



Knots and Crosses

Without a CDS with full operational powers, net-centricity in the defence forces will continue to remain flawed

NETWORK CENTRIC WARFARE (NCW) focuses on the combat power that can be generated from the effective linking and networking of the war fighting entities. 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 synchronisation to achieve the commander's intent. The concept focuses on attaining access to information which is resident in an information network and its speedy dissemination so that the commander's intent can be translated into decisive action.

NCW has a number of advantages. Firstly, it allows us to move from an approach based upon the massing of forces to one based upon the massing of effects. This allows us to reduce our battle space footprint which in turn reduces risk because we avoid presenting the enemy with attractive high value targets. The second key advantage is that it enables our force to be knowledgeable. Empowered with knowledge derived from a shared awareness of the battle space and a shared understanding of the commander's intent, our forces can display initiative to meet the commander's intent and be more effective when operating autonomously. The third key advantage is that there is effective linking achieved among entities in the battle space. This implies that dispersed and distributed entities can generate synergy and that the responsibility and work can be dynamically reallocated to adapt to the situation. The bottom line here is that NCW results in increased tempo of operations, increased

NCW results in increased tempo of operations, increased responsiveness, lower risks, lower costs, increased combat effectiveness and enables the commanders to cope with the telescoped timeframes available for decision making.

responsiveness, lower risks, lower costs, increased combat effectiveness and enables the commanders to cope with the telescoped timeframes available for decision making.

Network Centric Capabilities allow the force to attain improved information position, help clear the fog of war and enable commanders to improve decision making to fight in ways that were previously not possible. Realisation of NCW requires not only technological improvements but continued evolution of organisations and doctrine, and training relevant to doctrine for sustained development of information advantage. One of the strengths of NCW is its potential to offset a disadvantage in numbers, technology and position. NCW derives its power from strong networking of well informed but geographically dispersed force. The enabling elements are high performance information network, access to appropriate information sources, weapons reach and manoeuvre with precision and speed of response, value adding command and control processes to include high speed automated assigned resources and integrated sensor grids closely coupled in time to shooters and processes. NCW 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.

Although India has emerged as an IT workshop and research centre for the developed world, a clear model for migration of our armed forces into a platform-centric force has yet to emerge. We need to take stock of the current state of information evolution and define an unambiguous course for transforming the Indian Army (IA) into the NCW paradigm. Though we have doctrines for C4I2 and Information Warfare (IW), these two spheres are components of NCW and do not constitute NCW by themselves. NCW also encompasses policies, strategy, concepts, military organisations and adjustments. To transform the IA into an NCW-enabled force, we need a NCW doctrine as the start point.

There is plenty of debate in the IA as

to what net-centricity is and who should be in charge; claimants in this tug of war being Operations, Perspective Planning, Signals and Information Systems (IS) directorates. A dispassionate examination of net-centricity in the IA would clearly indicate that the fulcrum of net-centricity actually is the Tac C3I System (Tactical Command, Control, Communications and Information System) being developed by the IA. Under the Tac C3I, sub systems like the CIDSS (Command Information Decision Support System), ACCCS (Artillery Command, Control & Communication System), BSS (Battlefield Surveillance System), ADC&RS (Air Defence Control & Reporting System), BMS (Battlefield Management System) etc are in various stages of development and implementation. While the development of the Tac C3I is well under way and being undertaken as per a road map, frequent hiccups occur due to the tug of war within the service, egoistic stonewalling, resistance to change, perceived dangers to comfort zones and more significantly, lack of understanding of technology by senior officers posted in particular appointments. Perhaps, we need to learn from the Chinese model, where systematic institutionalised technological training is mandatory before general officers get posted to certain specific appointments.

Until now, net-centricity has followed the 'Bottom Up' approach not only in the army but in the defence forces per se. This perforce has forced an evolution, whereas, the necessity was and is for a revolution. The army is in the process of now working out an NCW philosophy while little progress on this aspect is being undertaken at the Tri-Service level. Lack of a 'Top Down' approach has serious ramifications. For example, while the DCN (Defence Communications Network) is being developed, virtually nothing is happening on how to achieve the services hand-shake that would ride the DCN. A vital requirement in a networked system is not only interoperability of the system under development but also facilitating information sharing among systems that were not originally designed to talk to each



A NEW BEGINNING The Army Chief inaugurates DG, Information Systems Headquarters in New Delhi.

other. For inter-services interoperability, there is requirement of a comprehensive and well documented tri-service model which forms the basis for reference at the conceptual and development stage. Finalising and adoption of standards and protocols, mutually compatible database structures, development/ deployment of interfaces between systems using disparate platforms and commonality of hardware are challenges which need to be overcome. Harmonising standards and protocols for the three services is a gigantic task that can only be solved through outsourcing, given the levels of expertise available within the services. This process is way behind, save a few in-house studies that are underway. Headquarters Integrated Defence Staff (IDS) is toothless not only due to lack of operational responsibilities, but more so in the absence of a Chief of Defence Staff (CDS). Without a CDS with full operational powers, net-centricity in the defence forces will continue to remain flawed. This, in turn, will affect net-centricity of the IA since no service can undertake operations independently.

