Conduct of Military Operations in Information Age: Implications for India

Major General Y K Gera (Retd)

Introduction

The 21st Century is witness to unprecedented revolution in the field of Information Technology (IT). Modern means of communication have turned the world into an integrated and seamless network of information. There has been a dramatic increase in use of Personal Computers (PCs), Internet, mobile phones, ipods, and spread of e-commerce. Business activities are being better coordinated with the setting up of inter-industry databases, transcending corporate boundaries and forming the nervous system for the full spectrum of corporate activities by sharing information.

Over a period of time, security paradigms have changed radically. It is economic security and energy security, which have attained higher priority. Disaster management capability, therefore, is as important, if not more, than war fighting capability. Asymmetric warfare, rather than conventional warfare, has attained ascendancy internationally. An adversary will seek to wage asymmetric warfare and cripple economic and energy infrastructures rather than engaging military targets. An alternative may be launching of cyber attacks to damage the railway, banking and power grid systems.

In the military domain the Information Technology is bringing about Revolution in Military Affairs. Information can be stored, manipulated and delivered as any other commodity thus enhancing its potential for influence in many ways, both in peace and war. Information Warfare1 has emerged as a major form of warfare, which encompasses actions taken to achieve information superiority by affecting adversary information, information based processes, information systems and computer based networks, while leveraging and defending one's own information.

India has earned a significant place in the global IT industry and aspires to be an IT superpower in the near future. With an expanding IT infrastructure, the nation is getting connected to the 'global village' at a rapid pace. Ironically, the technology that empowers us also exposes us to new threats.

Revolution in Military Affairs (RMA)2

RMA has affected the conduct of operations considerably. This has been enabled by advances in IT systems for aid to navigation, precision guidance and control of weapon systems. Developments in the field of network-centric operations and changes in doctrine leading to 'effects' based warfare, have contributed towards improved efficiency. The revolution is about connecting platforms, weapons, sensors, and decision makers and enabling exchange of timely, accurate, and relevant information and building a common operational picture. The essence is speed of command enabled by improvements in IT and telecommunications.

During the Gulf War in January 1991, images of Tomahawk missiles were shown on television screen hitting their targets in Iraq with astonishing accuracy. The destruction that these 'Tactical Land Attack Missiles'(TLAMs)3 inflicted upon command posts, communication structures, radars, early warning sensors and so on, demonstrated their strategic and tactical significance. The military as well as the national leadership in Iraq was virtually paralysed. The US led air strike missions virtually had a free run after the TLAMs were used with precision on carefully selected targets. Subsequently, TLAMs were used with precision in Sudan, Bosnia and Kosovo achieving the desired results both at the strategic and tactical levels. In Afghanistan, TLAMs were used in 1998 for destroying the militant training camps and hideouts of Osama Bin Laden. An analysis of various stages of TLAM strikes by the USA in different theatres reveals that only the launching of TLAM was conventional, the remaining functions were facilitated by the space based IT systems. These included the following:-

- (a) Intelligence about the target area.
- (b) Command and control of strike mission.
- (c) Weather forecast.
- (d) TLAM in-flight navigational guidance.
- (e) Damage assessment after the strike.

TLAMs can help the political leadership to flex muscles and exercise coercive diplomacy when required. Their long range, surgical precision and negligible collateral damage make them weapons of choice. This is particularly so because though nuclear weapons are considered as the currency of power, it is being advocated that in a civilized world these must never be used for fighting wars.

Comprehensive National Strength

Comprehensive National Strength is a combination of a country's overall capability in terms of its system of governance, economy, scientific base, military capability, human and material resources, social development, environmental factors, judicial system, diplomatic profile and internal cohesiveness. A country's ability to influence global and regional affairs is directly proportional to its perceived National Strength. India is doing well economically. However, there are certain issues, which if not addressed concurrently, can cause setbacks.

Threats and Challenges

As India grows economically and in strategic terms, its footprint will extend beyond the immediate region. It will have a growing role in international institutions and groupings. However, in this paper discussion is limited to military aspects.

