CENTRE FOR LAND WARFARE STUDIES

SEMINAR ON

DIGITISATION OF BATTLE FIELD 2013

31 OCTOBER 2013

General

The Centre For Land Warfare Studies (CLAWS) organised a seminar on Digitisation of Battlefield in collaboration with SP Guide Publications on 31st October 2013 at Hotel Le Meridien. The seminar focussed on critically analysing components of technology which are imperative for national security capability development. The seminar was well attended by serving officers, veterans of the Indian armed forces, members of the strategic community and representatives from defence industries.

Welcome Address: Maj Gen Dhruv C Katoch, SM, VSM (Retd) Director, CLAWS

The explosion of information technology has affected greatly the way warfare is conducted in present times and the manner in which it will take place in future. Battlefield digitisation provides commanders with a C4I2 enabled environment and empowers them with an integrated battlefield picture to enable domination of the battlefield. The seminar aims to bring into focus the impact of digitisation on the military and ways to control and dominate the battle space. It also aims to determine technological imperatives to build national capabilities.

Key Note Address: Lt Gen Anil Bhalla, VSM, Director General Perspective Planning & President Executive Council, CLAWS

Technology has increasingly been driving warfare. Future operations will be multi-faceted as the army is now looking into conflict prevention, deterrence, post conflict reconstruction measures. Operations will be multi-dimensional, inter related, increasingly joint and combined. Conventional army is needed on the western border with Pakistan because of the rising border skirmishes as well as the post 2014 withdrawal of US troops. Still technological asymmetric warfare will play a significant part in any outcome with the adversary. Traditionally Indian army has looked at battlefield however the term battle space is however more inclusive space, time, activity co-relation which are impacted by technology. This transformation in warfare has brought in a change in the cognitive domain of the battlefield.

Indian battle space is complex. Merging the highly modernised and digitised technology along with the obsolete technology that exists remains a lurking question. To achieve this, a framework is required, which involves us to rethink and restructure things. To enable a ground soldier to be effective in operations requires continuous up gradation of technology for which the existing mind-set needs to be targeted.

Space and cyber operations are the new paradigms that have the potential to inflict maximum damage on the adversary. Harnessing information that covers the entire spectrum of warfare at the tactical and strategic level without compromising on security remains a challenge. R&D, Defence industry and Perspective Planning need to cooperate in a big way to bridge the gap that lies in cyber security.

Digitisation of battlefield also needs to take into account the issue of human resources. There is a need to sort out problems pertaining to timeline and recruitment. Coordination between civil and military experts is essential for the Indian Army. The expertise needs to be networked to enable the army to operate in various types of terrain. Measures to integrate the air force and navy are also underway.

Session I: TECHNOLOGY – IMPERATIVE FOR NATIONAL CAPABILITY

Sensors :Utilisation and Trends – Maj Gen PK Srivastava, ADG Artillery(A), Artillery Directorate

Every soldier is a sensor since he is capable of perceiving and thinking and transferring that piece of information provided he has access to means of communication. There are varieties of sensors available. To name a few:-

- Recce Warriors
- Ghataks
- UAVs
- Aerostats
- WLR

However, the utilisation of sensors takes place at the battalion level, brigade level and the theatre level. The sensors at each of these levels are different. All the data has to be collated, collected and sent to the relevant command force. Presently, elementary software is available to do the needful. At the battalion level, the information is still sent manually while digitisation only starts at the brigade level.

Someone has to feed that information to the concerned centre. At each level there is addition of certain requirements which is compiled by the higher level and sent to the command and control. Each level also has certain sensors which are directly under its command and pass the concerned results/ information to the lower unit. The requirement of information increases as one moves up the ladder. Therefore, there is an immediate need of a totally automated software/system that runs round the clock. This has to happen simultaneously since managing UAVs in itself is quite a task. Presently it's being done manually with little support from the computers.

The two joint ISRC should be linked right up to the army headquarters. Currently an ISR summary is issued which is based on information received from all the sensors, this also gives out the latest information to all commanders. A common operations

picture is helpful where every activity is being recorded and has the potential to raise awareness of commanders.

After analysing the ISR summary, the commander should know what decision needs to be taken and that decision should be conveyed to all levels using the same network. To achieve this, we need proper visualisation software so that the commander at the theatre level is able to see everything happening on ground. Here, important activities are flashed through sound signals, so that the attention of the commander is automatically diverted in that direction.

