological infrastructure be nurtured to meet the hardware, software and joint doctrine challenges. We need to look at policies for sharing information and establishing priorities and processes for data exchange and engagement of targets. Cyber warfare technology needs to be nurtured to develop asymmetry against the adversary by denting his networks and downgrading his fighting ability. Our inherent strength lies in our dominance in the software fields. We need to strengthen this in-house capability to augment our technology and to enhance the effectiveness of our operators, transiting from the present capabilities to a network-enabled, and, finally, transforming into a network-centric force.