Network Centric Warfare

Lieutenant General Davinder Kumar, VSM and Bar

Introduction

Warfare has undergone a sea change to keep pace with the digitisation of the battle-field. The wars in Afghanistan and Iraq have proved beyond a shadow of doubt that the future belongs to Network Centric Warfare (NCW). While the term NCW has been used extensively in various forums and literature, there still exists a halo around it, in that NCW is only to do with technology and technical Arms or Services. This article attempts to highlight this fallacy and contains no technical issues. To the contrary, it highlights the importance of the contribution of end users in realising our aim of becoming truly network centric.

Historical Backdrop

A comparison of the Iraq war with the ancient battles indicates that the principles of warfare remain the same, till date. What has changed is the following:-

(a) Space has enlarged disproportionately.

(b) Borders are no longer well defined. In fact they may be non existent.

(c) Time is a major constraint.

(d) Enhanced accuracy and lethality of weapons and munitions.

(e) Wars have become impersonal. There is no element of remorse.

Lieutenant General Davinder Kumar, VSM and Bar is the Signal Officer-in-Chief, Army Headquarters.

Excerpted text of the talk delivered at the USI on 3 November 2004.

Abbreviations used in Figures 1 to 6 are explained at end note 1.

Journal of the United Service Institution of India, Vol. CXXXIV, No. 558, October-December 2004.

(f) Erosion of value systems. Rules and prudence do not matter. All is fair in love and war.

(g) All pervasive high technology media.

(h) Convergence of computers and communications, resulting in shrinking of the Observe, Orient, Decision, Action (OODA), loop.

Even a cursory look at the above changes clearly indicates that these have been merely physical. Logically, nothing has changed. The principles of warfare have remained unchanged. Only the parameters of warfare have changed. This only reinforces our belief in the famous adage – The more things change, the more they remain the same.

Present Day Environment

Over a period of time, security paradigms have radically changed. Physical security in fact, occupies the lowest priority in the security spectrum. It is energy security and economic security which have higher priority. Disaster management capability, therefore, is as important, if not more, than war fighting capability. Asymmetric warfare, ranging from nuclear, biological and chemical (NBC) warfare to counter insurgency (CI) or counter terrorism (CT) operations, rather than conventional warfare, is the order of the day across the globe with the former being both a threat and a deterrent. An adversary will, therefore, seek to wage asymmetric warfare and cripple the economic and energy infrastructure by means of high precision lethal weapons and munitions rather than engaging military targets. Alternately, the adversary will launch cyber attacks to cripple the banking, railway or power grid systems. The only constraint in doing so would be perception management through a highly influential, potent and high technological media.

Today the terrorist threat is real. Each terrorist network is part of a complex network of autonomous terrorist groups, thus forming an international terrorist internet. In India, there exists a nexus of terrorist and insurgent organisations which operate in Jammu and Kashmir, North East and the hinterland areas of

Madhya Pradesh, Bihar, Andhra Pradesh, Chhatisgarh and Jharkhand which makes extensive use of the internet. These organisations have cyber savvy terrorists who use the worldwide web, e mail and electronic bulletin boards and are involved in hacking of sensitive national websites. It takes a network to beat a network. CI and CT operations, therefore, involve CI and CT grids which are nothing but networks. Hence, in its simplest form, networked warfare against asymmetric warfare already exists.

Underlying Technologies

Warfare is essentially technology driven. Some of the underlying technologies which have transformed warfare are given below:-

(a) Smart weapons and munitions have led to stand off strikes from long ranges with increased lethality and accuracy. 70 per cent of the 28,000 bombs used in the Second Gulf War were smart. Compared to 1.6 million rounds per man in the world wars, only 10 rounds per target were used in the Gulf War.

(b) Improvements in technology in the fields of computers and communications have led to real time and near real time decisions by commanders and a high level of sensor to shooter integration.

(c) State of the art surveillance devices have turned night into day, thus increasing the shared knowledge of battlefield conditions. While 15 per cent of information on military targets was available in Operation Desert Storm, this figure was almost 70 per cent in Operation Iraqi Freedom and is likely to be close to 90 per cent by 2005.

(d) The impact of technology on media has led to strategic decisions being influenced by public opinion and tactical decisions being taken at strategic and even political levels.

(e) Anti-technologies have emerged, which are more advanced than the technology they negate.

