CENTRE FOR LAND WARFARE STUDIES (CLAWS) – SP GUIDE PUBLICATIONS JOINT SEMINAR ON NETWORK CENTRIC WARFARE IN THE INDIAN CONTEXT SEMINAR REPORT

General

The Centre for Land Warfare Studies, in association with SP Guide Publications, organised a one-day seminar on 'Network Centric Warfare (NCW) in the Indian Context' on 21 April 2011 at Manekshaw Centre, New Delhi. Held in four sessions, the conference looked at various aspects of the subject by noted experts. While Dr VK Saraswat, Scientific Advisor to the Defence Minister, delivered the Keynote Address, Lt Gen Mohapatra, SO-in-C, gave the Valedictory Address. The seminar was well attended by serving and retired officers of all three Services, scientists, and members of the corporate world and strategic community. On the occasion, the second issue of the journal *Scholar Warrior* published by CLAWS was released.

Inaugural Session

Welcome Address: Brig Gurmeet Kanwal (Retd), Director CLAWS

This seminar is a joint effort by the Centre for Land Warfare Studies and SP Guide Publications. Net Centric Warfare is an important facet for present day and future conflict scenarios and remains an important subject for study. We at CLAWS have consistently been engaged in the study of NCW and towards this end we have had a series of conferences and meetings which have also resulted in a book. Today we have a galaxy of speakers to look at specific aspects of NCW and its relevance in the Indian context. We are also fortunate to have Dr Saraswat, Scientific Advisor to the Raksha Mantri, to deliver the Keynote Address.

Keynote Address: Dr VK Saraswat, SA to the RM

I have been privy to many developments in this field, especially in the Indian context. With the advent of micro technologies, there is an era of new revolution. They transformed from 'Systems' in the 1970s to 'System of Systems' in the 1980s to 'Family of Systems' in the beginning of the 21st Century; presently there is a 'Global Information Grid'. The Next Generation Network (NGN) is a packet-based network that is able to provide telecommunication services and able to make use of multiple broadband, QoS-enabled transport technologies and in which service-related functions are independent from underlying transport-related technologies. It enables unfettered access for users to networks and to competing service providers and/or services of their choice. It supports generalised mobility which will allow consistent and ubiquitous provision of services to users. Military NGN lies in multiple layers of convergence, which include Application Convergence, Network Convergence and Service Convergence. Here, IP is the core that provides authorised users with a seamless, secure, and interconnected information environment, meeting real-time needs of NCW.

NCW is the key enabling concept that underpins the country's Military Future Joint Operations Concept. It does not, however, dictate how the military intends to fight. The military's NCW capability will provide the means for transition from a network aware force to seamless, network-enabled, information-age force. It translates information advantage into a decisive war fighting advantage. Information advantage is characterised by shared battle space awareness, shared knowledge of commander's intent, self-synchronisation, speed of command, and rapid lockout.

Integrated command and control of networked forces provides a "common" operational picture and reduced "Fog" of War. It provides shared and significantly increased Situational Awareness (SA) for the Commander, Subordinate Commanders, and individual war fighters. This enhances decision making both in terms of speed and quality of decisions. It also increases tactical agility and significantly reduces risks.

Satellite technologies of the future are critical to military operations. Satellites in general are becoming more capable, with higher power and larger aperture antennas to

promote frequency re-use and creating highly capable “super-computers-in-the-sky”. With electronically formed beams, the beam patterns can be re-formed on command to respond to needs at different times of day, or of changing requirements that emerge in response to market demand. Future technologies include Advanced Phased Array Antennas, Dynamic Beam Management, Advanced Antenna Systems, more efficient power systems, Turbo-coding, Advanced Modems, and new materials for light weight antennas (Inflatable Antennas).

In the Indian context, future NCW involves three domains:

Information Domain: It has disruption technologies to create theatre or battle space blind spots. These include cyber warfare, anti-satellite weapons, under water warfare, and directed energy weapons.

Physical Domain: It involves contact-less wars, missile warfare, submarine warfare, directed energy weapons and space control weapons.

Cognitive and Social Domain: It comprises asymmetric strategies, tactics and operational plans, doctrine to match threat assessments, local and limited conflicts under nuclear hangover.

