INFORMATION TECHNOLOGY AND CHANGING FACEOF WARFARE

> A downsized force and a shrinking defense budget result in an increased reliance on technology, which must provide the force multiplier required to ensure a viable military deterrent...Battlefield information system became the ally of the warriors. They did much more than provide a service. Personal computers were force multipliers.
>
> - Gen Colin Powell [1]

The battle cry of the communication revolution is "better, faster, cheaper." The only field where cost is continuously falling down with improved performance is Information Technology field. The fusion between computers and communication is complete. A $2000 laptop is more powerful than a computer worth 10 million dollar 20 years back. A 3 minute New York London phone calls in 1930 would have cost $ 300 in today's price, today it costs less than $10 and quality of speech is much better.

The revolution in information technology is also causing revolutionary changes in how warfare will be fought in today's information age. All over the world there is a dramatic reduction in cost and increase in facilities in all information technology fields. Cost of making a telephone call, sending a mail or data have come down drastically whereas the computing power of computer is increasing dramatically with rapid reduction of cost and size. The software interaction is becoming more versatile and more user friendly and fantastic facilities are available in these softwares. All the latest technology such as the Global Positioning System (GPS), satellite surveillance, fibre optic communication, Direct Broadcast systems (DBS), internet access, cryptography, sensors and precision weapons are commercially available in world market. Technology is improving the methods of obtaining and disseminating information. Though technology can be seen as a force multiplier, the limitations of information and technology as tools of war need to be recognised and their risk assessed. The success of the coalition forces at Persian Gulf war has drowned the lessons of the Vietnam war learnt by US Armed Forces. All the technical advantages of USA at Vietnam could not win the war for them . The "crude" forces defeated high technology force at Vietnam. One should not forget that "All the information in the world will not help poorly motivated, badly trained and undisciplined soldiers led by indecisive leaders fighting without a sound doctrine ".[2]

New Information Technologies. Much is being written about Information Revolution and Information Warfare. This revolution is based on many new Information Technologies which are listed in table 1.

Table 1. New Information Technology [3]	
Computer Aided Design Paperless Manufacturing Groupware On line services Document Management Customer Service Techno- logy Point of Sale Terminals Servers Networks Database Printers Voice Recognition Storage Protection	Fax Machine Scanners Pen Note books Flash Technology Advanced Fibre Optics Wireless Technology Video Conferencing Graphics Technology Data Compression Object orientation Virtual Reality Geographic systems.

Improvements in Warfighting due to Technological Changes Some of the improvements in the way future wars would be fought are:-

(a) Improved information integration speeds the decision making cycle by processing and distributing information more quickly.

(b) Information is force multiplier. It allows efficient allocation of scarce assets and improves target acquisition.

(c) The new systems provide fuller knowledge of enemy hardware, troop concentration, environment and terrain. Deny the same to enemy.

(d) At tactical level real time information on troop and force movements may permit more rapid and effective offensive or defensive actions. The side that loses its ability to detect the enemy and friendly situation will lose maneuver freedom.

(e) Information warfare techniques support "Information" attacks on political and economic infrastructure. [4]

Limitation and Risks Some of the limitation and risks due to improvements in information technology are :-

(a) The improvements of communications at the disposal of political leaders and military commanders has always carried the danger of

disrupting the chain of command. Senior commanders, with a real time picture of the battlefield, will be tempted to interfere in lower echelon decision.

(b) Stifling of initiative in subordinate commanders may be another problem. Even if the subordinates are not required to coordinate details with senior commanders, the junior leaders may be inclined to do so simply because the communication means are available. This could compromise initiative and undermine the effectiveness of command.

(c) Another danger is data overload. The danger now is that commander will be so bombarded by such a large volume of even unessential data that it will obscure the real issues that have to be interpreted. This is subjective and depends upon the intellectual capability and personality of commander and his staff. For example arguments are still raging about accuracy of bomb damage assessments in Gulf War. It is reported that a group of senior Marine Corps officers of US Marine Corps led by the Assistant Commandant of the Corps visited New York Stock Exchange to learn how brokers absorb, process and transmit the vast quantities of perishable information that are the life blood of the financial market. [5]

(d) Decision making tends to get bogged down due to "paralysis of analysis". Commanders wait for the last piece of intelligence that never comes.

(e) Rapid proliferation of information technologies particularly reduces the ability to achieve surprise.

(f) Improved information connectivity and distribution increase tension between operational security and effective planning.

(g) Vulnerabilities have increased as commercial tele communication networks and military networks are linked and interdependent. US Department of Defence relies on commercial telecommunication network for more than 95 percent of its information traffic. 6 This can be easily targeted by enemy.

(h) Given time, technology gap can be closed by enemy suddenly.

(j) Technology extends the time needed to develop new weapon systems reducing the speed with which they could be replaced in time of war.

