Network Centric Warfare in the Context of 'Operation Iraqi Freedom'

Shitanshu Mishra

Abstract

The Revolution in Military Affairs (RMA) moves on the wheels of Technology, Doctrine and Organisation; however, the main support structure, which gives it the predominant strength, is undoubtedly the technology. The changing concepts of warfare are driven by the available technology of the times. While sophisticated weapons and sensors have greatly enhanced combat efficiency, developments in Information and Communication Technology (ICT) have enabled greater connectivity and information sharing among widely spread force components. The concept of networking in business enterprises has found an equivalent in warfare in what is now referred to as 'Network Centric Warfare (NCW)'. NCW rests on the premise that the power of a force grows proportionate to the extent of networking among the weapons, sensors and the command and control (C2) elements, quite akin to Metcalf Law, which is applicable to any network. NCW not only enhances situational awareness, it is expected to drastically reduce the time for decision-making at higher levels of command.

This paper looks at the basic concepts of Network Centric Warfare and then goes on to examine how these concepts were actually tried out and put into practice in the recently concluded Gulf War II. The Indian efforts in this particular field, which are at a comparatively nascent stage, are also examined.

Finally, the paper tries to explore the future frontiers — what are the new technologies, which may usher in the global technological revolution with equally important consequences for warfare.

—*—

The concept of Revolution in Military Affairs (RMA) originated in the erstwhile Soviet Union in the early 1980s, and was referred to as Military Technological Revolution (MTR). Any revolution is expected to usher in

Strategic Analysis, Vol. 27, No. 4, Oct-Dec 2003

Revised paper received on December 17, 2003

fundamental changes in the system, and hence one may state that RMA is not a new concept, though the term has come in vogue only of late. The nature of warfare has changed continuously and newer technologies and concepts have been successful in creating a distinct asymmetry between two warring sides, resulting in a total rout for the side which failed to change with the times.

In the words of Saida Baider, "The information revolution and globalisation challenge two basic paradigms that used to lie at the heart of modern state security and strategic thought and practice: national sanctuarisation and global, pan-optic surveillance, through the use of spatially organised power for social control. Transnationalisation and interconnection (of players, vulnerabilities, risks and conflicts) are making the idea of a national sanctuary pointless, while global surveillance can do little to counter the virtuality and ubiquity of cyberspace, the invisibility allowed by new means of camouflage and deception, or the difficulty of identifying adversaries in, grey areas (Civil or military? Warrior or criminal? Combatant or non-combatant? Political group or mafia?)"[1].

RMA has three basic constituents. These are:-

- *Technology:* The integration of new IT into existing weapons systems and integrated C4ISR (command, control, communications, computers, intelligence, surveillance, reconnaissance);
- *Doctrine and operations:* Experimenting with technology to create new types of warfare; and
- *Organisation*: There can be no RMA without far-reaching institutional change, (jointness, business-style revolution in defence management, civilian-military integration).

It is the synergy among these three constituents that, according to Pentagon forecasts, will bring about RMA by 2025.

Wars are fought in three distinct domains: Physical, Information, and Cognitive.[2] The physical domain is the place where the situation that the military seeks to change, exists. It includes the reality parameters of strength, weapons, dispositions, etc., all very clearly measurable in terms of overall combat power. It is the domain where the physical platforms and the interconnecting communication networks reside. The Information domain

is where information is created, manipulated and shared, and ultimately utilised by the commanders and subordinates. The information, however, may not truly reflect the ground truth, unlike in the case of the physical domain. The cognitive domain is in the minds of the participants and relates to their perceptions, awareness, understanding, beliefs and values, which give a final shape to their decisions. This is the domain of intangibles: leadership, morale, unit cohesion, level of training and experience, situational awareness and public opinion. Battles and wars are actually won and lost in this domain. The attributes of this domain are extremely difficult to measure, and each sub-domain, i.e., each individual mind, is unique.

Thus, the realities of the physical domain are converted into selected data, information, and knowledge by the systems in the information domain, and these further assist the leaders in making judgments and taking decisions in their cognitive domains. A right kind of synchronisation in the time and space, resulting from conscious coordination and collaboration of the three domains, would lead to a winning act. Minimising the uncertainties in a war situation is the key to success, which usually comes to a side that makes the least errors and not necessarily to the side that was imaginative or bold.