Session 1

NCW and the Indian Armed Forces: The Present Status and Concerns

Tri-Service Effect Based Operations - Brig LB Chand, VSM, DACIDS JCES (Ops), HQ IDS

The integration of communications is taking place at the strategic level. All networks are designed and intended towards a target. The integration is taking place Corps HQ downwards and thereafter at the lateral level. Each network/usage of technology varies between Army, Navy and Air Force. Effect Based Operations (EBOs) are considered

one rung up higher in net-centricity as they are better conceptualised and quantified in today's context.

Implementation of this strategy was put into effect for the first time by the US. The USAF during the Gulf Air Campaign used EBOs that came to be known as *Parallel Operations*. The military and leadership is targeted sequentially in EBOs. Air Defence mechanism along with leadership as well as vital installations are also targeted simultaneously.

EBOs could be defined as a parallel campaign, targeting the full spectrum of the adversary (DIME-diplomatic, informational, military and economic) with the aim of achieving a pre-determined effect. EBOs are conceived and planned in a systems framework that considers the full range of direct, indirect, and cascading effects, which may, with different degrees of probability, be achieved by the application of military, diplomatic, psychological, and economic instruments. EBOs therefore, are a coordinated set of actions aimed at shaping the behaviour in times of peace, crises and war.

EBOs are a paradigm shift from Networks to Networking; the tenets of EBOs are as follows:

<u>Networked Operations</u>

Faster Targeting – Network enabled force in physical and cognitive domain leads to a shorter observe-orient- decide- act loop.

More Efficient Attrition – operations are target/objective based and enable optimum selection and utilization of the weapon system.

Man Out of the Loop – More efficient attrition is obtained by taking man out of the loop.

<u>Networking</u>

EBOs – Tackle both social and physical connectivity to achieve a desired effect.

Dealing with exploiting complexities of security, defence, economic and social.

Supporting Man in the Loop – The effects (both positive and negative) spiral into an avalanche effect once the leadership is targeted.

As a concept, EBOs are still evolving with different tracks being followed.

Effect Based Targeting – Primarily employed by the Air Force.

EBOs - Determine an end state – Army Commanders work towards defining an objective and along with supporting commanders effectively employ their resources to accomplish that end state (effect).

Shaping the Behaviour of Friends, Foes and Neutrals – Military/ Political/ Diplomatic/ Economic Means. EBOs would target the political, social and physical targets, leading to a desired effect both physical and behavioural by employment of full spectrum of national potential – political, military, economic, social, infrastructure and information. In the Indian context, EBOs are inclusive of a Grand Strategy which, deals with the full range of issues associated with the pursuit of national interests; encompassing diplomatic, information, military and economic strategy of the nation. Accordingly, there are four levels of war described as follows:

Grand Strategy Level – Joint Vision describing the national security objectives by the Cabinet Committee on Security (CCS).

Military Strategic Level – Deals with the application of military resources to achieve the national security objectives (Higher Defence Organisation).

Operational Level – The link between the strategic and tactical level and provides connection between the military strategic objectives and tactical employment of forces.

Tactical Level – The level at which unit/sub-unit operations are conducted; this level focuses upon the application of combat power to defeat the enemy.

In conclusion, the critical areas requiring focus in reference to the subject are policy on interconnect and integration of service networks, applications, intelligence and information and government-level organisational set-up. Insofar as the Indian score card is concerned, it could be placed at best at 55.58 per cent.

Indian Army's March towards Net Centric Warfare: Maj Gen DV Kalra, VSM, (Retd) former ADGIS

Technology has widely affected the battlefield environment in last few decades. The technological boom in today's battlefield milieu has contributed towards increased intelligence and surveillance capabilities. Technological advancement has provided enhanced weapon range, accuracy and lethality. Technology has also culminated in improved data transmission with increased volumes with high speeds. The impact of technology has provided us with faster processors and miniaturisation.

Network centric warfare is an information superiority-enabled concept that generates increased combat power by robust networking of sensors, decision-makers and shooters to achieve shared situational awareness, increased speed of command, higher tempo of operations, focused application of fire and increased survivability, which leads to enhanced mission effectiveness. Network centric warfare involves transforming information superiority into combat power by effectively linking knowledgeable entities in the battlespace. It generates precise war fighting effects at high tempo at the operational level. NCW focuses on co-relation between speedy attainment of operational level aims and strategic objectives.

