VIVEKANANDA INTERNATIONAL FOUNDATION

*Occasional Paper – July 2016*

# Strategic Gaps in India's Net Centricity

Lt General Davinder Kumar, PVSM, VSM Bar, ADC

## About the Author

***Lt General (Retd) Davinder Kumar*** is a scholar, soldier and a thinker. He retired as the ***Signal Officer-in-Chief of the Indian Army*** in September, 2006, after rendering 41 years of distinguished service. He was the ***CEO & Managing Director*** of ***Tata Advanced Systems Ltd,*** the *Tata's* lead vehicle in defence, aerospace, and homeland security from September, 2008till September, 2011. As part of the high level negotiating team of the Tata Group, he successfully negotiated formulation of JVs with Sikorsky, Israel Aircraft Industries, AGT for homeland security and HELA for microwave components. He was instrumental in setting up the first helicopter cabin manufacturing facility in India from ground breaking to start of manufacturing in 159 days flat. He has been on the ***Board of Directors*** of both Public and Private sector companies and *Member of select Advisory body of Tata Group on Telecommunications and the Steering Committee on Defence of the Tata Group*

An Expert in the Net Work Centric, Information and Cyber Warfare, he was instrumental for the approval and setting up of the *Army Cyber Group* and the First *Information Warfare Brigade* of the Indian Army. He was the Project Director of Army Strategic Communication Network (ASCON) and is the author of the Defence Communication Network (1995), Tactical Communication System (1996), and ASTROIDS besides a number of regional optical fibre and satellite based networks in some of the most inhospitable terrains in the North and East India*. He headed the national study on Cryptography, was a member of the National Committee on spectrum management and Adviser on IT to the state of Madhya Pradesh*.

He has worked with *Indian Space Research Organisation* (*ISRO), Oil India*, and the *Planning Commission*. He has been an Examiner for the University Grants Commission, on the Court of The Indraprastha University, member of the *Hardware and Human Resource Groups of the IT Task Force* and the Advisory Committee of *National Disaster Management Authority* appointed by the Prime Minister. He was member of the committee which formulated the I T Act;

 

2000.He is a recipient of five National Awards including the highest for *Distinguished Service of the Most Exceptional Order.*

*He also got the Best Engineer Award in 2005 and is the only serving officer to have been awarded the Fellowship of Indian National Academy of Engineering.* He has over 400 papers to his credit and has also been invited to speak at various international fora like *RAND Corporation*, International Telecommunication Union (*ITU), World Battle Space Research Organisation*, *Brookings Institute, ASPEN Institute,* Wharton *University* and Centre for Strategic and International Studies, Beijing.

 

# Strategic Gaps in India's Net Centricity

In the digital battlefield of 21st century, Technology and Information are the new currencies of power. Exploitation of both of these to create efficiencies, economy of effort and facilitate full spectrum operations; nuclear to asymmetric and strategic to tactical, is the essence of Net Centricity.

Synergy through sharing of information in all its stages, namely collection, storage, processing and dissemination, is at the heart of net-centric capability. It also encompasses Information denial, perception management through exploitation of electronic and print media, social networking and warrants involvement of all organs of the nation from the very beginning.

Net centricity is technology intensive with Information and Communication Technology (ICT), communication networks and media as the nucleus. The primary aim of net centricity is to bring about informed decision making, synergy, maximum effects and higher speed in execution while ensuring extensive battlefield transparency. Paradoxically, net centricity demands synergy to create synergy.

While the principles of war and the need for net centricity have not changed, the parameters have changed drastically. The battlespace has enlarged disproportionately making the physical borders irrelevant and changing the concept of national sovereignty. When combined with the accuracy, range and lethality of present day weapons and munitions, it has given rise to a new concept of Effect Based Operations. Ubiquitous application of ICT has resulted in a Digital Battlefield with tremendous increase in the speed of operations, diffusion of power, associated vulnerabilities and Information Warfare emerging as a new dimension of warfare.

The Indian Government, Security Forces, Intelligence Agencies, Industry and all security related organisations need to prepare to operate and fight in this evolving battlefield environment where the "bits" may cause more damage than the "bullets" and in all probability would precede the bullets.

Central to this preparation would be our national security doctrine supported by enhancement of our Net Centricity through advanced technological,

 

organizational, training and related capabilities in all dimensions of land, air, sea, outer space and cyberspace across full spectrum of warfare.

This is an inescapable requirement for binding the nation's comprehensive combat power into a viable and coherent force. It would be economical, enhance our kinetic effectiveness, command and control and provide various options, through situational awareness, for both protecting our own assets and addressing the weaknesses of our adversaries in offensive operations.