Currently, we are grossly lack digitisation and utilisation of sensors since we still depend on intelligence derived from surveillance and reconnaissance. We need persistent surveillance in which degradation and target acquisition gets integrated during war. In hybrid warfare there is a need to target non-conventional warfare techniques as well. These activities have to merge at the national level and training assignments should be an ongoing process functional even during peace time.

Platforms : Make Technology the Driver - Lt Gen K Surendranath, AVSM**, SM, VSM, COS, Headquarters Southern Command

Today it is possible for people to operate equipment from thousands of kilometres away and hit targets which are talking to each other in Afghanistan and Somalia with the help of network centricity. However, the Indian Military still emphasises increased technological use in platforms.

Network centricity enables a commander to create the desired impact when equipped with the knowledge of his troops, enemy and the lethality of weapons at his disposal. Chinese have a mix of missile and air force technology to facilitate delivery of pay loads in high altitude as existing in Tibet. This has been possible through networking and integration.

There is a need to network the existing platform technology within the Indian military. One part is the sensor network, this data needs to processed and digitised so that the commander can perform accordingly. Hardware is changing rapidly, at times within 6 months to two years, whereas software is something that can be changed in a shorter time frame. Therefore, software development is required to process the requirement at each command level in which the hardware can later be plugged.

Once the whole system is networked, one can base the strategy on effects rather than concentration of forces. Since the 1960s, platform technology has slowed, with an increasing explosion of information. This is also because platforms cannot be guarded without network centricity. Therefore attention and resources should be plugged towards getting information and networks. For example, tanks which have been designed 30 years ago are still in use and can now be modernised through technology and their application can be made more potent through networks.

Technology transfer does not come easy. It comes with collaboration, which is possible only after both the parties have assessed the core competencies they have to offer. Unless we push hard and put the maximum amount of money and other resources into our projects and networks, technology and platforms will not work.

Core Technologies Impacting Modern Warfare – Lt Gen Anil Bhalla, VSM, Director General Perspective Planning & President Executive Council, CLAWS

War is a product of its age. The tools and tactics of how we fight have always evolved along with technology. Warfare in the Information Age will inevitably embody the characteristics that distinguish this age from previous ones. These characteristics affect the capabilities that are brought to battle as well as the nature of the environment in which conflicts occur. Often in the past, military organisations pioneered both the development of technology and its application. However, today, technology is being driven primarily by the demands of the commercial sector. Furthermore, technology is being applied commercially in ways that are transforming warfare around the globe.

The advent of nuclear weapons, however, revolutionised warfare forever. For the first time, a weapon had been built against which there was no effective defence, the link between victory and survival was cut. Thus the very nature of war as an instrument in the hands of the political hierarchy is being questioned.

To comprehend the nuances of the effects of technology in future warfare, we must first visualise what Future Battlefield milieu would be like**.** The future battlefield will extend beyond immediate geographical space and physical domain with the increasing ability of the warring sides to look deep into each other's arena. There shall be near real time flow of information due to advance integrated sensors. Precision fires would enhance lethality, cause heavy degradation and provide deep strike capability. Non linearity of mechanised operations may dictate the order in the plains sector but in the mountains it is still likely to remain a war of attrition. The battle would extend into multi spectral domains, conventional, sub conventional & non conventional. Technology would be a major force multiplier and would drive cyber, space and information warfare and these would be fought in the backdrop of nuclear environment.

In our quest for modernisation and seeking new technologies, an indigenous strong Science & Technology base is a must. This would lead us to realise a strong defence industrial base. There is a need to map our technological status and identify the gaps, then prioritise technologies to be developed; thereafter the methodology of development either through transfer of technology, partnership or a collaborative approach needs to be ascertained. The major challenges that we are likely to face are absorption of technology, the need to shorten the technology development cycle and an effective approach to deal with technology denial regimes.

Anti-Technology – Shaping the Battle Field- Lt Gen Davinder Kumar, PVSM, VSM & Bar (Retd), former SO-in-C

Theory of duality is applicable in all aspects in the universe. Digitisation of battlefield cannot be proved unless the dual nature of technology is emphasised, i.e. to counter technology there is anti-technology. It is cheaper to harness and employ anti-technology. It can be defined as *technology used to interfere, diminish or negate the intended function of another technology*.