The range and lethality of weapon systems have increased over the years, as a result of technological advancement, and the time to target has reduced. The battle-space has also expanded in all the three dimensions. In part, this expansion has been the result of the improved flow of information. Distances in battle-space are no longer constrained by communications. Another factor is the development of rockets and missiles with longer ranges. This has further obscured tactical and strategic boundaries. In a digitised battlefield, timely access to intelligence can be matched with the operational mobility with great effect.

The increasing availability and affordability of information, information technologies, and information-age weapons have increased the potential of converting impotent adversaries into formidable foes. The resultant asymmetric warfare involves each side playing by its own set of rules that emphasise their respective strengths, while attempting to exploit adversary's weaknesses.[3] Each side would vie for information superiority, which is defined as, "A state of imbalance in one's favour (relative advantage) in the information domain that is achieved by being able to get the right

information to the right people at the right time in the right form while denying an adversary the ability to do the same".[4]

Network Centric Warfare

Network Centric Warfare (NCW) recognises the centrality of information and its potential as a source of power. The RAND Corporation defines NCW as, *"... the linking of platforms into one shared awareness network in order to obtain information superiority, get inside the opponent's decision cycle, and end conflict quickly.*[5]" NCW is not narrowly about technology, but about an emerging military response to the information age. It involves networking in all the three domains, and displays the following characteristics:[6]

- *Physical Domain:* All elements of the force are robustly networked achieving secure and seamless connectivity and interoperability.
- *Information Domain:* The force has the capability to share, access and protect information to a degree that it can establish and maintain an information advantage over an adversary. Also, it 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.
- *Cognitive Domain:* The force has the capability to develop high quality awareness and share this awareness. It also has the capability to develop a shared understanding including the commander's intent. Moreover, it has a capability to self-synchronise its operations.

In addition, the force must be able to conduct information operations across these domains to achieve synchronised effects in each of these domains. The force will thus be able to generate increased combat power by better synchronising effects in the battle-space, achieving greater speed of command, and by increasing lethality, survivability and responsiveness. Structurally, the NCW model involves an operational architecture with three critical elements:

- Network grid for sensors (sensor grid).
- Network grid for shooters (engagement grid).

- Command and control grid (C2 grid).

Metcalfe's Law, as applicable to communication networks contends that the power of a network increases with the square of the number of nodes connected to the network. NCW builds on this law by asserting that maximising the number of nodes increases the chances of realising the promise of the networks through ubiquitous connectivity and interoperability. It also increases the survivability of networked operations in case of an attack since the functionality of the network stays even when a large part of it is adversely affected.[7]

The concept of calculating conventional force levels to achieve an objective has been radically altered on account of force multipliers. Smart munitions delivered from a single aircraft or a ship are more likely to accomplish certain missions, which perhaps could be achieved by employing an air-force squadron during the Second World War. Advancing columns of armour can be identified from space, and targeted in real time using a handful of missiles. Enemy command and control structure can be identified and attacked with crippling accuracy. A small well equipped and better trained force can cause much more devastation and accomplish more than what was possible in earlier wars.

President George W Bush characterised US military as, "…*defined less by size and more by mobility and swiftness…relying heavily on stealth, precision weaponry and information technologies.*" The transformation of the military is built upon new systems, such as Cooperative Engagement Capability Sensor linking system, new capabilities such as striking distant and time-critical targets, and most of all, an integrated war-fighting machinery with full interoperability among all the components of decision-making and executive authority. NCW is all about relationships, adaptability, and change, with information technology allowing it to happen.

Communication Infrastructure for NCW

Communication support topology in network-centric warfare environs is more infrastructural and network-based as against hierarchical. Dispersed and well spread out static and mobile infrastructure forms the basic backbone fabric, with the users hooking on at convenient points to derive vertical and horizontal communication support. The key characteristic is that, bandwidth is always scarce, required as it is for transmission and

reception of digitised terrain topologies with three-dimensional overlay enhancements along with realtime battlefield visualisations from the airborne platforms such as unmanned aircrafts and satellites. Information and electronic warfare are yet other consumers with large bandwidth requirements. The battlefield electronic scenario would be a milieu of the conventional and the state-of the art.