In the near and mid-term, the Armed Forces are more likely to fight non traditional conflicts involving counter terrorism on land, at sea, and in the air. In addition, the Armed Forces may be called upon to stabilise volatile strategic environment around India through power projection if required. Force may have to be projected to secure our off shore assets, island territories, Indian diaspora abroad, and to assist friendly nations when invited. In addition, the Armed Forces are called upon to undertake disaster management and peacekeeping operations. The modern battlefield scenario is characterized by rapid mobilisation, accurate battlefield visualisation, integration of surveillance systems with weapon systems and increased requirement of shared battlefield awareness. These necessitate a paradigm shift towards network centric warfare.

STRATEGIC ISSUES

India's Military Capability

India has highly professional and well-equipped armed forces that are capable of acting at short notice to protect its national frontiers. Apart from the Service specific commands, we have created two integrated commands, i.e. the Andaman and Nicobar Command and the Strategic Forces Command. Though these are tri-service commands, they have specific roles and are not structured for military intervention, power projection, humanitarian assistance and other eventualities that may arise in the regional and global context.

The Group of Ministers in their recommendations on "Reforming the National Security System" in February 2001 had stated-"The Chiefs of Staff Committee (COSC) has not been effective in fulfilling its mandate. It needs to be strengthened by the addition of Chief of Defence Staff (CDS) and a Vice Chief of Defence Staff (VCDS)." With greater emphasis on joint and integrated operations in the future, the system was to be reorganised with a CDS and a VCDS together with an integrated staff. Although the staff has been provided, due to various reasons the CDS has not been nominated. At the regional commands there is no "Jointness" in planning as per the present organisational structure. Each Service plans separately and attempts to coordinate operational plans later at the regional command level, with the other Services. The regional command headquarters of the three Services are neither co-located nor networked. Hence joint operational planning and real time sharing of intelligence picked up by various sensors of the three Services is not possible. As future conflicts are likely to be of short duration, requiring selective use of force, lack of integrated organisations would preclude optimisation and efficiency in joint operations.

India needs to create appropriate military capability taking into account likely threats to national security and the role envisaged at the regional and global levels. In this context, India's experience in Sri Lanka and the Maldives would provide valuable guidance. The command, control, communications and surveillance requirements for such a capability would have to be specially structured. Sufficient redundancy would need to be catered for to absorb add-ons by way of specialised elements that may be required for humanitarian, peacekeeping and peace-building operations. Capability to sustain forces away from our shores should be catered for. This would require maritime and aerospace assets. Interoperability and interfacing with friendly forces of foreign countries should be factored in.

The approach should be to build capability to be able to respond immediately with a small balanced and self contained tri-service force in any contingency. Additional forces can be built up as the situation develops. The political 'will' to create and commit such a force would have to form part of India's Security Strategy.

Information Infrastructure

Critical National Information Infrastructure4. The critical sectors of our nation include energy, transportation, banking and finance, telecommunications, defence industrial base, government, and emergency services. Most of these sectors are dependent on cyberspace for their functioning.

Defence Communications Network. The three Services are modernising their networks and suitable gateways are being catered for integration at appropriate levels. The existing communication networks do not allow the type of interoperability required. The completion of the Defence Communications Network (DCN) 5 which is being fielded as tri-services strategic communication network for implementation of the Command, Control, Communications Computers, Interoperability, Intelligence, Surveillance and Reconnaissance (C4I2SR) concepts, will lead to the connectivity down to corps headquarters in the Army, maritime operations centres in the Navy and air defence direction centres and airfields of the Air Force. The tri-service architecture has been finalised after conduct of military war games.

Army's Information Infrastructure. It is based on optical fibre cable, microwave, VHF and UHF radio, coaxial cable and satellites, and is either owned or hired media. More and more data is being processed and stored on networks. Networks have enabled integration of the sensors, shooters and decision- makers, enabling faster reaction time. Network survivability in the modern warfare would be critical and may prove to be a battle winning factor.

Network Centric Warfare

What is Network Centric Warfare (NCW)6? It is a product of convergence of computers and communications and their exploitation to bring to bear maximum combat power at the right time and place. The essence of NCW lies in translating information superiority into combat power by effectively linking knowledgeable entities in the battle space. Akin to the Metcalf Law 7, power of a force grows proportionate to the extent of networking among weapons, sensors, and command and control elements. Thus, networking is a potent force multiplier. Network centric operational concepts are based on:-

- (a) Dominant manoeuvre.
- **(b)** Precision engagement.
- (c) Focussed logistics.
- (d) Full dimensional protection.