Impact on Battle Space

Three ingredients viz time, space and force, together define the velocity of warfare. Time has become highly compressed and operations are independent of night or day. This has led to the shrinking of the OODA loop due to increase in Information, Surveillance and Reconnaissance (ISR) assets. The sensor to shooter cycle has reduced from 72 hours in the First Gulf War to 12 minutes in the Second Gulf War. Space has enlarged exponentially and is the new frontier while cyber space is the new dimension. Force multipliers are increasingly being used with telling effect.

Evolution of Network Centric Warfare

The inescapable need for NCW has arisen due to the following reasons:-

(a) Simultaneous operations in geographically dispersed locations, widely dispersed Command and Control (C^2) elements, ISR and weapon platforms.

(b) The need to optimise employment of available resources within the time constraints.

(c) The need to counter asymmetric warfare.

What is Network Centric Warfare ?

NCW is a complex term given to a simple concept. Numerous definitions of NCW exist, each one probably more confusing and complicated, to a lay man. Its simplest definition is, "It is a product of convergence of computers and communications and its exploitation to bring to bear maximum combat power at the right time and at the right place".

No matter what the definition, the essence of NCW lies in translating information superiority into combat power by effectively linking knowledgeable entities in the battle space. NCW is premised on three hypothesis as under:-

(a) Information sharing promotes shared awareness across the networked force.

(b) Shared awareness improves collaboration and synchronisation.

(c) Improved synchronisation yields greater mission effectiveness because of the following :-

(i) Speed of command.

(ii) Sharing of resources.

(iii) Increased lethality, survivability and responsiveness.

Network centric operational concepts are based on:-

(a) Dominant manoeuvre.

(b) Precision engagement.

(c) Full dimensional protection.

(d) Focused logistics.

)omains of Warfare

There are three established domains of warfare (Figure 1)[1] ıs under:-

(a) **Cognitive Domain.** This encompasses the mind of the war fighter and his supporting populace. Intangibles like leadership, morale, training, public opinion and so on are part of this domain. Intent, doctrine, tactics, techniques and procedures also form part of this domain. Most battles and wars are won or lost in this domain. Put simply, it involves carrying out of appreciation and formation of operational directives and orders.

(b) **Information Domain.** Information is created, manipulated and shared in this domain. It facilitates communication of information among war fighters and needs to be protected to enable the force to generate combat power. Command and control and commander's intent are conveyed in this domain. In fact it is "Ground Zero" in the battle for information superiority. It involves collection of information, converting information to intelligence and passing of operational directives and orders.

(c) **Physical Domain.** This is the traditional domain of warfare and contains physical platforms and communication networks that connect them. Strike, protect and manoeuvre across the environment of ground, sea, air and space takes place in this domain. Combat power is traditionally measured in this domain. In simple terms, it involves actual destruction of the enemy.

Information Superiority

In NCW, information superiority is achieved by the integration of sensors, shooters and decision makers. The fundamental block for information superiority, which contains the sensor grid and shooter grid riding on the information grid (the network of networks) is shown in Figure 2. The geographical representation of the same is shown in Figure 3. The information grid provides the computing and communication back plane while the sensors and shooters plug into the information grid. Figure 4 is a simple depiction of networking of sensors, shooters and decision making entities in a human body to reiterate the point that the basics have not changed; only the parameters have.

Information Operations

Information Operations (IO) are inherent to NCW and are nothing but the actions taken to achieve information superiority by influencing the adversary's information based processes, information systems, communication and data networks. It is a deliberate attempt to gain access to, tamper with and exploit information and information systems of the adversary, while at the same time preventing him from doing the same to us. The components of IO are:-

(a) Command and Control Warfare (C2W).

(b) Intelligence Based Warfare.

(c) Counter Surveillance Warfare.

(d) Perception Management.

(e) Net Warfare.

(f) Electronic Warfare (EW).

IO consists of information dominance and information assurance. While the former is an offensive action the latter is a defensive action.

NCW Infostructure

The available infostructure is shown in Figure 5. It shows how the army information infrastructure is part of the defence information infrastructure, which in turn is a part of the national information infrastructure. Figure 6 shows the network of networks that would exist in any NCW oriented conflict. It is the seamless integration of these networks which provides the underlying infostructure resulting in network of networks – the essence of NCW.