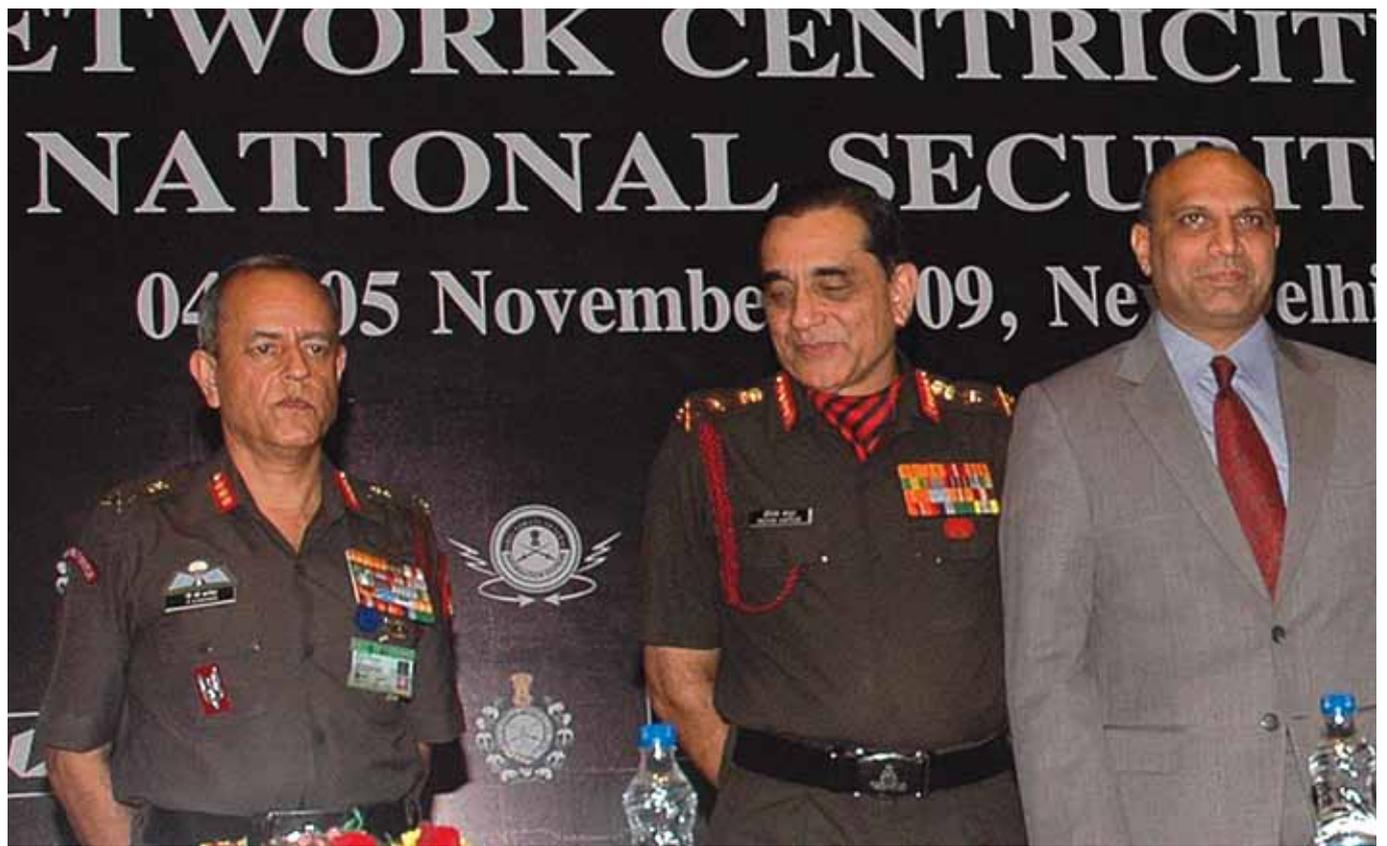
Within the IA there is a lack of a ‘Top

Down’ approach, which essentially should have flowed from an NCW philosophy laid down by the Operations Directorate. This has resulted in avoidable aberrations. Prime examples are lack of a policy on data handling and data storage and this responsibility being handled by Signals instead of Information Systems, number of policies on cyber security issued by multiple agencies, responsibility of cyber security with Signals instead of Information Systems and resistance to set up an Army Information Assurance Agency under the latter that would encompass cyber security. There is no policy on simulation and war-gaming, insecure army intranet hampering implementation of e-learning, fielding of army wide area network on army intranet without ensuring full security, non enunciation of bandwidth requirements of the IA in sync with increasing net-centricity in short, medium and long terms, Infantry wanting to handle computer and radio sub systems and software integration of Project F-INSAS by themselves and not letting Information Systems handle the same ensuring ab initio army wide integration including

time and costs savings, inordinate delay in developing the Tactical Communications System (TCS) severely restricting the test beds of the Tac C3I and eventual fielding of its sub systems.