Unfortunately, our efforts towards net centricity, particularly during the last decade or so, have been tardy at best. Consequently, while we have islands of excellence in each Service and in the Government, they lack effectiveness and synergy. Our Commanders and policymakers largely continue to be technology shy and prefer to operate in their comfort zone of industrial era warfare of tanks and guns. They still seem to be fighting the last war as is quite evident from the literature available in the open. There is an urgent need for the Government to intervene at the highest level to ensure development of Comprehensive National Power relevant to the emerging contours of warfare across the full spectrum. This is a strategic requirement in the light of threats faced by India as also her projected role in the Asian region.

## What India Must Do

## National Security Doctrine & Vision

To start with, we need to promulgate the National Security Doctrine and the related comprehensive vision document, policy and the road map for capacity building in the contemporary and futuristic battlefield scenarios. These should be formulated together by all the stakeholders, duly approved by the Parliament, backed by necessary finance and an empowered implementing organization accountable to the Government. Based on this document, we should work out the technologies, organization, training and human resource requirements. We should take the existing assets in account, transform and integrate those with the new system.

 

## Technology

Availability of requisite technology by way of hardware, software, and semi-conductor chips fabrication facilities, electronic manufacturing eco system, R&D infrastructure, system integration capabilities, and an enabling policy framework for involvement of the private sector and academia and skilled human resource are some of the challenges India faces to harness technology and implement relevant net centric solutions. While, in some cases, policies have been promulgated but their implementation is completely lacking. We hope that these would receive due attention from the present Government. We need an urgent and innovative drive to build these capabilities and achieve "Technological Sovereignty" preferably by 2020 but by 2025, the latest. Time is certainly at a premium.

## Organisation

An extremely significant aspect of 21st century warfare is the fact that when threatened, it is not only the Armed Forces but the entire nation, the government and all its organs, the media and the people; which will have to respond in an integrated and unified manner. Herein, therefore, lies the absolute importance of organization transformation for net centricity.

The single point politico-military dialogue, which is required to establish a coherent national strategy and quick decision making is lacking in the present security setup**.** We needed the Chief of Defence Staff yesterday! The inescapable doctrinal implication of this post is the integration of conventional (including cyber, outer space and Special Forces) and nuclear doctrines. This is also required to negate the glaring anomaly in our security decision making structure by way of the absence of a military high command in decisions of war and peace. Present security environment necessitates Joint threat assessment, planning and execution within the Armed Forces and with the Ministries. There is an urgent and definite requirement of greater integration of the three Service Headquarters with the Ministry of Defence. Further, an institutionalized policy framework is required for Service headquarters and Integrated Defence Staff to interact with other Ministries and Government institutions. A cohesive, practical and responsive civil-

 

military framework is absolutely essential for comprehensive capacity building for 21st century warfare, economy of effort and as a foundation for advanced net centricity in our national security set up.

In the current security scenario, nuclear, space, cyber security and Special Forces capabilities are at the heart of a nation's comprehensive combat power. Decisions regarding formulation of Cyber, Outer Space and Special Forces organisations need to be expedited as indeed the formulation of Integrated/Joint Theatre Commands. At least two of these, one for the plains sector and the other for the mountains must be cleared immediately. It may be noted that operationalisation of these commands is likely to take anything between five to seven years. The recent statement of the Raksha Mantri in this regard is quite encouraging,

Concurrent exercise to streamline the existing organisations and provide resources for raising of new units/formations is badly overdue. The announcement of Lt Gen DB Shekatkar Committee is welcome. Similar studies, by eminent people, have been carried out before but their recommendations were either not carried forward due to vested interests or implemented partially creating confusion and uncertainty. The political leadership has to demonstrate the will and the ability to take hard decisions with risk management strategies in place, for an effective and quick organization transformation. India needs highly synergized, integrated, mobile, lean and mean, joint organisations, relevant to 21st century warfare, supported by efficient logistics and infrastructure. Organisation transformation is likely to take 3 to 5 years to become effective and operational from the day it is started.

## Communication Networks

Communication Networks are at the heart of Net-centricity. These form the Nervous System for management of a nation's comprehensive power and would be the primary targets of the adversary, most likely in the very start of hostilities. Hence their survival and availability are of utmost importance. There is an urgent need to upgrade and integrate existing networks of the three Services with the national networks, and place them under a single

 

authority. Indian standards for communication and data networks must be propagated without any further delay.