Change in Tactics Due to NCW

The most common formation used by offensive formations in conventional warfare is the wedge formation wherein, as forward troops penetrate, the area behind is secured by units in close proximity. In NCW era, wedge tactics will be replaced by swarm tactics, wherein offensive formations operate as small battle groups in a wide geographical area. Technology allows soldiers to keep track of each other despite being out of sight. Move forward does not take place in any specific formation and there is no worry about securing the rear. The location of own and other friendly entities is known. When the enemy attacks, air cover is sent immediately to protect own force till support forces arrive. Joint warfare, therefore, is of paramount importance.

The benefits of swarm tactics are low cost of war, simultaneity of operations and ability to cover more ground and wide dispersion. In addition, it will be possible, through chat sessions, for any problem to be evaluated and shared by many in real time. However, the drawback of swarm tactics are isolation of troops, information overload and curbing the initiative of junior leaders.

In the Second Gulf War communications played a pivotal role and the war was "wired" as under:-

(a)	Surveillance (Sensors)	– Joint Surveillance Target Attack Radar System (JSTARS), Predator (unmanned drone).
(b)	Commuhication Platforms	– Predator, Line of Sight Relay Stations, Border Relay Station, Military Satellites.
(c)	Planners and Decision Makers	– Pentagon, Forward Commands, Tactical Operational Centres.
(d)	Weapon Systems	– Appache Longbows, M11A Abrams Tanks.

NCW In The Indian Context

The Indian Army doctrine on NCW which was released in October 2004 highlights the following issues:-

(a) Emphasis on Information Warfare.

(b) Creation of technological asymmetry to increase battle field transparency and situational awareness.

(c) Development of force multipliers with enhanced precision and stand off engagement capability alongwith sensors.

(d) Directive style of command.

(e) Perception management.

(f) Emphasis on command, control, communications, computers, intelligence, survellience and reconnaissance (C4ISR) systems.

(g) Investment in infostructure.

(h) Changes in concepts, organisational philosophies and attitudes.

(j) Impact on low intensity conflict and asymmetric warfare.

The above doctrine notwithstanding, a lot needs to be done to make us truly network centric. This includes:-

(a) Synergy at the national level.

(b) Jointmanship.

(c) Organisational adaptation.

(d) Single point accountability.

(e) Training and human resource development (HRD) policies.

(f) Indigenous technology base.

(g) Cryptography and analysis.

(h) Legal framework, particularly related to cyber space and cyber warfare.

(j) Specialised laboratories and focused research.

(k) Content management.

(l) Data bases and data base management.

(m) User involvement.

(n) Institutionalised international exposure and interaction.

What We Need to Do ?

The transition from platform centricity to network centricity will involve:-

(a) Radical attitudinal change.

(b) Formulation of a credible joint war fighting doctrine.

(c) Reduce decision making cycle by means of centralised planning and decentralised execution.

(d) Realistic organisational reappraisal and adaptation.

(e) National and organisational will.

(f) Prevention of fratricide by effective and fool proof identification friend or foe (IFF) systems.

While hard work, knowledge and luck are important for the success of any change, it is attitude which is most important and without which no change is possible. We would do well to remember that, "The most difficult thing in putting a new idea in a soldier's mind is to get the old one out". Hence change of attitude needs a conscious and deliberate effort at all levels.

At the micro level, we need to develop technology and anti technology, transform our command styles, increase user awareness and address issues of information assurance and cyber security. In addition, our tactics and training will need not only to match, but exceed the velocity of warfare of the enemy in all dimensions.

Conclusion

Future wars can only be won by forces which are network centric. NCW is one in which the threat is national and not graded or restricted to a few regions. It will affect all citizens irrespective of where they are and all war fighting elements will come into effect on day one. It will involve synergy at the national level in the areas of decision making, quick response, minimum collateral damage, disaster management, energy and economic security and awareness to counter psychological warfare. The migration path to network centricity will have to be traversed in a phased manner from the existing fragmented networks and stand alone automation systems to seamless converged networks and intelligent systems. Sooner rather than later, users will have to shed their inhibitions and cynicism with respect to information technology and be part of the NCW revolution. In short we will have to make haste slowly. "NCW is to warfare what e-business is to business".

