Future Role and Shape of The Corps of Signals

Lieutenant General Harbhajan Singh, PVSM (Retd)*

Introduction

The Corps of Signals will be celebrating its Centenary on 15 Feb 2011. It's journey through the last 100 years encompassing many wars and national emergencies, not only in India but in other parts of the globe, has been a saga of rich heritage. Signal communications have come a long way from heliographs, lamps and flag signalling to satellite communications, radio relay, internet and cell phone technology. This is an appropriate time to look at the future role and shape of the Corps of Signals.

Nature of Warfare

A revolution is taking place in the way wars are being conducted. This has been so visible in both the Iraq wars, NATO's actions in Afghanistan and the manner in which world's most powerful nations like the USA, China, Russia and NATO countries are organising and equipping their forces. At the heart of most military developments are the new systems and gadgetry incorporating latest electronics technology for surveillance, target acquisition and weapons. Nothing above the ground/sea seems invisible. Weapons delivered from the air, ground, and on and even below sea have become highly accurate and devastating. Electronics have made distances inconsequential.

In modern warfare, there is a need for sharing real time information amongst different echelons and components of a force, exercising effective command and control, keeping in view the urgency to speed up action employing the best possible assets, and to prevent casualties from friendly fire. Commanders and staff need up to date tactical picture of enemy and own assets much before the enemy is able to do so, in order to coordinate own effort and pre-empt him. Nuclear weapons have not been used in any of the conflicts so far, except towards the end of World War II, against Japan, but their mere existence affects the strategic thinking and measures have to be taken, for a rare contingency – if they are ever used.

Network Centric Warfare

This Doctrine has been propagated by the US Department of Defence and envisages 'translation of information advantage', enabled in part by information technology (combination of computers and communications) into a competitive advantage over the enemy. In order that information flows speedily vertically and horizontally, modern robust communication networks are necessary for real-time passage of information from the source to the decision makers and dissemination of plans and orders by them i.e. effective command and control.

This information would mostly be in the form of computer data, displays and overlays by various surveillance, intelligence and weapon systems, fighting formations, logistics entities as also command and control headquarters/ nodes. The associated computer systems would store and update required information, process it and the authorised users will be able to access the same. The system will ensure that every user has same information. The conventional speech and text messages would supplement them and will not be the prime means. Highly sophisticated electronics, communications and software technology is involved in developing such systems and make them interwork. The Corps of Signals will plan, provide and manage the networks on which this information will flow.

Electronics Technology Advancements. Increased micro miniaturisation, storage and processing speed and power leading to easily understandable displays, hand held devices, video, internet / intranet, voice recognition / voice operation seem to be the direction electronics research is taking. Convergence is the buzzword!! Nano technology may not be too far off!! Side by side is the increased use of wireless for mobile communications, based on higher and higher frequency bands, which means shorter ranges, requiring increased number of relays and communication nodes. For longer distances, satellite communications and lower frequency radios would continue. Fibre optics will continue to be used, particularly for backbone communications.

The Electronics Age. The world is experiencing the Electronics Age and electronics are all pervasive. The military is heavily dependent on electronic communications, computers, other electronic gadgetry and internet for conducting operations on the ground, on the high seas and for the air battle. The citizens, businesses, financial institutions, law enforcement agencies and important services like transportation, health care, water supply and the rest are equally if not more dependent on electronics and computers. Any disruption to these electronic systems can play havoc with military operations, functioning of the Government and daily lives of the citizens.

Information Warfare. Such technology or systems on which the military and daily life of citizens are so dependent become a critical resource and hence a target for enemy action or conversely targeting the enemy. Therefore, electronic warfare and cyber warfare, targeting communication and computer systems electronically, in addition to attacking them with kinetic or radiation weapons have assumed great importance. These therefore are important components of 'Information Warfare', as these target flow of information. (It is clarified that Information Warfare, called 'The Fourth Dimension of Warfare', encompasses some more important aspects like deception, managing perceptions and propaganda, which are not discussed here). While most of the offensive aspects are practiced during hostilities, intelligence gathering facets of Information Warfare go on even during no war conditions, the world over.

American General Omar N Bradley had once opined that 'amateurs talk tactics but professionals talk logistics'. However, in this era of Network Centric Warfare, military professionals should first discuss 'Information ascendancy'. Information ascendancy/superiority has two connotations. It entails safeguarding own electronic and information systems against enemy electronic or kinetic attacks and at the same time successfully attacking the enemy's electronic/information assets, circumventing the defensive measures he would take. The attack has to be dovetailed with the overall operational plan and so timed that the enemy is muted at the critical junctures in the battle. A force which does not have updated information about the enemy and own troops will be like a blind boxer, trying to throw punches but the same mostly missing the opponent!! To achieve success, great deal of technical intelligence gathering about enemy's information systems will have to be undertaken prior to commencement of hostilities.