(k) Is it better to have a larger force with lower technology or a smaller one tied to advanced systems? The larger force is more expensive in terms of maintenance while the smaller one costs more to procure.

(l) Though the command communication have become both increasingly important and vulnerable, disrupting enemy communication could be counter

productive,if they have been yielding valuable intelligence or if the enemy then resorts to communication that are not susceptible to monitoring.

(m) Gulf War gave a wrong impression that war can be nearly bloodless. All the munitions used in Gulf war were not PGM. Only 6.2 percent of munitions used in Kuwaiti Theatre of Operation in DESERT STORM were precision guided.

(n) Possession of superior technology does not ensure its effective use. This can be countered for example, chaff used against radar. In a May 1994 letter to Military Review. Capt William Uemura reported his observation on a tactical operation centre during Operation Desert Storm, "Staff officers...cranking out large operation orders with their new laptop computer. It was a terrific tool, used badly".

(o) Non battle tested equipment may not perform to expectations. Performance of patriot missiles was a butt of joke in Israel.

COMMUNICATIONS

> "If there was a World War - III the winner would be the side that can best control and manage the Electromagnetic Spectrum"
>
> - Admiral Thomas H Moorer,
> Chairman of US Joint Chief of Staff.

War in Information Age would depend on electromagnetic spectrum dominances. This is as important as say air superiority. Sophisticated communications systems and data networks are the backbones on which Information Warfare would be fought. With the expertise available today both inside the services and outside in business, phenomenal communication infrastructures can be built up which some time earlier one could not even imagine. The USA did not have much communication capability in gulf when Iraq invaded Kuwait. Yet at the peak of gulf war the communication systems provided could handle 7,00,000 telephone calls and 1,52,000 messages per day. The communicators managed and monitored over 35,000 frequencies to ensure interference free radio connectivity for the theatre. It was the largest single communication mobilization in military history. The communication systems used 118 mobile ground stations for satellite communication supplemented by 12 commercial satellite terminals. However, this was to be done by improvised methods. A group of innovators who by unorthodox and unauthorised use of military and civilian informationware discovered how to bend the rules, end-run the bureaucracy and exploit the off the shelf hardwares and software to get the job done promptly.[7]

Some important aspects of communications which should always be kept in mind are :-

(a) The bandwidth used should have the capacity and flexibility for the full flow of data. Commander's critical information requirement must be met. Do not send critical information over jammable fragile media. Do not send high volume information over narrow, slow media. In the communications bottlenecks do not choke decision maker's communication with less important transmissions.

(b) The communication systems should be robust, Off the shelf equipment has its own vulnerabilities, fragility and limitations.

(c) Communications systems should be electronically survivable. Proliferation of various means would increase survivability. Hiding of command control and communications systems, use of small, movable COMSAT receivers, burying of field and fibre optic cables, use of redundant pathway, keeping a back up communication plan, upgrading of communication systems would go a long way in making the communication systems survive in hostile electro magnetic environment. Avoid C3 standardization. Full standardization promotes vulnerability.

(d) The Command, Control Communication and intelligence system must be interoperable. That is why the system is called C4 I2 system. The incidents at Granada, where a US soldier could not get a fire support message passed to the US Navy ships lying in sight off shore and he had to call from a phone booth to Pentagon to get the same and the Air Task Order (ATO) in the Gulf war had to be printed, copied and carried to the Navy by hand because communications were incompatible, are well known. Such incompatibility can cause disasters in next war. [8]

(e) All armies acknowledge the need to maintain communications with the flanks and higher formations. In practice the link to higher and lower formations are given the most importance while the flank communications is given lesser priority. This is bound to happen in a hierarchical system like army because most orders and information flow from higher to lower formations. If communication is lost there is no alternative other than to re-establish it. However, in information age when hierarchical systems are going to be replaced by networked systems, commanders must maintain communications with the flank units and through them to other units to update the common ground picture.

(f) In a hierarchical organisation as the size grows organisational structures become more complex with greater layers. The organisations tend to be unresponsive, bureaucratic and top heavy. With the introduction of modern

communication means organizations all over the world are getting restructured and redundant management layers are being removed. The case of restructuring our defence forces organisations in view of the advances in information technology to provide more responsive organisations need to be looked into. For example, can we remove Corps HQ and have only Div HQs under a Theatre Command ? Toefflers stated "until recently 10,000 - 18,000 man division was thought to be the smallest combat unit capable of operating on its own for a sustained period. It would typically include three or four brigades, each with two to five battalions staff. But the day is approaching when a capital intensive third wave brigade of 4,000 - 5,000 troops may be able to do what it took a full size division to do in the past ".9 Currently the US Army is contemplating dramatic organizational changes. In a testimony before the Senate Armed Service Committee, US Army Chief of staff General R Sullivan stated, " We must continue restructuring our organisations, both tactical and administrative, to take full advantage of the ongoing technological revolution. The time has come to redesign the force for the 21st Century and the Army has started that process. We will call the force, Force XXI."

