Challenges of a Digitised Battlefield

Lieutenant General Davinder Kumar;
PVSM, VSM and Bar (Retd)*

Introduction

Digitised Battlefield is centric to the concept of Network Centric Warfare (NCW), the warfare of the twenty first century. It demands full integration and synthesis of different organs of governance like the armed forces, para military forces, intelligence agencies, transport, health, media, disaster management, energy and so on. Digitisation, massive deployment of Information and Communication Technology (ICT), organisation transformation, large scale system integration and human skill development centred around the national doctrine are the essential pre-requisites to develop capabilities for NCW in a digitised battlefield environment. These capabilities include Command, Control, Coordination, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) systems, digital weapon platforms and digital forces.

Digitised Battlefield

Digitised battlefield depends on *the degree of Integration of the technical components* such as:-

(a) Computer processing, data storage and retrieval.

(b) Advance software and hardware.

(c) Display Systems.

(d) Man-Machine dialogue and Interface.

(e) Sensors.

(f) Communication networks.

(g) Combat Identification, Positioning and Navigating Systems.

Digitising the battlefield is a complex, lengthy and expensive process. It requires a very high degree of commitment, focus and

***Lieutenant General Davinder Kumar; PVSM, VSM and Bar (Retd)** was commissioned in the Corps of Signals in Dec 1965 and retired as Signal Officer-in-Chief in September 2006. Post retirement he has worked in the Corporate sector, contributed extensively in professional journals and has been a member of National IT Task Force and number of Committees.

Journal of the United Service Institution of India, Vol. CXLI, No. 590, October-December 2012.

vision of the emerging and future security paradigm and technologies. It presents unique and enormous challenges, each requiring synthesised effort of a number of agencies. While this paper, lists some of the challenges in the Indian context, it is for the reader to determine where we stand with regard to this Information Age Warfare capability in a digitised battlefield.

Vision, Policy and Road Map

The first challenge is to have a comprehensive vision document, policy and the Road Map formulated together by all the stake holders, duly approved by the Government and backed by necessary finance and an empowered implementing organisation accountable to the Government. Based on this document, we should work out the technologies, organisation, training and human resource requirements. We should take the existing assets in account and integrate those with the new system.

Electro-Magnetic Space Management

The Electro-Magnetic (EM) Space is a Global common. In the present environment, it is extremely complex, crowded and needs to be managed and regulated dynamically in real time. The situation is much more challenging in a digitised battle space environment where practically every system, starting from a diesel generator to a missile system, requires spectrum to operate or else it contributes to "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 are being used by the adversary and the civilian networks. The increasing EM density of users and high power in weapon radar systems and communications have an impact on electronic control and devices that may malfunction, get de-sensitised or have undesired effects called the Electromagnetic Environment Effects or E3. The development of high energy beam weapons, LASER weapons and designators, UAVs and other aviation resources, missiles and Ballistic Missile Defence (BMD) systems and satellite constellations have further added to the challenge of management and regulation of EM space.

We would need a system and organisation 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 in real time. This would require modelling and simulation of the battlespace EM environment and highly skilled man power. It would be a national effort with dedicated organisation within the Defence and Security forces. China has a training base in inner Mongolia for training in EM battlespace management. The system can simulate natural, civilian and EM environment similar to the battlefield.

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. We need to have a dedicated organisation at the National level for this as also to decide on the standards to be incorporated.

C4ISR Systems Management

A viable and efficient C4ISR systems management is at the heart of a digital battlefield. This presents the challenge of:-

(a) Secure information management, storage, processing and dissemination.

(b) Fielding of different sensors for providing battlefield transparency.

(c) Sensor to shooter integration through powerful, responsive, secure, survivable, self forming and self healing resilient networks.

(d) Real time bandwidth management.

(e) Very high speed data processing, data storage, management, analysis and transmission.

(f) Survivability, protection and redundancy of systems.