Domains of Warfare.8 There are three established domains of warfare :-

- (a Cognitive Domain. It encompasses the mind of those fighting the war and the supporting populace. Intangibles like leadership, morale, training, public opinion and so on, are part of this domain. Intention, doctrine, tactics and techniques form part of this. Most battles are won or lost in this domain. It involves carrying out of appreciation and formulation of operational directives and orders.
- (b) Information Domain. Information is created, processed and shared in this domain. Collection of information and converting it to intelligence and passing of operational orders and directives is done in this domain. Information superiority is achieved by the integration of sensors, shooters, and decision makers.
- (c) **Physical Domain.** This is the traditional domain of warfare and contains physical platforms and communication networks that connect them. Strike, protection and manoeuvre across the environment i.e. ground, sea, air and space takes place in this domain. In simple terms it involves actual destruction of enemy.

Information Operations (IO). These are actions taken to achieve information superiority by influencing the information based systems, processes, communications and data networks of the adversary. It is a deliberate effort to gain access to, temper with, and exploit information systems of the adversary, while at the same time preventing him from doing the same to us. It comprises information dominance and information assurance. While the former is an offensive action, the latter is defensive in nature. The components of IO are as under:-

- (a) Command and Control Warfare.
- (b) Intelligence Based Warfare.
- (c) Counter Surveillance Warfare.
- (d) Perception Management.
- (e) Net Warfare.
- (f) Electronic Warfare.

NCW: Army Doctrine. The Army doctrine on NCW was released in October 2004. Highlights are as under;-

- (a) Emphasis is on Information Warfare and fielding of C4I2SR systems.
- (b) Creation of technological asymmetry to increase battle field transparency and situational awareness.
- (c) Development of Force Multipliers with increased precision.
- (d) Perception management.
- (e) Emphasis is to be laid on C4I2SR systems.
- (f) Impact on low intensity conflict and asymmetric warfare.
- (g) Changes in concepts, organisations and attitudes. The Armed Forces are not integrated. Some stand alone capabilities exist within each Service. The Network Centric Warfare will have to be forged on suitably integrated organisations, new technologies, joint concepts and doctrines, and joint training and communication architecture.

Transition from Platform to Network Centricity. It will involve the following:-

- (a) Radical attitudinal change by the military leadership and transformation in style of command.
- (b) Joint war fighting doctrine.
- (c) Centralised planning and decentralised execution.
- (d) Create integrated regional commands.
- (e) National 'will' to take hard decisions.
- (f) Develop appropriate technologies.
- (g) Increase user awareness and address issues of information assurance and cyber security. Our tactics will need to exceed the velocity of warfare of the enemy in all dimensions. It would involve joint training.

CONDUCT OF TACTICAL OPERATIONS IN INFORMATION AGE

Technology and Transformation in Military Operations

Throughout history military doctrine, organisation and strategy have continually undergone profound technology

driven changes. Newer technologies and concepts have been successful in creating a distinct asymmetry between the warring sides, resulting in the rout of the side, which failed to change in keeping with the times. Industrialisation led to attrition warfare by massive armies in World War I. Mechanisation led to manoeuvre predominantly by tanks in World War II. The information revolution implies the rise of a mode of warfare in which neither mass nor mobility will decide outcomes; instead, the side that can disperse the fog of war and yet enshroud an adversary in it, will enjoy decisive advantages. Information is becoming a strategic resource that may prove as valuable and influential in the post- industrial era as capital and labour have been in the industrial age. In the tactical field, in order to enhance the conduct of military operations, there is a need to integrate all aspects of information and accomplish its full potential.

Information is the foundation of knowledge based warfare. It enables commanders to coordinate, integrate, and synchronise combat functions on the battlefield. Commanders seek information dominance that defines how the adversary sees the battle space, creating the opportunity to seize initiative and set the pace of operations. There is a need to embrace the emerging information era as it is bound to have a major influence on operations. Successful integration of information systems is bound to affect the full range of military operations including contributions to increased lethality, survivability and operational tempo across the spectrum of conflict. In the Armed Forces due to various constraints we have to live concurrently with the past, the present, and the future families of equipment and associated technologies. While the process of jointness and integration is taking time, we have to optimise the use of modern systems being inducted in the Services progressively.