Information Technology (IT) vision of the Indian Army includes transformation into a dynamic network centric force, achieving information superiority through effective management of information technology. Indian Army has made adequate progress in Geo Information System (GIS) which provides the spatial orientation and context to the OIS and MIS system. It forms the base over which the other functionalities and applications ride. The modern GIS system includes features of network analysis, 3D visualisation, flythrough & simulation. A few of them also possess the image processing and change detection. Army Strategic Operational Information Dissemination System (ASTROIDS) is a secure information dissemination system which connects Army Headquarters with Command and Corps Headquarters for exchange of terrain, operations intelligence and logistics information.

Command Information and Decision Support System (CIDSS) is the hub centre of tactical C3I which connects Corps headquarters to infantry battalion. It has computer nodes linked through suitable communication media and provides processed information to commanders and staff on terrain, operational, intelligence and logistics functions for decision making. Battlefield Support System (BSS) has been developed to provide an automated data fusion of surveillance devices and operational information system to commanders at field force level so as to facilitate decision making in battle in near real time. Artillery Combat Command and Control System (ACCCS) and Air Defence Control and Reporting System (ADC&RS) are in their advance stage of development. Indian Army is making conscientious efforts to overcome various challenges thrown by fielding of new system.

NCW: Strategic to the Tactical: Col KPM Das (Retd), Vice President, National Security and Defense Solutions, CISCO

The levels of war are doctrinal perspectives that clarify the links between strategic objectives and tactical actions. There are no finite limits or boundaries between the levels of war; strategic, operational, and tactical (SOT) and the levels of war are not necessarily associated with specific levels of command, size of units, types of equipment, or types of forces or components. However, certain commands tend to operate at particular levels of war, e.g. Army Commands typically operate at the strategic and operational levels of war while a Corps will typically operate at the operational and tactical levels of war. Actions are strategic, operational, or tactical based on their effect or contribution to achieving strategic, operational, or tactical objectives. It is difficult to decide exactly where a strategic movement ends and a tactical movement begins, yet in conception the two are distinct.

NCW can be easily equated to preparation for a good and well planned game of football to draw out relevant inferences. Both have few rules and few opportunities to restart play on favorable terms. In both cases every player to be aware of the field, the person who is controlling the ball, where the ball is on the field, capabilities and positions of

own and rival players and dynamic interactions of these factors. Both NCW and game of football teach fresh players to play specific, limited roles, standard/copybook situations. Mature players are given more freedom, more responsibilities, with an aim to create positional advantage to own team. At the highest level of the game or NCW, play is fully fluid with complex moves and changing. Both situations demand ability to sense, react and attack with minimal verbal communications.

NCW poses a varied set of challenges which necessitate due attention of command and staff at all times. Some of them are asunder:

Bandwidth is as much a resource as ammunition and Spectrum is as much a resource as weapons.

There is a need to Include separate section in Operational Orders (OO) of formations.

There is also an urgent need to include equivalent of G6 in Div Staff (Signals) responsible for bandwidth, spectrum and cyber-security.

Convergence of ICT, Cyber security and Information Security under single agency in the battlefield and mutual synergies.

Reach to information is related to richness of information. “Richness” of information helps quality of interactions. The information should be finally available to the soldier on ground in a simple usable form. NCW is not a technical game as most of us think it to be. It cannot be left to few highly technical persons in the organisation. Technology has to be inducted into everyone involved in the system. Training with network-centric-architecture is necessary for readiness into battle.

Session II: Future Prospects and Challenges for NCW

Chairperson: Lt Gen VK Kapoor, PVSM (Retd), SP Guide Publications

Before we delve into the concept of Net centric warfare (NCW), it is important to look at its foundation. It is the concept of operation to achievce out strategic objective of war with least amount of tactical force. More importantly, NCW needs to be used *skillfully*. The future wars between two states under the nuclear hangover is highly unlikely. The Indian Army was not even allowed to cross the border during the Kargil War.

If this is the reality, then what kind of wars are we looking at for in the future? Undoubtedly, the arrow points at NCW. At this juncture, its important to question that what is the kind of force that will be used in this warfare and it is imperative to ready the forces for 'other' types of conflicts. NCW compels us to think big with small, precise and effective force.

NCW - Navigating the Road Ahead: AVM DN Ganesh, (Retd) former ACAS (PA&C)

Network-centric operations extending from the ground up to space renders obsolete the traditional dividing line between strategic and tactical operations, enabling hitherto distinct levels of war to be merged into simultaneous, precise and carefully orchestrated operations aimed at nerve centres of leadership and command and control at the very outset of hostilities. Towards achieving network centricity, it is essential to chart out a road map for the future to discard technology that we do not require or are not suitable for our operational environment. For instance, we should not blindly follow other countries in acquiring new technologies. Security challenges faced by India are different from other countries therefore their technologies may not be always tailor-made for our conditions.