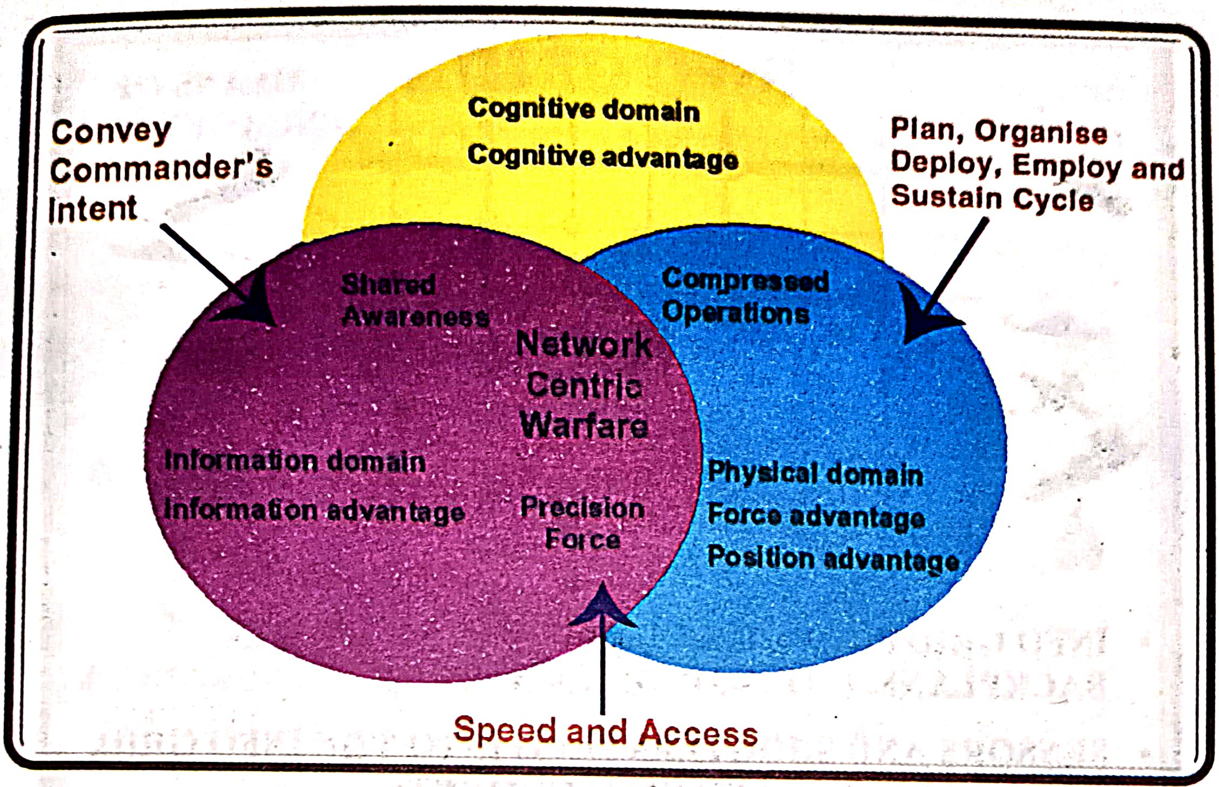


Figure 1 : Domains of Warfare