(a) **Chinese Potential.** India has two likely adversaries who are challenging it's sovereignty i.e. China and Pakistan. China in particular is laying great emphasis on Information Warfare and this forms a very important aspect of Chinese Strategic Doctrine. China has set up a Cyber Base, which seems like Cyber Command, and raised Information Warfare brigades and divisions. This indicates an important direction of Chinese military modernisation. An important reality for planners of India's Defence networks must be to take into account Chinese capability to destroy satellites in orbit, which they have already demonstrated. There is another Chinese angle as well to be wary of. Indian providers of communication networks and power grids etc are using Chinese electronics components and hardware. It is possible to inject electronic sniffing, trojans and even virus producing bugs in such hardware/associated software, which could prove catastrophic when let loose. In this regard a short spy story is worth recounting here. Some Russian embassies acquired the US made photo copying machines. The Americans built in a chip, which recorded images of all documents photocopied. These were retrieved periodically by the maintaining crew. This was decades ago. These days much more sophisticated intelligence seeking and malfunction creating programmes can be inserted in chips.

(b) **Indian Capabilities**. The Corps of Signals, which is the electronics fountainhead, has taken some meaningful steps in this direction. However, there is a need for the top military leadership to lay much greater emphasis and accord very high priority to the offensive aspects of the Fourth Dimension of Warfare, as it is a very important force multiplier. No wars can be won without robust and sustained offensive action. Disabling/disrupting enemy's communications, computers and other information systems and at the same time safeguarding own, are the key for achieving information superiority, which is the aim of Information Warfare**.** India can and must surpass the Information Warfare capability of likely adversaries. We have the brains and electronics knowhow which need to be harnessed towards this goal. It is relevant to mention that India has youngsters like Ankit Fadia, who as a New Delhi based schoolboy wrote a book on hacking and was consulted by FBI of the USA for decoding terrorist messages dealing with 9/11!!!

Changing Role of Corps of Signals

Since its inception, the prime role of the Corps has been to plan and provide communications to the Army and to a limited extent to the Navy and the Air Force, primarily for command and
control. After Independence, it has been responsible for ushering in a number of electronics systems in the Army. These are as under:-

(a) Signal Intelligence

(b) Computers

(c) Electronic Warfare and lately

(d) Cyber Warfare.

Electronics and Cyber Warfare are key components of Information Warfare and are the prime 'force multipliers' in Network Centric Warfare. In order that the Corps of Signals can focus on Information Warfare, it needs to reorganise itself and allocate additional resources, for raising new units. It should be formally assigned the role of 'Information Warfare' and 'Ensuring Information Superiority'. Accordingly, its personnel ought to be called Information Warriors.

The Corps of Signals has excelled in harnessing new technologies for developing state of the art networks for command and control. It has put in place automated modern networks like Plan AREN, ASCON, AWAN and Tactical Communication Network (TCS). These require reduced intervention by Corps of Signals operators, and commanders and staff can make use of them directly. This is gradually changing the role of the Corps of Signals from 'Operating' to 'Network Planning and Provision'.

Greater Emphasis on ISTAR (Intelligence, Surveillance, Target Acquisition and Reconnaissance) Systems and Communications. Modern communication networks have been given acronyms command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR). The British use the Acronym C4ISTAR (TA stands for Target Acquisition). ISTAR part of C4ISTAR systems and networks are critical to achieve victory over the enemy in a Network Centric Warfare. The development of networks, therefore, requires greater focus and priority. Presently these systems and associated networks are being developed in isolation by different agencies. It would speed up matters, if a PMO (Project Management Organisation) is set up to coordinate, integrate and expedite development of such networks. The Corps has to ensure that these activities meet the set technical standards, are interoperable and can fully integrate with C4ISTAR.

Electromagnetic Weapons. These are a type of Directed Energy Weapons which use electromagnetic radiations to deliver heat, mechanical or electrical energy to a target to cause damage. They can be used against humans, electronic equipment and military targets, depending on the technology used. Research on such weapons needs to be carried out on high priority and the Corps of Signals should give the required impetus.