The operational tempo would be overwhelming, with enhanced situational awareness of commanders aided by the electronic and automated sensor systems that would convey a wide array of inputs to the central data bases of the C^4I^2 (Command, control, computers, communication, intelligence and interoperability) systems. These would, in turn, assist in making well informed decisions. The deployment of the sensors and the forces would be geographically widespread, dictated by the terrain and other operational imperatives. The sensors would be integrated to the datacentric systems through reliable, secure, scalable and redundant data networks comprising an assorted mixture of media and technologies, both state-of the art and legacy, like copper cable, Microwave (MW), Private Branch Exchanges (PBXs), satellite stations, Optical Fibre Cable (OFC), Wireless in Local Loop- Code Division Multiple Access (WLL-CDMA), etc. Battlespace management in these bits-and-bytes-dominated environment has to be an integrated seamless process in which the flow of information, tied to its time sensitivity, is of paramount importance.

Security of Communication and Data Networks

Security of the Defence networks involves protecting the networks at multiple levels and multiple points to ensure fallback support in the event of breaches. The media, whether wireless or wire line has to be secured by use of bulk media encryption systems in addition to the use of Terminal/ Subscriber End Secrecy Devices (TESD/SESD) to ensure user-to-user confidentiality of voice communication. On the other hand, data systems need to be made impregnable by additional measures such as physical access control, employment of application level security systems like Firewalls, Intrusion Detection Systems, Anti-Virus Systems, etc. The use of Public Key Infrastructure for encryption and digital signatures is necessitated to ensure integrity of data, confidentiality of information, authentication of users, as well as non-repudiation for all messaging and formal correspondence over the data networks. The backbone is required to be secured by use of bulk media encryption systems. The security of the

network, however, would have multi-layered architecture, depending upon time criticality and the consequentiality of the information being carried.

NCW: 'Operation Iraqi Freedom'

'Operation Iraqi Freedom' (called 'Operation Telic' in UK and 'Operation Falconer' in Australia) was launched by coalition forces comprising of forces from USA, UK and Australia besides some other smaller countries, under the leadership of USA. The coalition headquarters was established in As Salihiyah, Qatar in the deployable Central Command (Centcom) Forward headquarters. The US' 101st Airborne Division, 1st Armored Division, 3rd Infantry Division, 4th Infantry Division (Mechanized), the 1st Marine Expeditionary Force, Special Forces, US Navy and US Air Force were the main players, besides the contingents from other countries. The following were under the Force HQ :-

- Special Operations Component Commander Brigadier-General Gary Harrell, in Qatar.
- Coalition Maritime Component Commander (CMCC) Vice-Admiral Timothy Keating, at Al Manamah, Bahrain.
- Coalition air Component Commander (CACC) Lt General Michael Moseley, at Prince Sultan Air Base, Saudi Arabia; and
- Coalition Land Forces Component Commander (CLFCC) Lt General David McKiernan, at Camp Doha in Kuwait.

Strategic communications were provided by the Operational Strategic Communication Architecture (OSCAR). Bandwidth, rather than military robustness was a major consideration, and hence commercial off-the-shelf (COTS) equipment was mostly used. OSCAR, with a hub-and-spoke configuration, ultimately covered eight countries, with 44 nodes, 30 satellite heads, six security domains, and provided access to eight secure voice networks, with a 54 MBPS information flow.[8]

At the tactical level, a two-layered network was assembled.[9] The first layer focused on a single channel radio and Tactical Satellite System (TACSAT). All the command posts — Division Main and Rear, the Assault Command Post (ACP), and brigade and separate battalion Tactical Operation Centres (TOCs) — were hooked up into single channel

networks. The TACSAT provided a 25 khz and a 5 khz channel, the former being used as the command net and the latter for the fire support. TACSAT had to be duplicated with Combat Net Radio (CNR). The radio used was in High Frequency (HF) and Extremely High Frequency (EHF) bands.