In the traditional battle space to counter bow and arrows, there was anti-technology available in the form of shield and body armour. In the Industrial age, anti-tank technology and weapons have kept pace with the development of existing technologies. Evolution both in technology and anti-technology has augmented capability and survivability of tanks in battlefield so much so that the utility of tank is diminishing. To restrict mobility of tanks people use logs, trenches anti-tank mines whereas incorporation of machine guns, camouflage systems and armour thickness are certain protective measures taken to save the tanks from any harm. Detection and location of tanks has become increasingly possible. To negate camouflage and concealment technology, we have radars, infra-red sensors, satellite imagery, UAVs etc.

Coming to anti-technology and its R&D aspect, increased detection capability is the prime focus. Matured technology in the form of electro thermal mechanical guns are now in place, efforts are being made to put the stealth technology into tanks too to protect them from radar detection. The most important anti-technology is electronic countermeasures (ECM). Radar is one of the most versatile and prominent sensor available in land, sea and air which contributes greatly to battlefield transparency. Target modification presents to the radar a different object that one wants to be seen as by changing electrical properties and shaping the target effect. This ECM is practiced by armies across the world. Many countries have exclusive aircrafts only meant for ECM.

There are counter electro optic systems available to beat night vision devices both by dazzling and damaging. Infra-red counter measures provided by means of flares have already been deployed by Israelis and the United States. Anti-radiation missile is another anti technology which is only meant to destroy radars. It can be used against communication systems and jammers. Anti-radiation systems have been provided to Pakistan by China.

Electromagnetic Pulse acts like a stroke of lightening but is stronger and faster. These are specialised weapons designed to destroy information systems. It does not destroy buildings or humans and is therefore an attractive technology. They provide an edge in strategic warfare. E bomb has the capability to neutralise vehicle system, target system, communication system, navigation system, long and short range sensors.

The anti-satellites are designed to incapacitate or destroy satellites. India has all the parts and the capability but it has not been translated into action. Chinese are investing a lot into anti satellites. At the heart of asymmetric warfare is the cyber warfare which is an anti-technology and often more powerful than weapons of mass destruction. China has harnessed this anti-technology to counter the technological capabilities of United States. Investment in technology and anti-technology would remain an area of focus in a difficult operational scenario. IEDs, anti-air craft missiles, cyber warfare have become prime agents of asymmetric warfare.

Unified Battle Space- Col KPM Das (Retd), CISCO

It's essential to draw synergies in a military space to reduce costs. Building technology needs innovation in the cognitive domain for which people should have the desired skill set and capabilities. To take the route of indigenisation at least in the Indian context will take at least 10 to 15 years.

Technology is largely constrained by the hardware deficiencies. Despite the existing challenges, unification of battle space has to be looked into. Even if an equipment is bought in the strategic space, it will also have an impact on the mobile and deployed domain. There is a need for a master electronic platform for all systems under development. All one needs to do thereafter is to pull out and insert cards, depending on which system to use. This system will also make the training mechanisms much easier.

Joint operations will involve integration. We need to find smart ways of trusting the concerned parties. To achieve this, indigenisation will play a major role where innovation has to maintain a continuum and strong defence R&D has to put be put into place with greater emphasis on building smart platform technology.

Command and control systems would like to see a unified view of the network. However serious integration into the operation needs to be ensured. The development of software, its size, weight and application should be of a small footprint so that it requires a small hardware. Voice, data and video need to be looked at in a unified way. Defence forces going back to the old order, one has to see a unified battle space.

Procurement cycles at present are long and strenuous. It would be a better idea to shift our focus to two year acquisition cycle which will solve the purpose and meet the requirements. Procurement cycle around the world is same but fundamentally it takes time to procure large systems. This needs to be acknowledged it and factor it into planning. This will lead to optimisation of capital funds.

Concluding Remarks by the Chairperson: Lt Gen Davinder Kumar, PVSM, VSM & Bar (Retd) former SO-in-C

The relevance of technology in establishing military strategy and capability is well known. India has seemed to have missed the industrial revolution as far as building a

viable military capability complex is concerned. We are not doing well in the ongoing information revolution as well. Strategic deficiencies and our defence forces continue to depend on imported material and systems. There is little follow up on the process of indigenisation, even when it has been declared that by 2020, 70 percent of our defence production would be indigenous. Technology and war have never been far apart. Possession of technology is imperative for national security. Nations have to develop technology absorption capabilities; skill set capabilities and production, procurement policies. Development of core competencies in critical and sensitive technologies is the key to large scale system integration which requires knowledge and experience.