Appreciation of Situation

For undertaking tactical operations an appreciation of the situation is generally carried out. For evolving a plan of action some of the following factors are considered:-

- (a) **Ground.** It involves awareness regarding terrain including objectives and targets and battlefield transparency.
- (b) **Relative Strengths.** Strength of available enemy and own forces that can be employed for undertaking operations.
- (c) **Time and Space.** This factor has a bearing on timely completion of operations being undertaken as well as linkage with higher commander's subsequent plans.

Affects of advances in IT on different factors considered for conduct of tactical operations are discussed in succeeding paragraphs.

Ground

Battlefield Transparency.

- (a) **Digitisation.** Till recently for decision making, commanders relied on situation reports, marked maps with overlays, reconnaissance reports and intelligence summaries. The staff officers after piecing together the available inputs carried out analysis and generated alternatives to help commander in decision making. The digitised system depicts more accurately, own locations including subordinate units and sub-units as well as the enemy locations. The battlefield has become more transparent and more sophisticated means will have to be adopted for camouflage and concealment. It will provide sufficient details to enable commanders a better comprehension and situational understanding.
- (b) Network Technology. Sensor-shooter integration enabled by network technology and availability of intelligence, surveillance and reconnaissance assets like UAVs, drones, RPVs, and space platforms have increased battlefield transparency. During operation 'Desert Storm' the USA had no more than 15 per cent information on military significant targets. This figure increased to above 65 per cent during 'Operation Iraqi Freedom'.
- (c) Space: New High Ground. Rapid and responsive military operations require timely and accurate reconnaissance reports, weather monitoring, precise navigation assisted by Global Positional System (GPS) and reliable communication linkages. We need to have control of space, which empowers assets to detect, identify, monitor, track and even destroy enemy resources.

Relative Strengths

Lean Forces with Technological Superiority. Technology enabled lean but more lethal fighting force can succeed in offensive operations against numerically superior force which may not be possessing sophisticated weapon systems. This aspect got highlighted during 'Operation Iraqi Freedom'.

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

Lethality and Smartness of Munitions. Out of approximately 28,000 bombs dropped in Iraq, during 'Operation Iraqi Freedom' 70 per cent or so were smart bombs leading to an environment where "every thing that could be seen, could be hit, and everything that could be hit could be killed."

Time and Space

Time. In the past, commanders enjoyed a comfortable cushion of time as they approached the 'next hill'. Sensorto- shooter links have been automated to reduce the time lag between identification of target and decision and effective engagement. Ranges and lethality of weapons has increased and time to target has reduced. The trend of compression of time would increase in future leading to a higher velocity of warfare. An untrained commander will be seriously handicapped because of inability to act or even react in fast changing situations.

Space. The battle space has expanded in all three spatial dimensions. In part, this expansion has been the result of improved flow of information. Distance in battle space is no longer constrained by telecommunication technologies. Another factor is the development of rocket and missile technologies with longer ranges. This has further obscured tactical and strategic boundaries. There is a requirement to redefine battle space in the digital era. In a non-digital battlefield, operations require a linear concept of allocating troops to face a host of contingencies. In a digital battlefield we have time and information as the operational mobility can now match the intelligence and can exercise appropriate option.

Implementation of Tactical Operational Plan

Acquisition of Intelligence. During peace time the focus is on strategic intelligence involving use of satellites, sensors, interception and monitoring of adversary's networks and communications. Over a period of time database regarding adversary's orbit and details of formations and units is created. On mobilization during the concentration phase tactical intelligence must be built on the database already available. A doctrinal template of adversary's pattern of conduct of operations should be made and validated as more and more inputs become available. With the fielding of tactical Command, Control, Communications, and Intelligence (C3I) system, it will be feasible to generate near real time situational awareness. The digitised system is bound to be a good tool to create accurate, timely and useful picture regarding the enemy.