Characteristics of a Network-Centric Environment in an Indian environment.

- Perils of Emulating US Example – The US follows a different charter and may not be always applicable to the Indian environment. Therefore, we should create our own list of effects and what technologies are required.
- Staff and Line Functions – There is a need to redefine Staff and Line Functions. Everyone in the hierarchy should be treated with the same professional faith and communication from bottom to top must also be given credence.
- Access to Information – As there is a constant flow of information from multiple sources, there is a need to rethink existing guidelines.
- Time – the Fourth Dimension – In addition to aerospace, surface and sub-surface operations, time has evolved as the critical fourth dimension of warfare. Real-time transfer of data, communication and Battle-field damage assessment (BDA) reports have become vital in deciding the outcome of a conflict.
- The key technologies for a Network-Centric Environment are: Intelligence, Surveillance and Recce (ISR), Image Intelligence (IMINT) and Data Fusion, Self Reliance Through Development of Key Technologies Like CCDs & Processing Speed, Data Transfer – Satellite to Ground, Data Transfer Between Ground Stations, Manned Aircraft, UAVs and Satellites, Homogeneity of Ground – Sea – Aerospace, Architecture and Procedures for Interaction in a Network-Centric Environment and Information Security.
- Training and HRD are other important facets as ultimately it is the man behind the machine who controls the technology.
- In the emerging network-centric environment it is essential to integrate data transfers from varied platforms on one network. There is tremendous amount of data going up and down. Homogeneity ground-sea-aerospace mediums have to be achieved. The Integrated Air Command & Control System (IACCS), AWACS and Data Linking projects of the IAF are examples of integration of all ground radars with airborne platforms like AWACS and interceptor aircraft, through a complex system of data transfer and communications involving fiber-optic lines

and voice/data channels in various frequencies. Dedicated battlefield communication systems would, ideally, need to be tailor-made for a network-centric environment; a system for J&K may be fundamentally different from a system for Andaman & Nicobar area.

- A Joint HQ integrating the audit trail, IW and security and Security plan controlling flow of information and data to all component HQs in flat structure is proposed for conducting future operations.

The Way Ahead

- Integrate and use what we have. Use available tools with imagination and innovation.
- Your goals start from your war plans; divide them into achievable modules while maintaining your capability.
- Address each module separately; but make each module open-ended for subsequent integration.
- Plan small changes incrementally, easier on fiscal planning; ensure the organisation is comfortable with the change.
- In each module, identify key effects, and through them the technologies required to achieve those effects.
- Plan for and integrate obsolescence.
- Though we may be far from jointness, ensure our equipment isn't, as that's what will take time.
- National capability is a must; but not at the cost of wasted time; procure if required, with follow-up engineering.

Cybersecurity – Trust, Visiblity, Resilience: Harvinder S Rajwant, VP, Borderless Network Security, CISCO

With the Indian Armed Forces procuring newer hardware and equipments, more and more communication devices are added every year to the inventory. With this, the

vulnerability of these devices to spoofing and interception for political, military and economic gains have also increased. A large number of IT and IP (Internet Protocol) enabled devices are in use by the Armed Forces. Even devices such as mobile phones, even without internet access are susceptible to data theft and monitoring. For instance, the recent Stuxnet virus was designed for a Siemens software and was not Internet-based.

In the event of the above, cyber security and security of armed forces communications has assumed vital importance in an environment where our adversaries are constantly making efforts at breaching the security walls of the communication and information networks of the country. According to a news report China has a yearly budget of $55 and over 10,000 hackers dedicated to carry out hacking activities.

It is essential to have cyber security mechanisms that build safety within the internal communication networks of the armed forces and detect hacking or attempts at intrusions. The electronic espionage activity can then be isolated without interrupting of affecting the mission critical operations.

Traditionally we designed our networks as entities within silo's – the enterprise with its perimeter – with external facing applications, internal operations, and everything was secured. Today, the increasingly broad range of devices we are using (MACs, PCs, iPhones, smartphones) requires us to reconsider the Device Border. Another shift happening is the application border: Software as a service, video, cloud. You want your applications to work everywhere, regardless of device or location.