The second layer was a more robust voice and data network using Mobile Subscriber Equipment (MSE), onto which the division, brigade and battalion TOCs and command posts were connected. The MSE network also enabled video conferencing among commanders. The Defense Collaborative Tool Suite enabled them to share data files and alter displays as if they were video conferencing a Powerpoint presentation. Other divisional elements such as air defense artillery, logistics and military intelligence employed their own specific data networks through the MSE network. Company-battalion and platoon-company levels had their own internal communication, with a capability to connect to the nearest MSE node.

The MSE network comprised several signal nodes. At the heart of this network was the node centre providing switching, radio systems, network management and support. This node is responsible for backbone network connectivity, subscriber number management, network communication security management and line-of-site radio links to adjacent node centres and other units. The node centres provide 1,024 kbps links.

The divisional signal unit also had a few Contingency Communications Parent Switch (CCPS) and Contingency Communications Extension Switch (CCES) nodes which provided telephone line connectivity, remote radio access unit support and a CNR interface. The CCPS and CCES are also referred to as the Force Entry Switch. Its role is to provide connectivity from a force entry location to the sustaining base or an intermediate staging base. In addition, Small Extension Nodes (SENs) supported the aviation brigades, separate battalions and brigade support areas.

MSE is linked from node to node with line-of-site (LOS) radio shoots, mainly using the Enhanced Position Locating Reporting System (EPLRS). For long distance hauls, multi-channel satellite terminals, or MUXSATs were utilised. These were specially useful for providing the vital links between TOCs separated by hundreds of kilometres. MUXSATs provided a 2,048 kbps link between Division Main Headquarters and Division Rear Headquarters, and 1,024 kbps links were provided from divisional

command posts to brigades, as also to the corps. Army's Force XXI Battle Command Brigade-and-Below (FBCB2) battle management system, initially designed to work with EPLRS and create a battlefield picture of friendly and enemy platforms, was provided with a satellite interface and fielded to every coalition ground force unit down to company commanders.

Another interesting feature was the Jump Command Post created for the airborne assault. Known as C2 helicopter, it provided frequency Modulation (FM) and ultra-high frequency (UHF) and HF radio communications, and also single channel satellite links for command and control purposes, in the same way as that for the ground forces. The C2 aircraft is actually a flying command post, which could carry the divisional commander. The communication suite for the more advanced, upgraded version, known as advanced airborne command and control system (A2C2S) includes LOS radio such as the Single Channel Ground Airborne Radio System (SINCGARS), Advanced System Improvement Program (ASIP) and UHF HAVE QUICK II. Non-LOS links include demand assigned multiple access (DAMA), wideband radios such as Near-term Digital Radio (NTDR) and the Enhanced Position Location Reporting System.

The backbone of US command and control network are the two Internet Protocol (IP) networks engineered over the data communication infrastructure explained above — the Non-secure Internet Protocol Router Network (NIPRNet) and the Secure Internet Protocol Router Network (SIPRNet), which provide web access to various types of data. The latter, being secure, is used for operation orders, situation reports, intelligence reports, etc., but it is a 'NOFORN' system, implying that foreigners are not allowed access. For the coalition forces a Coalition Wide Area Network (COWAN) was engineered using a software which replicated SIPRNet web pages on COWAN provided that the security classification was appropriate. The UK also developed and introduced 'X-Net', which provided limited interoperability with SIPRNet to British Headquarters, enabling them to exchange information with certain addressees and limited access to information.[10]

The most effective exploitation of the networks came in the form of K-web or the knowledge wall, a large screen display panel, with web data feeds from an anchor desk. Each war fighting and support function – strike, air defence, intelligence, meteorology — had an anchorperson feeding latest

updated information from that functional area to the respective portion of the wall. The K-web was used effectively for planning, briefing and execution of plans. The screens could display large scale GIS maps and provide multi-source data fusion for collaborative visualisation and decision-making. An added advantage was offered by the chat service on the web, which could assist in clarifying any nagging doubts.