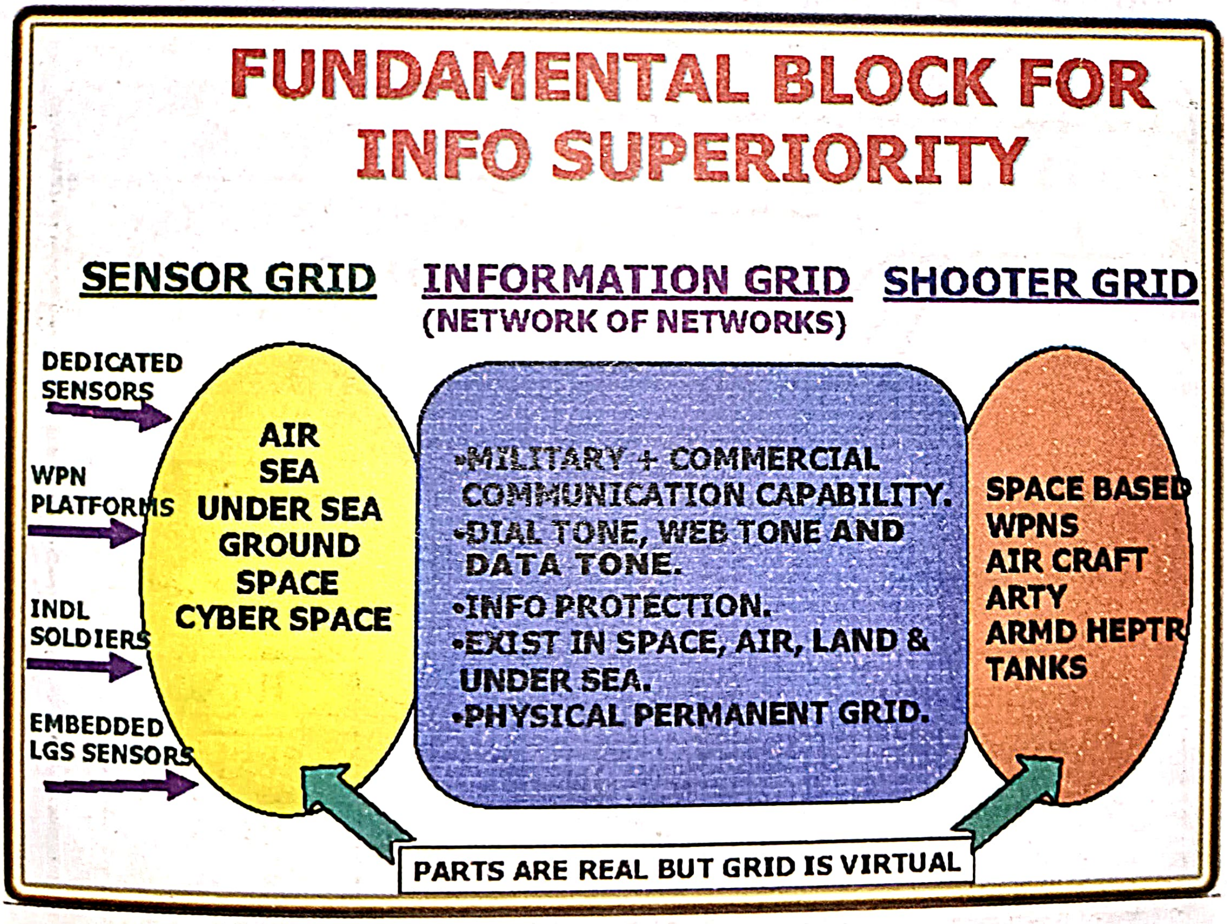