We have to adopt the correct approach to cyber security where Identifying and managing the resources that have access to information assets is critical to establishing a state of trust in any organisation; prevent and detect threats by ensuring visibility in the enterprise information spectrum and having resilience or the ability to respond and recover from breaches and disruptions.

As General Keith B. Alexander, Commander, US Cyber Command said: "We need real time situational awareness in our networks to see where something bad is happening and take action there at that time. That is both a coordination issue amongst the

services and agencies, and a situational awareness issue. We do not have a common operational picture for our networks. We need to get there. We need to build that." No single company can solve the complex challenge presented by the Internet but steps have to be taken by all stake holders involved in achieving or enabling network-centricity to achieve a secure communication environment.

Spin off Benefits of Commercial Technologies: Wg Cdr Arif Khan (Retd), Ericsson

With the changing nature of warfare, it is important to keep pace with the emerging technologies in the market. While commercial evolution remains unprecedented, the evolution in terms of the defence of the country remains far behind. At this juncture, one can easily utilise the benefits of Commercial Off The Shelf (COTS) technologies. Following are the drivers for adopting COTS technologies:

- More capacity
- More proven quality
- Less cost
- Shorter delivery times
- Drives the NEW technology

Undoubtedly, one cannot ignore the specific requirements demanded and needed by the defence forces of the country. Following are a few important defence requirements:

- Military Frequency band
- Security requirements
- Transec which includes protection against jamming and interception
- Comsec comprises of encryption throughout the lifetime of equipment
- Rugged equipment, environment requirement
- Autonomous communication and mobility for Tactical communication

As the commercial sector is becoming more and more service oriented, their needs are becoming similar to the needs of the defence forces. In other words, the commercial sector capabilities are approaching military needs. Following are a few aspects:

- Security - Social media, banking and more... All is done over your cell phone
- Scalability - Smaller cells, islands of extra capacity, frequency re-use
- Mobility - Cell phones and laptops rather than fixed phones and desktops
- Availability - Online 24/7
- IP based networks - Services are being designed for IP based networks
- Increased data capacity - 1 Mb/s of IP data to all users in the network
- Flexibility - Future proof, one system fits all, layered architecture

One can also see the transformation towards IP Network. Because of the introduction of multiple services and needed interoperability between services and units, the needs of the defence forces like prioritisation, quality of services (Security, IP introduces new security risks), voice Services (interoperability to legacy systems and quality of services) and autonomous operation are becoming important even for the commercial firms and services.

To illustrate, the third generation (3G) HSPA network can be used by the defence forces purely because it is portable, rapidly deployable and supports autonomous operation. Other 3G-based FWS characteristics are:

- Autonomous operation
- Commercial spectrum 2100 MHz
- 30 min. Initial commissioning at staging area
- Power up in a few minutes – one button operation
- Capable of forming a community network for extended coverage (network of 10 systems)
- 3G Video calls
- High Speed Data (HSPA support)

The trend is towards COTS and All IP as it brings more capacity at lower cost and are approaching military needs and brings enhanced benefits (3G).

Discussion

A number of infra-red and other applications based surveillance solutions are available for deployment in the areas infested with Left-Wing Extremism in the country. UAVs are available to transfer real-time information but in certain areas restrictions can be imposed by terrain and lack of accessibility.

There is a need to increase jointness and build inter-operability between all the three services and process information seamlessly.

Using COTS technology has its own ramifications. For instance, are systems that integrate with integrate with existing equipments available. COTS is not a solution in IT security. Security and the extent of ruggedness of the equipment are other dis-advantages in using off the shelf technology. But in the absence of solutions available domestically, sometimes there are no options but to buy off the shelf.

Encrypting internal networks and hard disk/USB drives can prevent breaches by external agents.

CIDSS should include a feedback loop where there is flow of communication up the chain, ie, from the soldier to the commander.

There are a large number of politically and commercially motivated targeted operations launched clandestinely by players all over the world. Even non-internet based applications or isolated networks are prone to breaching.

Today, technology may be available in the civilian domain prior to being used by the military. These devices may already be embedded therefore comprising their security parameters.

Concluding Remarks by Chairperson

In today's operating environment there is a need to have flatter organisations and evolve joint concepts and joint war fighting doctrines. The doctrines on paper are un-matched on the ground. This gap has to be breached. Induction of new technology is extremely slow and it may impact future operations. There is a need to build test beds for experimenting with joint network platforms. Effect-based operations (EBO) should have an inter-agency construct that would include all the players including the political, diplomatic and intelligence components within the theatre of operations.