Dissemination of Information and its Use. A difficult challenge to the efficient use of information is getting the right information to the right place at the right time. To a certain extent technology can help in finding a solution. Proper placement of hardware, user friendly software, use of access codes, and so on can help in promoting functional efficiency. Information overload should be guarded against. To do so two alternate approaches can be adopted:-

- (a) Disseminate only information considered appropriate to the task in hand. The commander should be able to work with the available information.
- (b) Hold information in the central data base. The commanders and staff should be able to retrieve what is needed.

Unity of Command. It demands a clear comprehension of the doctrine, strategy and training needs at different levels. There is a need to make available appropriate resources at each level. In order to ensure reliability and flexibility, sufficient redundancy should be built while planning networks. System architecture should enable delegation and decentralisation.

Dispersion of Forces. Due to battlefield transparency, wide dispersion of forces with ability to concentrate quickly for offensive action would be required. Commanders will have to anticipate two or three moves ahead to optimise operational effectiveness. Mobility of forces in the area of operations should be ensured by appropriate means depending on the nature of terrain.

Manoeuvrability. Availability of adequate reserves and their employment at the appropriate time can be a battle winning factor. Reserves once deployed should be created again. Near real time flow of battlefield information can help the commander to anticipate well in time. This will help in maintaining momentum and subject the enemy to shock action. To exploit favourable situations, manoeuvrability of forces and flexibility of mind on the part of the commander are very essential.

Personal Dimensions of Command

Fielding of C4I2SR System. There appears to be a lurking fear of walking away from the personal dimensions of command into an impersonal cyber future. In actual fact many of the personal dimensions of command will remain unchanged and will assume greater importance. The fielding of tactical C4I2SR system will facilitate the commander to perform functions of command more efficiently.

Dissemination of Commander's Intention. The vertical and horizontal grid will facilitate dissemination of commander's intention in near real time in the formation. The digital format will facilitate a clearer picture and interaction among subordinate commanders so very essential for reaching a detailed and common understanding.

Physical Presence of Commander. Digitisation can help in building picture of when and where commander's presence on the battlefield will be crucial. This picture can be pieced together at an earlier stage than ever before. Commander should be comfortable with the information tools to facilitate his functions of command and yet be equally comfortable with standing on the jeep hood when the situation so demands. Subordinate commanders need to hear the tone of the senior commander's voice and the sense of urgency when the orders are given. Embedding of an audio network in the digital system to supplement orders passed on data network would be of help. Video teleconferencing can also help in projection of commander's personality.

Training of Commanders and Staff

Proper training needs to be organised to enable commanders and staff to become familiar with near real time availability of information and its form of presentation. In the information age commanders will have to get used to making decisions based on more accurate information than was previously available. After synergising doctrine, tactics, techniques and procedures; computer war games, telephone battles and exercises with troops should be conducted to enable all concerned to get a feel of the digitised environment and the likely way ahead.

CONCLUSION

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 have enabled greater connectivity and information sharing among widely spread force components. The concept of 'Network Centric Warfare' has been evolved for exploiting advancement in the field of 'Information Technology'. This concept rests on the premise that the power of a force grows proportionate to the extent of networking among weapons, sensors and command and control elements. The Indian Armed Forces are not yet ready for it. To attain the capability of switching to 'Network Centric Warfare', we need to do the following:-

- (a) Chief of Defence Staff should be nominated as per February 2001 recommendations of the Group of Ministers on "Reforming the National Security System".
- (b) Integrate regional commands.
- (c) Evolve a joint doctrine for fighting future wars.
- (d) Evolve joint communication architecture based on new technologies.
- (e) Progressive training to bring about attitudinal changes on part of the military leadership.

There is a need to embrace new information technologies to enhance the art of command and control at the tactical level. While the principles of conduct of warfare may not change, the information technology tools have vastly altered the breadth and pace of commander's actions. We should optimise the gains from information technologies and work out what needs to be covered during training at different levels in the interest of functional efficiency.

.Major General Y K Gera (Retd) was ADG SI and CSO Central Command; and Deputy Director and Editor of USI from 01 Jan 1997 to 30 April 2007.

Journal of the United Service Institution of India, Vol. CXXXVIII, No. 571, January-March 2008.