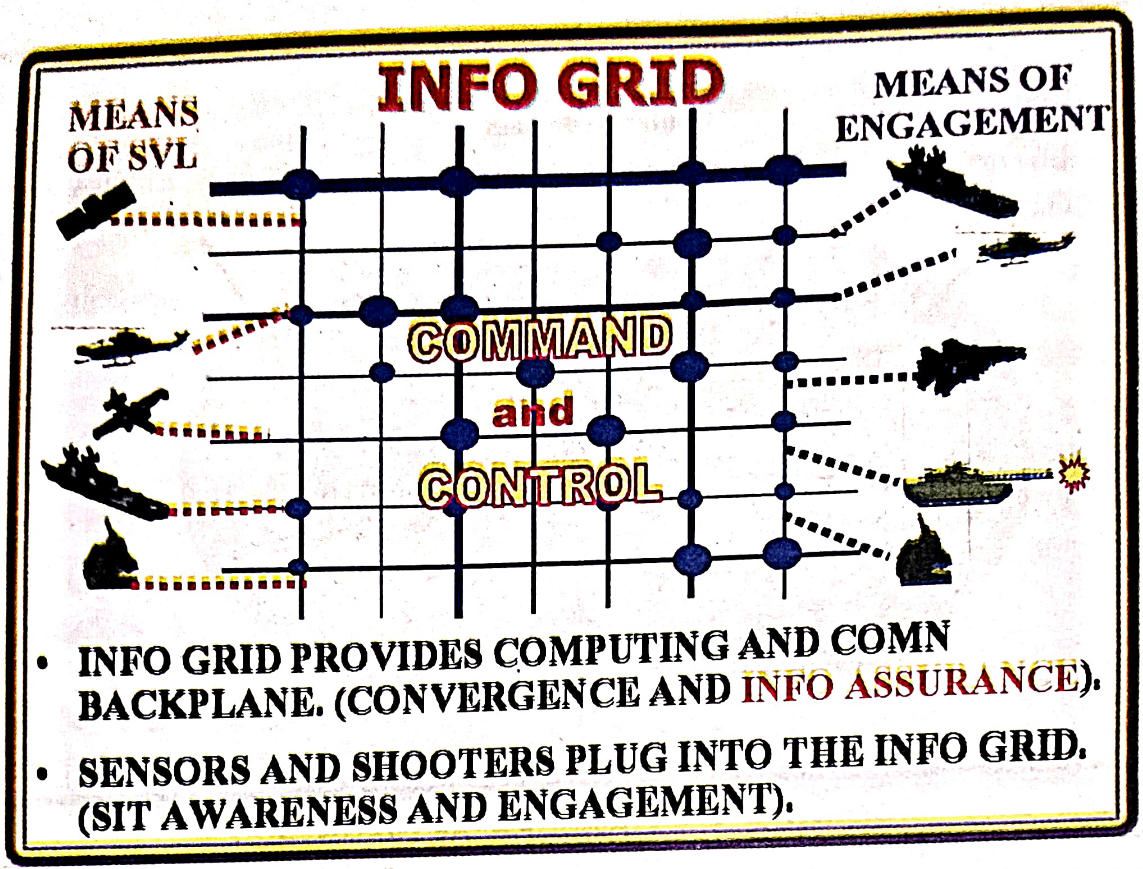
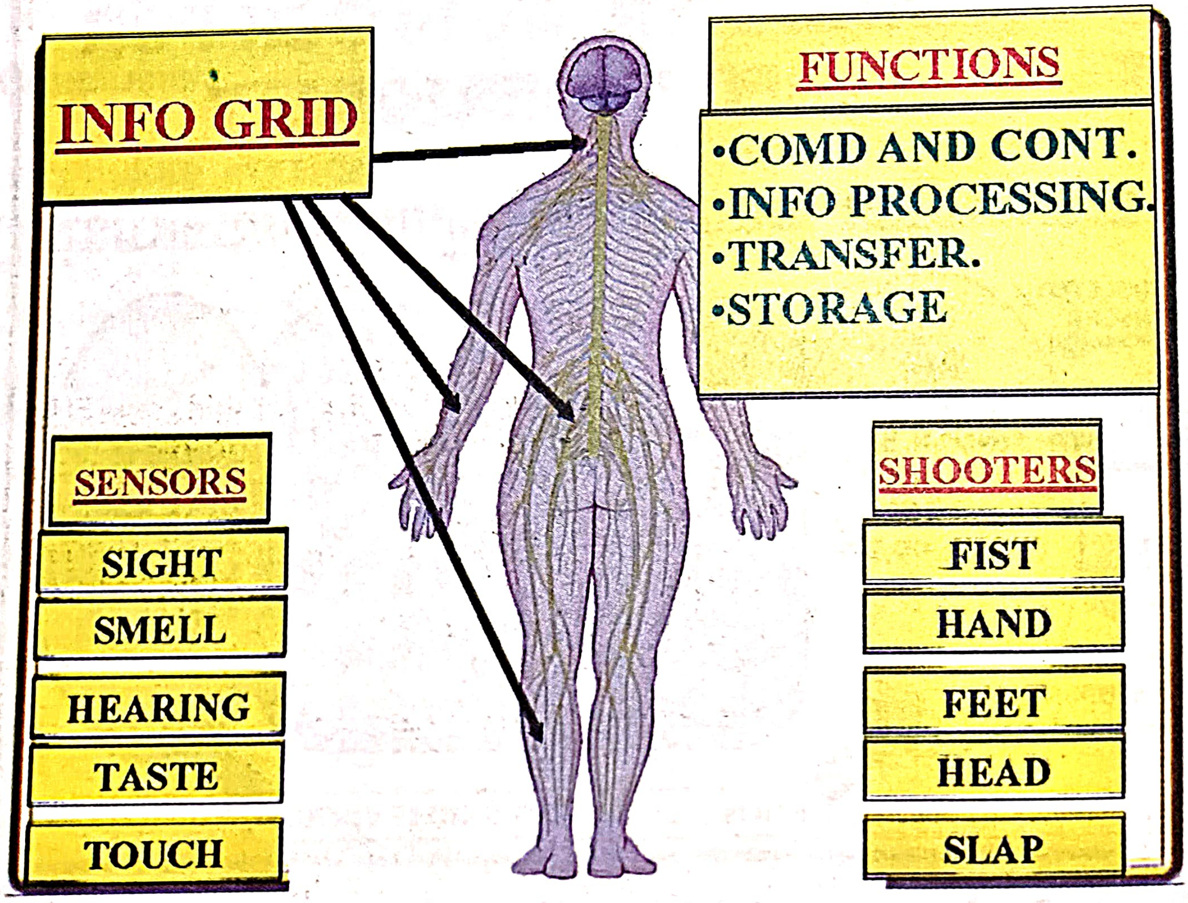