The information operations encompassed the whole spectrum of effect-based missions from psychological operations and system security to intelligence gathering and infiltrating enemy communication networks. In order to have an idea of the gains of the NCW during the operation, one must look at the following facts:- [11]

- A total of 1,801 combat aircraft were fielded by the USA, Australia and the UK , from March 19 to April 18, 2003. The largest subset of aircraft within this was dedicated to intelligence, surveillance and reconnaissance (ISR) activities. The coalition forces also fielded 80 ISR-dedicated platforms in support of their operation. Collectively, these aircraft are reported to have completed 1,000 ISR sorties, and as a result, generated 42,000 battlefield images, 3,200 hours of full motion video, 2,400 hours of signals intelligence (SIGINT) coverage and 1,700 hours of Moving Target Indicator (MTI) radar imagery.

- RQ-4A 'Global Hawk' unmanned aerial vehicle (UAV) was used first time as a strike coordination and reconnaissance asset, and it was found to be particularly effective in locating air defence and surface-surface missile targets. Pairs of 'Rivet Joint' aircrafts were used to accurately locate moving targets, such as surface-to-surface missiles and SAM launchers.

- US Navy E-2C 'Hawkeye' 2000 aircraft was used to direct air strikes during adverse weather conditions.

- E-8 Joint Surveillance Target Attack Radar System (JSTARS) aircrafts were used to provide dynamic surveillance and targeting during 'brown out' conditions. The MTI capability of the B-1 strategic bomber's radar was used in an ISR role.

- There was a use of the Global Positioning System (GPS) guided

munitions, providing a high degree of resistance to adverse weather conditions and enhanced accuracy.

- Extensive usage of electro-optical and laser guidance pod systems was done for targeting and damage assessment.
- Airborne Warning and Control Systems (AWACs) aircrafts were used as dynamic tasking tools. The availability of the Joint Tactical Information Distribution System (JTIDS) and other types of data modems played a significant role in the direction and redirection of airborne strike assets.
- A combination of dynamic data exchange and the latest generation of guided munitions allowed single platforms to effectively engage multiple targets during the same mission.
- Space-based reconnaissance assets, as part of the overall sensor network detected 26 missile launchers, 1,493 static 'infra-red' events and 186 high explosive events.

Instant communication systems, GPS and laser-targeting systems meant that the US Special Forces on the ground could call in an air strike at a moment's notice. Rather than take off from their carriers to attack pre-arranged targets, Navy warplanes could fly out to loiter, waiting for the call. With their new generation of precision weapons, the warplanes could strike a column of men suddenly materialising out of the hills**.** The best example of the success of NCW was the attack on a restaurant in Baghdad where President Saddam Hussein was expected to be present. A B-1B bomber was tasked in the air, and a successful attack was effected in 12 minutes from the first information to the aircraft.

RMA: The Ultimate Objective

Operations in Iraq were demonstrators of the transformations encompassing a variety of advances in Information Technology (IT), Precision Guided Munitions (PGMs) and Space Technology. The combined effect of these resulted in total asymmetry of the two warring sides, in spite of the fact that the coalition forces were numerically weaker than the Iraqi forces. Even a semblance of resistance, as was witnessed during 'Operation Desert Storm', was not to be in the Gulf War II. A beleaguered Iraq, devastated by long spell of wars, and sanctions imposed by the world

at large, was no match for the technological skills of the US military during the main phase of the war. However, this asymmetry was eroded considerably after the capture of Baghdad, when widely dispersed pro-Saddam troops chose conventional methods of attack in a kind of guerilla warfare for inflicting casualties.

A high degree of battlefield transparency in the form of Sensor-Shooter integration was achieved through network technologies and availability of intelligence, surveillance and reconnaissance assets like UAVs, and space platforms. During 'Operation Desert Storm', the USA had no more than 15 per cent information on militarily significant targets. This figure increased to above 65 per cent during 'Operation Iraqi Freedom'. Likewise, whereas in_Kosovo, about half the ordnance dropped was precision-guided, and in Afghanistan, it was about two-thirds; in Iraq more than 70 per cent of smart bombs were used. Use of precision munitions is increasing in part because the falling prices of electronics has made this class of weapons a one line-item in the Pentagon budget that is getting cheaper. At the time of Gulf War I, smart munitions cost US$ 250,000 to US$ 1 million apiece; the new smart bomb that debuted in Afghanistan, called JDAM, cost around US$ 20,000. While getting cheaper, smart munitions have also become more effective. According to a Pentagon analyst, about 80 per cent of smart bombs struck within a few yards of their aim points with dramatically better accuracy than in any prior air campaign. NCW made a very positive contribution in achieving this sophistication.