(g) However, one should not forget that more formidable, better trained armies have often been able to fight on even when their communications were inoperative. During the Normandy Campaign in 1944, the Germans often had to fight under conditions of radio silence. Yet sound tactical doctrine, good leadership at lower levels and sheer toughness allowed them to fight numerically vastly superior Allies to a stalemate for almost two months before attrition finally ground the German Forces down. 2

LEADERSHIP

"Wars may be fought by weapons, but they are won by men. It is the spirit of men who follow and of the man who leads, that gain the victory".

- Gen George S Patton.

Information technology and precision weaponry will not necessarily guarantee success on future battlefields Commanders must become experts on using information. By knowing the limitation of a sometimes coarse systems and the opportunities provided by Information Technology they can use it as a combat multiplier.

Change of Mindset. Eliot A Cohen writes "The new technologies will increasingly bring to the force the expert in missile operation, the Space General and the Electronic Warfare wizard - none of them a combat specialist in the old sense and a fair percentage of them, sooner or later, female. Military organisations still need, and will always need, specialists and its physical and intellectual demands have grown"5 The mindset of military higher echelons also have to change to

accommodate the push button soldiers and their General and should be given their dues. The tooth to tail ratio would reduce drastically. The United States sent 5,00,000 troops to the Gulf and there were 2,00,000 to 3,00,00 backup troops. The tail included the real 'stars' of Gulf War , American Software Soldiers, the computers programmers mostly civilians.

In future battlefield the combat arms soldier "is not a mere ammunition mule and bullet hose holder. He understands both mechanised and foot soldier tactics. He is skilled in the operation capabilities of helicopters and fixed wing aircraft, for he is most often the controlling agent. Directing aircraft means he understands antiaircraft weapons. He is skilled in geometry and navigation to direct mortars and artillery... Armor and anti armor, mine and countermine weapons and tactics, use of demolitions, computers, motor vehicles, laser designators, thermal sights, Satellite communications, gears are part of his kit"10. To operate in this environment a soldier has to be well educated, intelligent and of high quality. Toefflers argue that the Gulf War was a "high tech" War in which the human element in combat was eliminated is a fantasy. The forces sent by the allies to the Gulf War was the best educated and technically expert army ever sent to battle. Over 98 percent of US Army's all volunteer force at the time of Gulf War were high school graduates. Many were better educated than that. Gen Dennis J Reimer of US Army in a speech given to US Army Command and Staff College, Fort Leaveneworth on 13 September 1995 stated, " The individual Computer is a 'rock in a rucksack' and we must figure out how to make it better if we are going to get anything out of it. Right now, it has just added weight to the Infantryman and we have to do better than that. We must ensure that quality soldiers are there to handle Force XXI. " [11]

"Although many things in the world have changed, war in the future will continue to require well-trained, well equipped men and women who are willing to put their lives on the line and do the hard, dirty work of war.

There were no Silver bullets. Our forces must be more lethal, faster, better protected and versatile.[12]"

INDIAN CONTEXT

The revolution of Information Technology has started affecting all walks of life in India as well. It is but natural that the Armed Forces would also start using Information Technology for improvement in their capability to wage war. However, a realistic assessment of the available state and use of information technology should be made before we jump into any conclusion. One should not forget the propagators of information warfare are basically advanced high income countries with access to all the technology whereas we in India as part of South Asian Countries have a lot of catching up to do.

Personal Computer and the Internet are two indicators of level of information technology available to a particular country. A comparison between certain countries on these issues would not be out of place here.

Country	Number of PC per 1000 people	Number of Internet connection per 1000 people
USA	328	230.01
South Korea	120.08	6.53
Malayasia	39.08	2.08
Brazil	12.09	1.24
China	2.02	0.02
India	1.03	0.01
Pakistan	1.02	Negligible

Over the past three years, the number of computers for every 1000 people is increasing rapidly in both India and China. However, the gap between India and China seems to be widening. [Sources : World Development Indicators 1997] [13]

Human Resources Development

> "The instruments of battles are valuable only if one knows how to use them."
>
> - Ardent De Picq, Battle Studies

Current Information Technology systems can move information around automatically, change and highlight specific aspects and present same facts in various ways without human involvement. The user, whether a commander, staff officer or administrators sometimes gets confused. The Information Technology tool is available which should be understood and used by all.

Personnel of all arms need to be trained to operate and exploit the system. There is no way out but to learn basic minimum requirements to function in today's IT environment.