Figure 2 : Fundamental Block For Information Superiority



- INFO GRID PROVIDES COMPUTING AND COMN BACKPLANE. (CONVERGENCE AND INFO ASSURANCE).
- SENSORS AND SHOOTERS PLUG INTO THE INFO GRID. (SIT AWARENESS AND ENGAGEMENT).

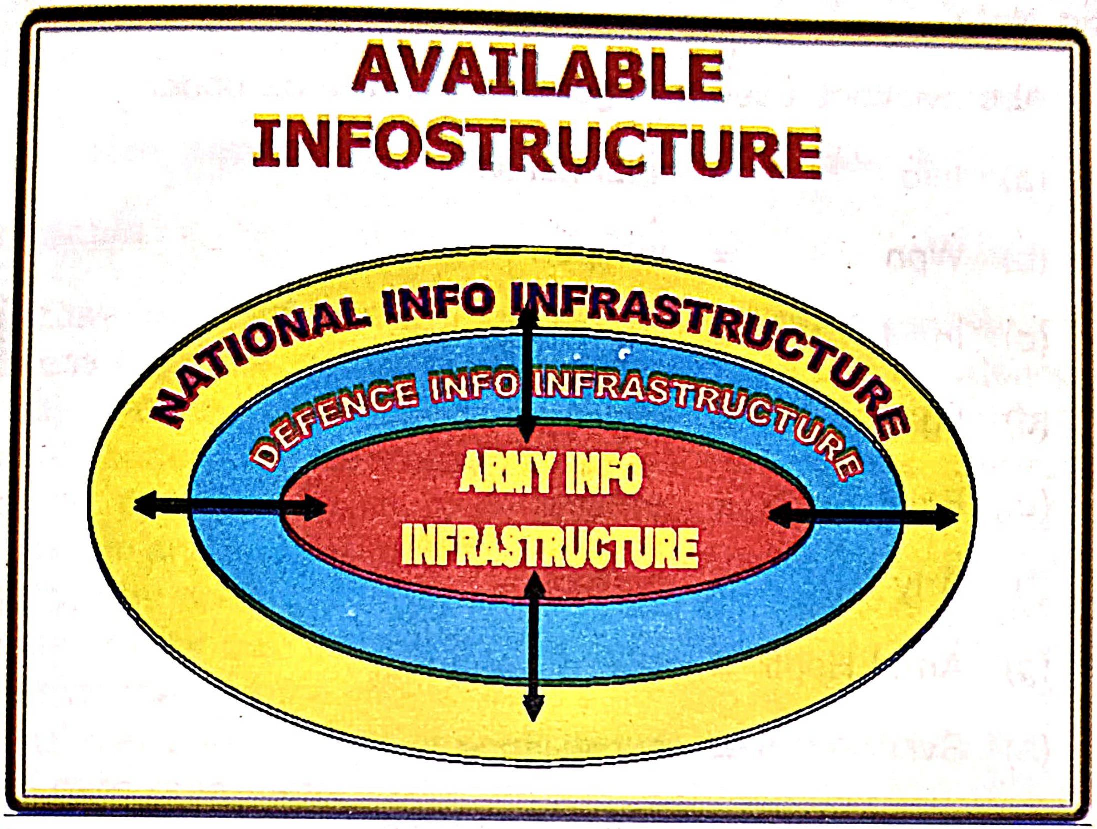
Figure 3 : Pictorial Representation of Information Grid