Another important aspect of the operations was the extensive use of the space technology and satellites. Rapid and responsive military operations require timely and accurate reconnaissance reports, weather monitoring, precise navigation, and long haul fail-safe communications. Global Positioning System (GPS), Geographical Information Systems (GIS) and satellite communication system assets were used for detecting, identifying, monitoring, tracking and ultimately destroying enemy resources. In numerous examples in Afghanistan and Iraq, a soldier on the ground would use a laser rangefinder linked to a Global Positioning System receiver to get a target's coordinates. Those coordinates could be sent via satellite radio to a command site hundreds of miles away, which would then send them to a bomber. The coordinates were then loaded into GPS-enabled bombs that receive navigational signals from satellites and can adjust their course in flight. Bombs fitted with GPS kits allowed the airplane to stay safe at

30,000 feet or higher while dropping bombs that are accurate to within a few yards, even through heavy cloud cover or darkness.

Lastly, the communication infrastructure created for NCW also assisted greatly in the Psy-ops during the entire operations. Military operations have become spectator events watched in real time by the people worldwide. The ability to provide graphic and live coverage of events is compressing time and space. The gap between political, strategic and tactical levels is being bridged. Media is becoming a potent weapon to shape public opinion (Perception Management). It gained momentum with the trend of embedded journalists in Iraq, who could report directly from the battlefield.

Communications for Joint Operations: An Indian Perspective

Even though an Integrated Defence Staff headquarters has been in existence for sometime, a communication network to cater to joint operations in theatres of our concern by all the three services will take long. Indian aspirations towards RMA will remain unfulfilled till we are ready for the NCW, the first and foremost requirement for which is a communication network which allows interoperability of the highest order among all the constituents of the war fighting machinery. It may, however be added that the three services have modernised their respective networks, and suitable gateways have been catered to for limited integration at appropriate levels.

The future may beckon the Indian military to fight a war as part of a coalition force, in a NCW environment. It is therefore imperative that adequate infrastructure be developed to be able to meet the challenges of C4I2SR (Command, control, communications, computer, intelligence, interoperability, surveillance and reconnaissance), not only in terms of hardware, but software and most importantly, joint training too. A few aspects, which may pose serious concerns, and hence need to be given due thought, are as follows:-

- Will there be an information overload? How do we manage and ensure that the data received from various sensors and other sources are adequately filtered, evaluated and used in a timely manner?
- There is bound to be significant interference and spectrum management problems, both intentional (due to enemy actions) and unintentional. Devices are available to disrupt the GPS, and

jam the satellite communications. The electronic warfare will have a much larger scope and a role to play in the future.

- Cyber warfare, especially the offensive part may have a more devastating effect. This aspect needs a more detailed analysis and necessary defensive countermeasures should be developed indigenously to make our own systems more robust.

- Considering the fact that space technology has an important role to play in NCW, India must increase its space activities and set up platforms to support indigenous GPS-like systems in order to avoid negative interference or denial by others, when most needed. For this purpose, better coordination between the Space Agency, DRDO and the Services is essential. It needs to be noted that China has already embarked upon an ambitious plan in this field.

- More emphasis ought to be given to the psychological operations as part of overall strategy, and all fresh approaches and means should be explored in this area.

- NCW demands a new strategic thought, doctrine and organisation to support the operations. The Integrated Defence Staff must commence concretising the same for effecting the transformation in right time.

India certainly has an edge over all her neighbours in the field of Information and Communication Technologies (ICT), and this advantage must not be lost. The present symmetry between India and Pakistan can be turned to an asymmetry advantageous to India by leveraging the technological prowess by the right mix of strategic thinking, planning, better coordination with DRDO and defence industry, and most important, envisioning our objectives for tomorrow.