A key element in the digital battlefield is the value of Situational Awareness information. This information needs to be shared among

various combat teams and assets on ground, at sea, in air or in barracks. To achieve this information sharing, systems must communicate over variety of mediums and with absolute security to protect sensitive data.

As security forces become more dependant on IT, they will develop new kinds of vulnerabilities and present new challenges in protecting the information. With the need to connect and share communications, the requirement of cross domain products that can enable classified data to flow appropriately across boundaries between networks with different security levels becomes more acute.

With the battlefield transparency as high as 90 per cent, we need to conduct the warfare in an entirely different manner. While camouflage and concealment will always be important; greater emphasis will have to be laid on deception, dispersal, mobility and organisational transformation. Each of this is a challenge by itself. Decision making will have to be very quick in an environment of greater ambiguity, uncertainty and information overload.

In a digital battlefield, while C4ISR is a necessary requirement, we have to have systems, drills and capabilities to interfere and negate the adversary's C4ISR assets through electronics, cyber and physical means. At the same time, we have to protect our assets and take necessary measures to successfully operate in that environment. In China, "Detection Evasion" is central to military training for Detection in today's environment means Destruction. Camouflage, Denial and Deception are integrated and monitored in all field exercises as part of, "Counter Reconnaissance Evasion Technique"

Information Warfare (IW)

IW has added a new dimension of warfare where information dominance will decide the winner of any conflict in this information age. Information Assurance presents the challenge of 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. Concurrently, crypto analysis capability 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 is the real challenge.

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, Deception, Denial and Perception management through very skilled use of media, intelligence and communication assets is the real challenge.

Interconnection and Interoperability

Interconnection is defined as communication between different networks. This kind of communication deals with the lower protocol layers; e.g. on Open System Interconnection (OSI) reference model is related to the physical layer, data link layer and the network layer. *Interoperability is a state which interconnected systems can reach. It is the communication from one active process to another active process.* Interoperability refers to the ability of two systems to exchange data :–

(a) With no loss of precision or other attributes.

(b) In an unambiguous manner.

(c) In a format understood by and native to both systems.

(d) In such a way that interpretation of data is precisely the same.

Implementation of interconnection and interoperability is mainly about standards such as:-

(a) Information processing standards

(b) Data transport standards

(c) Information standards

(d) Human Computer Interface (HCI) standards

Hence, to achieve Interconnection and Interoperability of different information systems, a strategy of common hardware, software, standards and specifications architecture is required as the base. Each of this activity provides a major challenge.

Integration of legacy systems provides yet another challenge where development of suitable Interface would be the way to go. There are two significant differences between interfacing and interoperability : –

(a) With interoperability, the exchange of data is performed without the need to translate to an intermediate level

(b) Interoperable systems will provide exactly same, "answer" in the presence of identical data

Digital Imagery

A digital battlefield is characterised by high resolution digital imagery from various sources and the capacity to manipulate, model and combine the images. Inherent to this capability is the availability of digital maps, overlays, sophisticated hardware and software and very well trained human resource in the form of image analysts and interpreters. Rapid advancement in the sensor's capabilities and the availability of different sensors, the capacity 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 design, development and manufacturing of sensors indigenously.

Data Management

The sensors at the tactical, operational and strategic levels and other intelligence sources create a very large amount of data running into tens of terabytes. This data has to be stored, processed, analysed and transmitted in a fully secure manner to all concerned ensuring its integrity and timeliness. *The real challenge is synthesising and analysing the data collected and convert the same to usable information;* and to quickly disseminating the results in the desired format to all those who need it. This has to be done 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. Related and perhaps bigger challenges are the standardisation of

formats amongst the Services, digitisation of the existing information and its integration.

Indigenous Position Locating System

A digital battlefield, in our context, will require a home-grown and owned Position Location System which could be used to meet the pointing, navigation and target detection requirements of indirect fire weapon systems, radars, intelligence systems, communications, combat aviation, special operations, manoeuvre, own and enemy force tracking and forward observers. The challenge is in the fielding, operation and sustenance of such a system in an extremely hostiie physical and electronic environment.