Low Intensity Operations. India has gained considerable experience in Low Intensity Operations. These are mostly conducted at company and platoon level. Electronic Warfare has played a key role even in this kind of warfare. Greater degree of Electronic Warfare capability should be inbuilt at battalion level and individual soldiers provided communications.

Cyber Warfare. It covers three areas – intelligence gathering, defence and attack. A beginning has been made by the Corps of Signals in Cyber Warfare. But the emphasis seems to be on defensive aspects. We should take a leaf from the USA and China, who have set up Cyber Commands. There is a need for building-up offensive capability.

Communication Networks in the Army

Communications at Corps Level and Below. The communication infrastructure down to Corps Headquarters is static, has been planned and stabilised over a number of years. It has more than one layer / alternatives and as such has resilience. Its operation and network management should pose less problems. The communications in the Field Force i.e. at Corps and below would need to be mobile and flexible, and require re-engineering quite often. These are also likely to suffer more damage as well; the degree would increase while going down to divisions, brigades and battalions/regiments. This is the area where active operations take place, which decide the outcome of a war. Also, reaction time is the least at these levels. Therefore, need for additional layers of communications in field communications cannot be over emphasised. In addition, more equipment and manpower resources would be needed, including reserves, and should be built-in the establishments.

Artillery Networks. Artillery (missiles, rockets, guns, mortars) is the most potent component of any Army, coupled with close air support including armed helicopters. They require the fastest, most secure and robust communications. The Corps of Signals should take a lead role in developing and integrating networks for fire support, so that these are fully integrated in C4 ISTAR.

Planning for Nuclear Environment. The possibility of a nuclear war is remote. However, fool proof communications with 200 per cent redundancy need to be catered for nuclear assets and constantly tested and reviewed, to meet any eventuality, howsoever remote.

Recommended Signals Set-Up at Corps Level. The following recommendations are made :-

(a) **Information Warfare Brigade.** It is recommended that an Information Warfare Brigade be made an integral part of each Corps. It should comprise an Electronic Warfare regiment and a Cyber Warfare regiment. A separate regiment is also needed for providing intelligence, surveillance, target acquisition and reconnaissance (ISTAR) network, so that their needs are taken care of by a dedicated Signal unit.

(b) **Command and Control.** The Chief Signal Officer at Corps Headquarters will be the overall commander and adviser on Communications and Information Warfare as also Electronic Warfare, on the lines of a Commander Corps Artillery (CC ARTY). The Chief Signal Officer will have to spend much more time on Information and Electronic Warfare aspects than hitherto fore and should be authorised required staff for this purpose.

Concluding Remarks

The Corps of Signals is gearing up for Network Centric Warfare as part of Revolution in Military Affairs (RMA). The military, functioning of the Government and life of citizens is heavily dependent on electronics communications and computers. Information Warfare is a fall out of heavy dependence on and criticality of such systems. China, the USA and NATO countries are laying great stress on this Fourth Dimension Warfare.

Modern static communications / backbone networks have been well developed by the Corps. However, the capability of China to destroy satellites in orbit is a potent threat to integrity of satellite based strategic and tactical networks. This needs to be taken serious note of. The architecture of communications at Corps and below has to have a number of layers with a view to ensuring their survivability against kinetic and electronic attacks.

Development of systems and networks for ISTAR portion of C4ISTAR needs greater urgency and focus. Their development should be put on fast track and a Project Management Organisation (PMO) set up for this purpose. Development of Electromagnetic Weapons should also be accorded priority.

The users are now able to pass their own messages, data and dial telephone calls. This has resulted in gradual dilution of operating role of the Corps and the emphasis is shifting to network planning and provision.

The growing importance of Information Warfare dictates that it should be formally made a primary role of the Corps of Signals and the Corps tasked to ensure information superiority, for which offensive aspects of Information Warfare need much greater emphasis. It is recommended that an Information Warfare brigade be raised as part of each Corps, with the Chief Signal Officer acting as the adviser to the Corps Commander, on the lines a CC Arty is for artillery. Informatics has brought about the Fourth Dimension Warfare and India should try and excel in this very important facet of RMA, for which the Nation has the required brain power and wherewithal.

***Lieutenant General Harbhajan Singh, PVSM (Retd),** of the First Course National Defence Academy and 10th Regular Course IMA, was commissioned into the Corps of Signals in Dec 1952. In 1971, after attending EDP Training in the USA, he started formalised Computer Training in the Army at MCTE, Mhow. He retired as Signal Officer-in-Chief in Jan 1991. Post retirement, he has been writing on National Security and Military matters.

Journal of the United Service Institution of India, Vol. CXL, No. 582, October-December 2010.