VALEDICTORY SESSION

Concluding Remarks: Brig Gurmeet Kanwal (Retd), Director, CLAWS

Former US President George W Bush launched an education policy called "No Child Left Behind." But in the Indian nation, insofar as the communications field is concerned, one "child," ergo, the armed forces, has been left behind. The country has grand plans for the distant future, but nowhere close to realising them in the near future.

Valedictory Address: Lt Gen P Mohapatra, PVSM, AVSM, ADC, SO-in-C

In the realm of net centric operations, the issues which come to mind are increased situational awareness, shortening of the OODA loop, focused logistics, the ability for precision strikes etc. These all stem from net centricity and are all oriented towards the intent of essentially improving mission effectiveness.

Two important components of the transformation of a force to net centricity are:

1- The capability and development required to become net centric:

India has approximately 15000 km of land borders and 7500 km of coastal borders, including island territories. It is faced with two very powerful potential adversaries, with whom it has waged a large number of conflicts and wars. Net centricity in the Indian

domain therefore, would be unlike, net centricity in the West, where it has been employed to an extent, for the forces of the West have been pitched against relatively weaker adversaries. In addition, net centricity at lower levels of integration – at the battalion level - is easier than at the level of a brigade, division or corps. One must also be cognisant of the fact that almost half of India's 1.3 million-strong force is perennially deployed in operations, whether on the International Border (IB), Line of Control (LC), Line of Actual Control (LAC) or in counterinsurgency/counterterrorism (CI/CT) operations. Many of these operations are in extremely remote and inhospitable areas with sub-zero temperatures. Therefore, when one speaks of net centricity in the Indian context, the geo-diversity of deployment, the operational imperatives and the force the Indian armed forces are pitted against, must be kept in mind.

The Chief of Army Staff (COAS) has directed that India to be prepared to fight across the entire spectrum of conflict. This would include the gamut from positional, to attrition, to maneuver, to asymmetric, to virtual – all under a nuclear overhang. And as in the instance of Operation Vijay, it may even sometimes be operations reminiscent of those engaged in the First World War. The geo-diversity previously spoken of, combined with the continuous changes in technology and the requirements of the users (the change in which is a consequence of the change in technology) has driven the armed forces to a large number of disparate systems and networks, ranging from those based on OFC, microwaves, mobile cellular technology, satellites and so on. Therefore, capability development, insofar as net centricity is concerned, would be a major area of focus.

2- The exploitation of net centricity to achieve operational effectiveness:

Net centricity is not a goal in itself. No force can talk of being entirely net-centric. It is necessarily an evolving process. It is not as much about networks but a co-evolution of all aspects of command and control, training, human resources, logistics, and operations. Therefore, it is less about networks and more about networking. In the cognitive domain, there is a reduction in the OODA loop, and diminished time for decision-making. Also, there would also be, notwithstanding checks and balances put in place, an information overflow, resulting in decision-making becoming more complex than earlier. The fog of war, under these conditions, may manifest in a different form,

because of the information overload. The fear of scrutiny of decision-making is also very important. When the entire organisational hierarchy is so transparent and visible, it may also result in tempering the commanders in their decision-making. The hierarchy of decision-making as observed in the past may be affected. There may be a tendency of either higher commanders trying to influence battles/operations, or lower commanders bypassing their responsibilities and passing on the decision-making process to higher commanders. Some other issues to contend with are susceptibility of both communications and non-communications to electronic warfare - cyber operations are also a growing threat. Notwithstanding the necessary checks and balances, as the threat grows, so does the vulnerability. Therefore, it is a continuous process. With regard to the sustenance of the network, in terms of bandwidth demand, there is a limitation of spectrum availability, even in the US. These are linked issues, which will have to be contended with.

The prioritisation of infrastructure to support net-centricity ought to be paramount. Subsequently, a convergence of networks is required for full spectrum interoperability – a network of networks. India will have to adapt its traditional methods of command and control with protection of networks from electronic warfare and cyber attacks. Last, but not the least, honing of HR skills is an equally important aspect. Many of these issues are being currently addressed, but are perhaps not being broadcast as such in the public domain.

The very existence of a network in place would be a great driver towards jointness. In the absence of the internet, one didn't feel its need. Once it was available, one saw the opportunities it opened up. Consequently, once the defence communications network, which is a tri-service network, is in place, it will add to inter-service synergy in a significant way.