In view of the threat of cyber warfare, India must develop indigenous capabilities in the design and manufacture of network products based on indigenous chips and carry out own system integration. This is a strategic deficiency which very seriously impacts on the survivability and availability of our Defence and National networks and hence the net centricity of India. In the interim, other requisite measures must be taken to protect our networks. This will require innovation as also the ability of our forces to operate without/restricted communications for limited periods.

For true and secure net centricity, operationalization of National Policy on Electronics, 2012 and establishment of viable Defence Industrial Base are strategic imperatives and pre-requisites.

## Command, Control, Computers, Communications, Intelligence, Surveillance and Target Acquisition (C4ISTAR)

C4ISTAR, in essence, is about co-evolution of Technology, Organization (i.e Architecture and Processes) and People and about **control and disruption** of Information and quick decision making. It is the vehicle to promote expeditious "synergy of effects" through effective integration of Sensors, Decision makers and Shooters.

Indian Armed Forces, individually, have done well and have developed rudimentary capabilities particularly at the operational and tactical levels. We need Joint C4ISTAR capabilities duly supported by technology, highly skilled human resource, innovation and training. Joint C4ISTAR enables ability to mass effects without massing forces; protects against asymmetric threats; and provides joint force flexibility, analysis, interpretation, and efficiency. It calls for Interoperability of systems and subsystems, standards and protocols for interconnection, integration and information management; policies, procedures and formats for Information assurance, data storage, data retrieval and data security and so on.

 

In a digital battlefield, while C4ISTAR is an inescapable requirement, we must have systems, drills and capabilities to interfere and negate the adversary's C4ISTAR assets through electronics, optical, cyber and physical means. Concurrently, we must protect our assets and ensure that they operate successfully in the hostile environment.

## Electronic Combat (EC)

Preparation for Electronic Combat in association with or independent of Kinetic war is at the heart of executing operations in the present day digital battlefield. Electronic Combat (EC) is an ideal tool for carrying out Asymmetric operations. Unfortunately, this aspect has not got the attention it deserves. India needs to develop her potential for EC and that would demand creation of indigenous capabilities in each of the components of EC. Electronic Combat would require capacity building in ElectroMagnetic (EM) Space Management, creation and negating the Electronic Environment Effects (E3), Electronic Warfare (EW) to include generation of and protection from ElectroMagnetic Pulse (EMP) and Electronic Deception.

## Electro Magnetic Space

The ElectroMagnetic (EM) Space is extremely complex, crowded, contested and needs to be managed and regulated dynamically in real time. The situation is much more challenging in a digitized battlespace environment where practically every system starting from a diesel generator to a missile system requires spectrum to operate or else contributes, "Noise" which restricts the availability of the EM space. Add to this the high power of various radars, communication systems and electronic warfare systems and the fact that the same resource is being used by the adversary and the civilian networks. Security and Availability of ElectroMagnetic (EM) Space would be critical factors in the execution of war in the Digital battlefield. Denial of EM Space as also ensuring its availability to own forces is the essence of "Spectrum Warfare" which in near future would include cyber warfare along with EW.

The development of high energy beam weapons, LASER weapons and designators, and other aviation resources, missiles and Ballistic Missile

 

Defence (BMD) systems; satellite constellations have further added to the challenge of management and regulation of EM space. We would need a system and an organization that would ensure the availability of the navigation and position locating systems, bandwidth, communication ranges and connectivity in an intense and hostile EM space environment, including ElectroMagnetic Pulse (EMP), in real time. This would require electronic intelligence, modeling and simulation of the battlespace EM environment and highly skilled man power drawn from the nation and abroad. It would be a national effort with dedicated organization within the Defence and Security forces.

## Electromagnetic Environment Effects or E3

The increasing EM density of users and high power in weapon radar systems and communications have impact on electronic control and devices that may malfunction, cause desensitization and random undesired effects called the Electromagnetic Environment Effects or E3.

## Electronic Warfare (EW)

Electronic Warfare (EW) is one of the sword arms of Information Warfare. This includes optical warfare and E-bombs for generation of non-nuclear EMP. As a corollary, we need to develop operation rooms, communication centres and command posts suitably protected from effects of EMP in particular and EW in general. India needs multi-platform and multi-frequency, light weight, high power and adaptable EW systems suitably integrated across the three Services for maximum effects. This requires a common EW policy, joint training, appropriate equipment and a central management organisation preferably under the Integrated Defence Staff. Indigenous development of EW systems is a strategic requirement. While India has done well in this field, she needs to develop systems for platforms like satellites, UAVs, drones and pods. There is an urgent need for coordination of R&D and all procurements to ensure economy and quick capacity building.