Following a recommendation made by the Defence Expenditure Review Committee, Headquarters IDS is in the process of creating an Information and Communication Technology (ICT) Branch headed by a three star level officer — DCIDS (ICT). There are attempts from some quarters to make this three star appointment, Signals specific. Communications and Information Technology (IT) are

While the development of the Tactical C3I is well under way and being undertaken as per a road map, frequent hiccups occur due to the tug of war within the service, egoistic stonewalling and resistance to change.



DISCUSSIONS UNDERWAY Minister of state for defence, Pallam Raju and COAS Gen. Deepak Kapoor at a Network Centric Warfare Seminar.

important components of NCW but by themselves do not constitute NCW. HQ IDS needs to ensure that NCW is linked with developing a 'NCW culture'. To avoid misinterpretation of NCW and avoid arm specific hegemony, it may be prudent to ask for a 'Transformation (Tfn) Branch' under a DCIDS (Tfn) — a general cadre officer with preferably the experience of having commanded a Corps. NCW itself needs to function on the 'All Arms Concept'. Ideally, this Tfn branch should oversee C4I2, IW, Electronic Warfare (EW), Space, Information Assurance-cum-Cyber Security, Communications, Joint Organisations etc. These spheres require to be viewed holistically under a single dedicated DCIDS in order to ensure a top down 'revolutionary' approach to NCW. This will automatically ensure exploitation of the complete NCW-cum-Network Culture spectrum. The proposed 'Tfn Branch' should be charged with the responsibility of 'transforming' the defence forces and ushering in a 'network culture'. The network culture is responsible for exponential increase in revolutionary trends. It has to be related to policies, strategy/concepts and most

importantly 'organisational adjustments'. We need a 'revolutionary approach' in NCW; a top down approach that starts from policies and results finally in a system adjustment. As it is, in the absence of an NCW doctrine/philosophy, our strategy and concepts cannot be fully accommodative to the requirements of NCW.

Cyber warfare is a potent instrument of war with means to weaken enemy capabilities even before the battle is joined. President Obama recently termed it as a WMD. Security of information and assets is vital to military where networked infrastructure involves country-wide WANs and numerous smaller networks in a 'Network of Networks' concept. With hackings, a daily global phenomenon, our network architecture must have robust protection including indigenous security algorithms. We must endeavour to prevent attack and if it happens, contain it and effect swift recovery. Malware penetrating the systems or embedded at manufacturing stage can be disastrous in military networks. We need foolproof mechanisms to check our system for Malware. This is very relevant to our industry and public sector undertakings where almost all computer parts and some software are imported, mostly from a country notorious for its

'botnets', 'bot' armies, extensive cyber warfare capability and the will to use it. While the US military is raising a Cyber Command, it may be prudent for us to create requisite dedicated cyber warfare Task Force and make 'cyber dominance' an essential component of our war doctrine. Only strategic networks of the IA will function on fibre-optic or copper-based media. Operational and tactical networks need high mobility, using combination of terrestrial, wireless links and satellite overlays plus robust ECCM (Electronic Counter-Counter Measures). Future combat systems will be increasingly reliant on mobile broadband tactical communications with resilient wide area coverage. The West has developed high quality, feature rich military communication systems. Lack of R&D in India and the increased requirements of high capacity state-of-the-art telecommunication systems for our military communications networks have prompted the import of COTS (Commercial of the Shelf) hardware. Unfortunately, adequate frequency spots and bandwidth required for optimally deploying these systems are not available for exclusive defence use. There is a pressing operational requirement of allocating a dedicated defence band with adequate frequency spots to

cater for existing and planned defence communication systems.