Today's Commanders and Staff may be provided with the following:-

* Intranets Respective branches and staff maintain servers loaded with constantly upgraded information on their area of responsibility. It would require robust communication support.

* E-mail It is likely to be the most assured way of ensuring that orders get to the recipient.

* Direct Broadcasting Satellites Fragile communication in the most intense stage of the battle can be overcome by use of Direct Broadcasting Satellites(DBS). Commanders would use narrow band, terrestrial, Combat Communications to call for information which is delivered from powerful satellite stations in the home base, in accordance with a predetermined schedule, direct to the terminal and display unit at the requesting HQ.

Ops Room Capabilities

The quality of information available to a commander should improve tremendously. The following would happen:-

(a) Paperless Ops Room. Future Ops Room would not be map free or paper free office, but paper used would be much less. Information will appear directly on the screens.

(b) Data Fusion Commander with access to number of servers maintained by respective branches or staff may need information fusion at ops room as well as presentation aids.

(c) Hypertext Information is likely to be presented in hypertext format i.e., click on the word and get more information. Staff would have to build hypertext structures which is a labour intensive task.

(d) Virtual Reality This may help commanders and staff to absorb complexity.

(e) Human Computer Response Presently for our interaction with information systems we are limited to keyboard and screen. More human response would be forthcoming with speech recognition system.

(f) Telepresence Remote controlled devices have started operating to deal with explosives. It would make its presence felt in mine clearing, recce and video conferencing.

Information Management Staff officers and clerical staffs in formation/unit headquarters will require to develop skills in Information Management. It is in this area that operational needs and technology interact

most intimately. It is for the operational staff to decide what information is needed by whom, how it should be presented, what is the pay off between speed and accuracy, what risks to be taken on security, who owns the information, who has the power to change and responsibility to upgrade or the access rights to read. The final requirement will be commanders who are unfazed by information in tetrabytes.[14]

The staff at fmn/unit HQ should be divided into following :-

(a) The Information Manager Responsible for the content and structure of the information and the channels and associated management structure for information dissemination.

(b) Cyber Librarian Maintains the Integrity of information and ensures that information structures support the plan of the Information Manager.

(c) Web Master Ensures the tools for using the technology eg the browsers and search engines are readily available and understood by all who need them. He also upgrades the system. He should be preferably a specialist.

CONCLUSION

"Changing any military's doctrine, however, is like trying to stop a tank armour by throwing marshmallows at it. The military, like any huge modern bureaucracy, resists innovation - especially if the change implies the downgrading of certain units and the need to learn new skills and to transcend service rivalries. To define a new doctrine, to win support for it both in the armed forces and among politicians, and then to actually implement it with trained troops and appropriate technologies is a tremendous task, and no one man, General or not, could possibly hope to accomplish it. It would take a campaign - one in which ideas would be the bullets." [15]

The competition for information is as old as human conflict. Nations, corporations and individuals each seek to increase and protect their own store of information while trying to limit and penetrate the adversary's. However, around 1970 extraordinary improvements in the technical means of collecting, storing, analysing and transmitting information started happening. This information revolution is showing no signs, of slowing down. This improvement of information technology will have dramatic impact on the battlefield and we, in the Armed Forces have to look into the great potential of this emerging technology. However, one should not forget that regardless of different technological levels of combatants on the future battlefield the side which have better leadership, better quality soldiers and unit training will be the winner.

BIBLIOGRAPHY

1. Colin L Powell, Information Age Warrior, Byte, July 92, pg 370.

2. RL Dinardo and Daniel J Hughes, Some Cautionary Thoughts on Information Warfare, Air Power Journal, Winter 1995.

3. US News and World Report, "The Information Technology," May 2, 1994.

4. Lt Cdr Jeffry A Harley, Information, Technology and Centre of Gravity, Naval War College Review, Winter 1997.

5. Eliot A Cohen, A Revolution in Warfare, Foreign Affairs, Mar-Apr 96 , p 43.

6. Maj Gen David L Grange and Col James A Velly Information Operations for the Ground Commander, Mil Review, Mar-Apr 1997.

7. Alvin and Heidi Toffler, War and Antiwar, Little Brown and Company, PP 76-79

8. Col Owen E Jensen, Information Warfare, Principles of Third Wave War, Air Power Journal, Winter 1994.

9. Toffler, ibid , p 76.

10. Ibid.

11. General Dennis J Reimer , Soldiers are Our Credentials, Military Review, Sep-Oct 1995, p 13.

12. General Gordon R Sullivan, A Vision for the Future,Military Review, May-Jun 1993.

13. Fact File : India and the World, The Hindu, 30 Jun 1997. p 16.

14. Maj Gen WJP Robins, OBE, Information Age Operation, Rusi Journal, Jun 97.

15. Tofflers, ibid, p 52.

Published in Combat, March 1998 issue.