## Electronic Deception

The term **electronic deception** means the deliberate radiation, reradiation, alteration, suppression, absorption, denial, enhancement, or reflection of

 

electromagnetic energy in a manner intended to convey misleading information and to deny valid information to an enemy or to enemy electronics-dependent weapons. In the current scenario, this would include Cyber Deception.

Among the types of electronic deception are:

- Manipulative electronic deception – Actions to eliminate revealing or convey misleading, telltale indicators that may be used by hostile forces
- Simulative electronic deception – Actions to represent friendly notional or actual capabilities to mislead hostile forces
- Imitative electronic deception – The introduction of electromagnetic energy into enemy systems that imitates enemy emissions.
- Electronic attack deception

There are many more types but the aim here is to highlight this strategic gap and to stress the absolute necessity of capacity building in this critical area through a dedicated organisation, technology, platforms, training and highly skilled human resource.

For true and secure net centricity, operationalization of National Policy on Electronics, 2012 and establishment of viable Defence Industrial Base are strategic imperatives and pre-requisites.

## Survivability

With the battlefield transparency as high as 90 per cent, the warfare will have to be conducted in an entirely different manner. Survivability of own assets would be critical requirement and must be factored separately in our war fighting Doctrine. While camouflage and concealment will always be important; greater emphasis will be on Deception, Dispersal, Mobility and Organization Transformation. Decision making will have to be very quick in an environment of greater ambiguity, uncertainty and information overload.

Deception would include Electronic, Optical, Physical and Cyber deception. Perception management plans by skilled exploitation of intelligence, communication assets, social, electronic and print media must be integrated and executed as part of the overall deception to ensure greater survivability.

 

Deception plan for each phase must be integrated with the operational plan, rehearsed and have viable alternatives to cater for contingencies. There is a definite requirement of dedicated organization for carrying out deception. Innovative ideas like "crowd sourcing" must be tried out to generate resources and increased involvement at the national level. Human resource will have to be highly skilled, and trained to ensure flawless execution. The impression one gets is that probably the criticality of this area in the conduct of 21st century warfare is not understood and if otherwise, it is not receiving the importance that it deserves.

We must design and produce requisite dummies, platforms and associated equipment and content for deception indigenously. One, however, does not see much action in this critical area.

## Information Warfare (IW)

IW is both an asset and a challenge to net centricity as it deals with the protection, interference and destruction of the "information" and the "information assets/systems" including the human resource.

Information Assurance concerns protecting own information in all its stages of capture, storage, processing and dissemination. The challenge is the design, production and fielding of cryptographic systems and their integration within the Services and other organs of decision making in the country. The networks and other communication assets will have to be secured through different levels of secrecy and protected from cyber-attacks and cyber espionage. Concurrently, counter intelligence and crypto-analysis capabilities will have to be enhanced substantially.

Information Dominance demands availability of potent Electronic and Optical Warfare and Intelligence Systems in all dimensions of a digital battlefield. Development of capabilities to launch cyber-attacks including use of cyber weapons for creating physical disruptions will have to be a part of our national security doctrine and the implementation of net centricity.

Perception management will start well before the commencement of the conflict and last much after its termination. Development of capability to launch "Social Engineering" Attacks in concert with deception and KE operations must be part of our capacity build up for net centricity.

 

## Information Management

Net centricity is all about information sharing to create synergies. Yet, very surprisingly, one has not come across any "Information Management Strategy" enunciated by any headquarters. The commanders and staff want right information at the right place and at the right time. We also say that they should not be subjected to "Information Overload". So who is responsible for these? One would like to believe that creation of an "Integrated Information Management Eco System" within the Defence forces should be the responsibility of the Headquarters Integrated Defence Staff. Within the Army, this would be an appropriate responsibility of the Directorate General of Information Systems.

Information management' is an umbrella term that encompasses all the systems and processes within an organisation for the creation and use of information. Effective information management is not easy. There are many systems to integrate, a huge range of operational needs to meet, and complex organisational and cultural issues to address.

Information Management is a subject by itself. It is complex but NOT technical. The aim in this article is to flag the issue and hope that this critical area gets due attention. It is a glaring strategic gap, a massive task and we need to start right away.