Fresh Horizons

The global technology revolution will bring in many new technologies in the not-so-distant future, and quite a few of these will have implications for warfare. It may be difficult to predict what will be the next step in the RMA, or how the war domains would be influenced by new technological developments. Some of the recent advances in the fields of electronics, bio-informatics, materials engineering and molecular/nano-technologies

do point to a different world in not-too-distant future.[12] The following are some printers in that directions:-

- *Smart*—Reactive materials combining sensors and actuators, perhaps together with computers, to enable response to environmental conditions and changes thereof. (Note, however, that limitations include the sensitivity of sensors, the performance of actuators, and the availability of power sources with required magnitude compatible with the desired size of the system). An example might be robots that mimic insects or birds for applications such as space exploration, hazardous materials location and treatment, and unmanned aerial vehicles (UAVs).

- *Multi-functional*—Micro Electromechanical Systems (MEMS) and the 'lab-on-a-chip' are excellent examples of systems that combine several functions. Consider aircraft skins fabricated from radar-absorbing materials that incorporate avionic links and the ability to modify shape in response to airflow.

- *Environmentally compatible or survivable* — The development of composite materials and the ability to tailor materials at the atomic level will most likely provide opportunities to make materials more compatible with the environments in which they will be used.

- *Miniaturisation* — This brings all-pervasive, self-moving sensor systems; nanoscrubbers and nanocatalysts; micro-electomechanical (MEM) devices; nano-robots; and even inexpensive, networked 'nanosatellites'. For example, the so-called 'nanosatellites' are targeting order-of-magnitude reductions in both size and mass (e.g., down to 10 kg) by reducing major system components using integrated microsystems. If successful, this could economise current missions and approaches (e.g., communication, remote sensing, global positioning, and scientific study) while enabling new missions (e.g., military tactical space support and logistics, distributed sparse aperture radar, and new scientific studies).

- *Precision weapons and non-lethal, anti-sensor/anti-electronic weapons* — These including High Power Microwave (HPM), and laser weapons will influence the warfare with an aim of minimising the collateral damage, especially during peace support operations

and operations other than war.[13]

Beyond individual technology effects, the simultaneous progress of multiple technologies and applications could result in additive or even synergistic effects. It is also possible that certain combinations of realised advances could have negative effects on each other, resulting in unforeseen difficulties. Unforeseen ethical, public concern, or environmental difficulties may be examples. This, only time will reveal.

References/ End Notes

1 Bédar, Saïda, The Revolution in Military Affairs and the Capabilities Race. Disarmament Forum. UNIDR.

2 Alberts, Davis S., et al, Understanding Information Age Warfare. US DoD Command and Control Research Program (CCRP), August 2001.

3 Alberts, David S., et al, Network Centric Warfare. CCRP, August 1999.

4 Information Superiority: Making the Joint Vision Happen. Office of the Assistant Secretary of Defense (C3I), Pentagon, Washington DC, CCRP, November 2000.

5 Mackrell, Eileen F., US Navy: Network Centric Intelligence Works. Proceedings. July 2003.

6 Alberts, David S., et al, no. 3.

7 Chen, Clement C., Anatomy of Network-Centric Warfare. *SIGNAL*. August 2003.

8 UK Command and Control During 'Iraqi Freedom'. *Jane's Intelligence Review*. July 2003.

9 *SIGNAL*. July 2003. Special issue on 'Operation Iraqi Freedom'.

10 UK Command and Control During 'Iraqi Freedom', no. 8.

11 Airborne surveillance assets hit the spot in Iraq. *Jane's Intelligence Review*. July 2003.

12 The Global Technological Revolution. RAND Publication at http://www.rand.org/publications/MR/MR1307/MR1307.

Col Shitanshu Mishra is Research Fellow in IDSA, and is presently working on 'Communication Technology and Counter Terrorism'.

He is Fellow of Institution of Telecommunication and Electronics Engineers (IETE) for more than 10 years, and a member of Computer Society of India (CSI) for well over 15 years. He is one of the founding members of 'Association for Security of Information Systems'.