Organisation Transformation

Acquisition of NCW capability requires three things at the macro level. These are:-

(a) Political Will

(b) Technology and

(c) Organisation Transformation.

The warfare of 21st century is characterised by Asymmetric Warfare in an environment of Informationisation. This demands a very high degree of synthesis and integration of the Security Forces, Government agencies, Industry and R&D establishments. The Armed Forces will have to:-

(a) Reorganise, equip, evolve and train to fight in an integrated manner in the digital battlefield with more than 90 per cent battlefield transparency;

(b) Acquire and face long range, highly lethal and precision weapons;

(c) Have greater mobility;

(d) Operate in an environment of uncertainty and ambiguity caused by information overload.

The bigger challenge perhaps is fighting an invisible enemy in the *Infosphere* and a terrorist both of which can create havoc in the area of their choosing. Hence, in the emerging security scenario, while technology will play a very major role; survivability

and exploitation of technology will demand a major organisation restructuring and a new approach to training to have human resource with necessary skill sets- a very big challenge in the prevailing atmosphere of one-upmanship and narrow view point. Some hard decisions are required urgently.

Accurate Weather Forecasting

Weather has always played a very important part in the warfare. Adverse weather conditions have been exploited to achieve surprise. In the present context, this has become very important for long range precision weapons, aviation, operations at sea, availability of surveillance and so on. Weather inputs will have to be integrated and factored in the overall operation plans. There is a need for Military weather forecasting capability through dedicated satellites and corresponding ground infrastructure.

Technology

Availability of requisite technology by way of hardware, software and their integration present the biggest challenge. The situation is further compounded by:-

(a) The lack of Military Industry infrastructure base in the country.

(b) Lack of integration between the Services, DRDO, academia and the MoD.

(c) Reluctance to invest in the R&D by the private sector.

(d) Complicated procedures and the reluctance of the private sector to invest in defence industry due to the perception that they do not have a level playing field vis-à-vis the Defence Public Sector Undertakings (DPSUs).

In this Info Age, the country has strategic deficiencies – we do not have a chip manufacturing facility, own secure Operating System, indigenous search engine and practically no expertise in Large Scale Integration of systems. The challenge lies in quick build up of requisite capabilities through a concurrent policy of technology development and technology insertion in a Public Private Partnership (PPP) mode backed by simple procedures built on trust and accountability. We need an urgent and innovative drive to pull in our talent and deploy them in achieving "Technological Sovereignty".

Human Resource Development

Digitised battlefield would need dedicated, highly qualified and focussed human resource to man, operate, and maintain various systems. It calls for specialists in various domains backed by a very dynamic and responsive organisation; procedures and processes. This is a time consuming process that would involve selection, intensive classroom training, operation in simulated environment and field exercises in different disciplines. It would take anything between three to five years to have the desired level of expertise assuming that the training policy, organisation and infrastructure are in place. Our capability to operate in a digitised battlefield is contingent on having appropriate and well trained human resource.

Conclusion

ICT through its all encompassing nature has changed the security paradigm wherein a Digital Battlefield has become centric to a nation's NCW capability. It has also changed the manner of conducting warfare with Information Warfare becoming the new dimension of warfare. Consequently, information superiority has become the war winning factor. *This environment demands creation of modern, capability based armed forces with high degree of jointmanship and synergy with nation's resources.* It also demands rapid and focussed technology development and insertion.

India and its Armed Forces are in a state of transition with islands of excellence in certain areas and perceptible deficiencies in some areas at the strategic, operational and tactical levels. This paper lists some of the major challenges that we face in having a true digital battlefield capability. Each of the challenge mentioned here is a subject by itself and would require detailed treatment by the Services, experts and the policy makers to provide our nation the capabilities in tune with our doctrine. We can judge where we stand today and what we need to do to quickly to bridge the gaps. It is a gigantic task which will require a very committed, innovative and forward looking leadership at all levels. The main challenges are – our cumbersome procedures, lack of unified thinking, R&D and strong defence manufacturing base and poor implementation.