- •COMD AND CONT.
- •INFO PROCESSING.
- •TRANSFER.
- •STORAGE

SENSORS	SHOOTERS
SIGHT	FIST
SMELL	HAND
HEARING	FEET
TASTE	HEAD
TOUCH	SLAP

Figure 4 : Networking In A Human Body



AVAILABLE INFOSTRUCTURE

Figure 5 : Available Infostructure

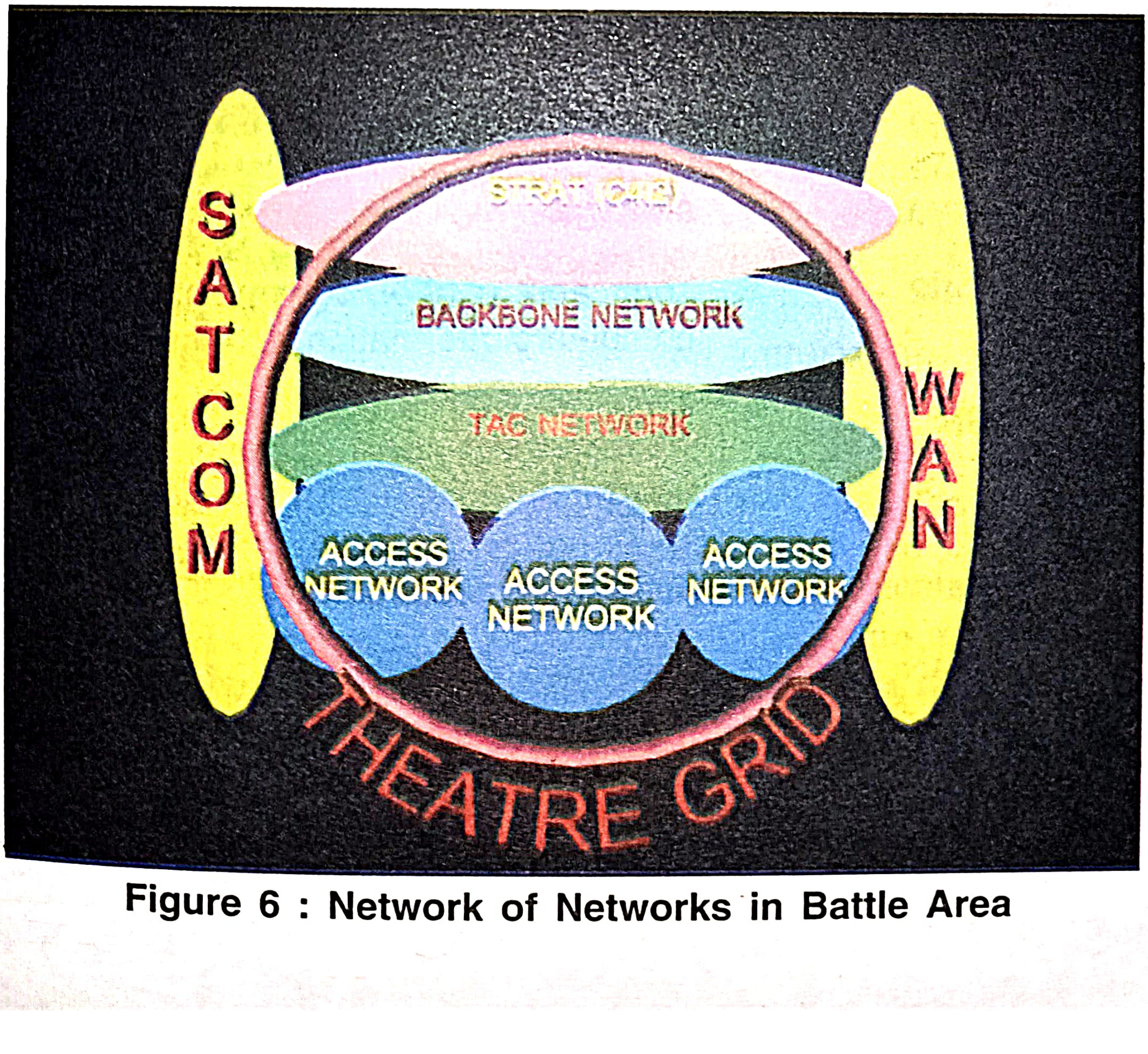


Figure 6 : Network of Networks in Battle Area

End Note

1. Abbreviations used in Figures 1 to 6 are as under :-

(a)	Info	=	information
(b)	Wpn	=	weapon
(c)	Indvl	=	individual
(d)	Lgs	=	logistics
(e)	Exist	=	existing
(f)	Arty	=	artillery
(g)	Armd Heptr	=	armed helicopter
(h)	Svl	=	surveillance
(j)	Comn	=	communications
(k)	Sit	=	situation
(l)	Comd and Cont	=	command and conrol
(m)	Strat	=	strategic
(n)	C4I2	=	command, control, communications, computers information and intelligence
(o)	Sat	=	satellite
(p)	Tac	=	tactical
(q)	Satcom	=	satellite communications
(r)	WAN	=	wide area network