Studies prove a strong relationship between personality and decision making. Personality influences general orientation towards goal attainment, selection of options, treatment of risk, and reactions under stress. Fog of war coupled with multiple or contradictory intelligence inputs further complicate decision making. A decision support system with capability of advanced MSDF (Multi Sensor Data Fusion) that presents a coherent COP (Common Operational Picture) at the tri-Service level is an absolutely essential. Also, updated and accurate knowledge of the terrain being a battle winning factor a superior quality GIS (Geographical Information System) platform providing intimate details of terrain is needed. Since proliferation of automated networked systems will induce dependence, even the smallest downtime can result in serious consequences. Therefore, reliability and robustness with almost 99.99 per cent uptime are vital prerequisites. In-built redundancy, interconnected through self-healing networks is the key. Benefits of virtualisation also need to be harnessed to provide high system availability. Multiple surveillance resources and weapon platforms require a robust and efficient BMS that is user friendly, not cumbersome, on-the-fly, rapidly adaptable to changing force levels and with high assurance secure communications for integrated and optimal employment of all combat resources at the point of decision. Artificial intelligence and Robotics are finding increased applications in military use. Intelligent systems that 'learn' from past experience can prove to be very useful in military applications like NMS (Network Management System). Similarly, robotics holds great promise for military use by way of unmanned vehicles for reconnaissance and surveillance, bomb disposal etc. Concentrated efforts are required for identifying areas in which these technologies can be exploited and contribution by agencies like CAIR and the domestic industry for development. The latter will need to be forthcoming in this regard as the past record of DRDO/CAIR in these fields has been pathetic to say the least.

Our networks will face serious threats even from non-nuclear EMP (Electro Magnetic Pulse) weapons and microwave weapons even before battle is joined. E-Bombs are a reality today. Although, EMP and HPM (High Pressure Microwave) hardening by retro-fitment

Harmonising standards and protocols for the three services is a gigantic task that can only be solved through outsourcing, given the levels of expertise within the services.

is a very expensive process, engineering EMP and HPM resistance into a system ab initio adds little to the overall cost. Given the incapacitating potential of these weapons, we need to develop such capability indigenously. Technological developments in the fields of IT and communications far outpace existing procurement processes. Long gestation periods of projects risk obsolescence and delays modernisation. Long time required to develop security algorithms and obtain SAG (Scientific Analysis Group) approval adds to the problem. There is a strong case for evolving a separate procurement procedure for IS and Communications, ensuring faster induction without compromising transparency and cost-effectiveness. As for HR (Human Resources), while we are training our personnel for system administration, operating and maintenance, outsourcing trained manpower by lateral induction of core specialists from the civil domain also merits consideration. Training is a challenge in transforming the army into a network centric force and is being addressed. However, what must be understood is that training not only involves training on new systems but also transformation in concepts and methodology of War. Some drastic measures are also needed to streamline procedures and prune service bureaucracy. For example, while outsourcing of a study to work out the IT training for the three Services was approved two years back, the request for proposal has yet to be issued by HQ IDS.

Concepts of individual services should flow from a joint doctrine. This will facilitate development of coherent tri-service networked architecture. Although development of automated OIS (Operational Information System), MIS (Management Information System) and GIS is currently underway in the Services, managing the actual transition is a major challenge which involves both the technological as well as psychological aspects of change. There is an inescapable need for standardisation and commonality of equipment and protocols so as to achieve integration of

the individual modules and systems for an integrated and resilient networked architecture.

Media redundancy, adequate bandwidth, robustness of transmission and efficient routing are vital for net-centricity. Exploitation of new technologies for development of Tac C3I system is adversely affected by availability of frequency spots for defence purposes in the desired frequency bands, albeit growth in demand for spectrum can be offset to some extent by deployment of new technologies like SDRs (Software Defined Radios). Effective management of a scarce resource like spectrum to assure connectivity is a major challenge in the network-centric environment. We must also focus on compression technologies for passage of information. Security of both stored data as well as transmitted information needs to be ensured by speedy development of robust security algorithms. There is still very little indigenous R&D in developing state-of-the-art technologies to meet the requirements of networked systems. There is a compelling need to develop our own operating systems, GIS software, computing and networking hardware with standardised proprietary protocols and standards. Development of new technologies, customised for military use and their working to operate in a synergised manner is the biggest implementation challenge in our efforts towards net-centricity.

The Indian military is at the threshold of the information revolution. HQ IDS and IS cells of the Services need to take a holistic view of the requirements and formulate a Joint NCW Doctrine which should act as a guiding document for evolution of the NCW architecture. Induction of Tac C3I of the army and corresponding systems of the navy and the IAF is well under way. Concentrated and focused efforts are now required to integrate these systems including into the overall national structure. Our force capabilities have at no point seen a 'revolutionary' jump. This can have serious implications in future vis-à-vis an adversary like China. More importantly, militaries, like ours, with long standing hierarchical organisational structures resist the 'network culture'. Shaping an organisation to meet new challenges is tough. The challenge to the IA and the defence forces is thus immense and needs to be addressed head on. ||