## Digital Imagery

Inherent to a digital battlefield is an efficient Geographical Information System (GIS), high resolution digital imagery from multiple sources and the ability to manipulate, model and combine the images. This mandates the availability of digital maps, overlays, sophisticated hardware and software and very well trained human resource in the forms of image analysts and interpreters. With rapid advancement in the sensor's capabilities and the availability of different sensors, the capability of fusing images from visible light to radar images to images transmitted by multi-spectral satellites is an operational imperative. Acquisition of this capability is a challenge as indeed is the development and manufacturing of sensors indigenously**.** This would form an important component of Information Management along with Digital Asset Management**.**

 

## Data Management

The sensors at the tactical, operational and strategic levels as indeed other intelligence sources create a very large amount of data running into tens of terabytes. This data has to be stored, processed, analyzed and transmitted in a fully secure manner to all concerned ensuring its integrity and timeliness. The real challenge is synthesizing and analyzing the data collected, convert the same to usable information; and to quickly disseminate the results, in the desired format, to all those who need it in an extremely hostile electronic and physical environment. It requires modern data storage and retrieval systems, highly qualified human resource and very robust and resilient data networks supporting bandwidth on demand. Related challenges are the standardization of formats amongst the Services, digitization of the existing information and its integration and indigenous development/absorption of technologies like the Big Data and Analytics.

## Indigenous Position Locating System

Indian Regional Navigation System (IRNS) is likely to be available by mid-2016. This would meet the strategic requirements of the pointing, navigation and target detection of indirect fire weapon systems, radars, intelligence systems, communications, combat aviation, special operations, maneuver, own and enemy force tracking and forward observers. The IRNS will have to be integrated with our digital maps, weapons and systems and be able to function in an extremely hostile physical and electronic environment. Also, we would need ruggedized GPS hand-held terminals.

## Internet Protocol (IP) Addresses

In a digital battlefield, all resources at land, sea, air and space are integrated through complex communication and data networks. These networks are likely to be working on IP. This would necessitate that every soldier, weapon and support system has an IP address. This is a huge challenge both from the allocation and communication security points of view and a great vulnerability to be managed. We need to have a dedicated organization at the National level for this as also to decide on the standards to be incorporated. Purely from security and survivability points of view, it may be desirable to have an alternate to IP addresses or perhaps have a dedicated internet.

 

## Training

This is an area in which we are lagging seriously and have not made the requisite investment. Our training set up requires major re-orientation. It is surprising that in spite of full-fledged Training Commands, we do not have training institutions and infrastructure for Information Warfare, Outer space operations, Electronic Combat, Asymmetric Warfare and Special Forces operations and so on. There is a great deficiency of language experts. There is an urgent need to have joint training establishments in these area and hasten the establishment of the Indian Defence University.

Net centricity capability demands highly qualified and skilled human resource. Their induction, training, periodic up gradation and retention would be major challenges as is the creation and availability of the related training infrastructure. More important is the training and orientation of the Commanders and Leaders to absorb and exploit this capability and integrate the same in our war fighting concepts.

## Conclusion

India has serious strategic gaps in her orientation and capacity building for the 21st century warfare. This is of grave concern particularly with reference to her Eastern neighbour which has undergone almost four decades of modernization and major organization transformation backed by a strong Defence Industrial Base and a state of the art training infrastructure. There is an immediate need to adopt a "Systems" approach and "leapfrog" the capability building through exploitation of dual technologies, national information infrastructure and involvement of private sector, Indian diaspora and Academia. This requires organizational, cultural and attitudinal transformation to bring in synergy, mutual trust and transparency. While one can see a few green shoots in the policies and decisions of the present Government, it will have to display greater political will and urgency in capacity building through incorporation of advanced net centricity in our Armed Forces.

 

## About the VIVEKANANDA INTERNATIONAL FOUNDATION

The Vivekananda International Foundation is an independent non-partisan institution that conducts research and analysis on domestic and international issues, and offers a platform for dialogue and conflict resolution. Some of India's leading practitioners from the fields of security, military, diplomacy, government, academia and media fields have come together to generate ideas and stimulate action on national security issues.

The defining feature of VIF lies in its provision of core institutional support which enables the organization to be flexible in its approach and proactive in changing circumstances, with a long-term focus on India's strategic, developmental and civilisational interests. The VIF aims to channelize fresh insights and decades of experience harnessed from its faculty into fostering actionable ideas for the nation's stakeholders.

Since its establishment, VIF has successfully embarked on quality research and scholarship in an effort to highlight issues in governance and strengthen national security. This is being actualized through numerous activities like seminars, round tables, interactive-dialogues, Vimarsh (public discourse), conferences and briefings. The publications of the VIF form the lasting deliverables of the organisation's aspiration to impact on the prevailing discourse on issues concerning India's national interest.

**VIVEKANANDA INTERNATIONAL FOUNDATION**
3, San Martin Marg, Chanakyapuri, New Delhi – 110021
Phone: +91-11-24121764, 24106698
Email: info@vifindia.org, Website: http://www.vifindia.org
Follow us on twitter@vifindia