SESSION II: CYBER AND SPACE

Remarks by Chairperson - Lt Gen (Retd) SP Kochhar, AVSM & Bar, SM, VSM, former SO-in-C

The chairperson underscored the importance of cyber and space in the overall theme of the seminar on digitised battlefield.

Cyber Warfare: Offensive and Defensive aspects– Lt Gen (Retd) SP Kochhar, AVSM & Bar, SM, VSM, former SO-in-C

What constitutes cyber? It is not only about data, software, and networks. It is a combination of everything an individual uses to achieve the desired results. In today's environment we cannot say that cyber is only for offense or defence. It's an end to end solution of anything which is electronic which includes data storage. In the present times one needs to be covered by seamless networks to be current and relevant. How to you build cyber security? What to build first, networks or security? Ideally they should go together as they can't be built overnight. The components come from different vendors and industry has one major aim, to reach targets. The ideal way is to build all the systems under supervision but indigenisation is not possible overnight. So we need to do it step by step. Any element you use in a network is a suspect. We need laboratories to sanitise the hardware and the embedded software. We need to set up labs for the imported products while we simultaneously develop our capabilities to produce domestically.

What is that one component that can take us on the path of cyber defence?

- Design and Fabrication. The costs aren't too high and the outlay will not be much for a country like India.
- We can make the most critical components so that we can create a niche for ourselves.
- At least in the most critical component we will be secure.

In India only the defence forces plan, test and roll out their networks in addition to systems and software. The telecom companies build their software and say they are cyber secure but it is not the right way. The hardware can be tweaked and manipulated. For instance telecom equipment was reconfigured in Pakistan recently

to block You Tube. This inadvertently caused disruption in Europe also for 2-3 days. However, the same can be done deliberately also. For cyber tools to be effective they have to be home grown. We have been grown up in an atmosphere where we start using things blindly instead of questioning it. Further, there is lot of overlapping and duplication. We need policy changes to enable and create the right atmosphere. The psychological impact is also crucial. At times the systems are fine but the psychological impact is negative and that affects the quality of work.

Coming to cyber offense and defence and a third term cyber exploitation, can these be handled separately? It may be administratively convenient to say that they should be handled by different people. But how can one defend something they do not know or take ownership? Cyber defence is bottom up. Everyone has to know how to handle and defend his systems. Cyber offense is different, it is top down. It has to come from the top level. Cyber exploitation is essentially intelligence. With further networks coming up they can be used not only by law abiding citizens but also anti-social elements. Business intelligence is used by corporations to gain competitive advantage however the same can be used by the military to collect intelligence.

We need to invest in R&D which currently is not adequate. The private industry is not investing as they don't see enough business opportunity. Concerted efforts are required in this direction from all concerned.

Space: Force Multiplier for Digital Battlefield - Maj Gen AB Shivane, VSM, ADG PP

Space is more than a domain for technologists. It is becoming an increasingly critical component of national security, sovereignty and well-being and more so in the military domain. In the present environment, as the battle lines between war and peace get blurred it is all the more important to have the capabilities to respond to any threat.

The three key areas are:

- Where does Space fit in digitised battlefield?
- Indian space canvas and capabilities, opportunities and emerging military applications
- Future space mission trajectory, threats and challenges

Part I: Space in the digital battlefield

Space is certainly not a new domain in India. The Pushpaka Vimanam, the Mysorian rocket by Tipu Sultan in battle of Guntur in 1792 are a testimony of our exploitation. Over a period of time the use of space based applications has escalated and their utilisation has manifested manifold. What is emerging in twenty first century is a transition from space being a force enhancer to a force enabler. Today nations are transiting from being space supported to space powered in which space itself is a separate domain contributing critically to the security and war fighting capabilities of a nation. Space is being increasingly looking at as a status of an emerging and a world power.

Summation – 1: There is a need to differentiate between space as a medium of supporting terrestrial warfare and viewing space as a medium of future warfare itself which are two different things.

Space is the ultimate high ground. Digitised battle space is essentially standardising the organisational structures and operational outcomes to win battle decisively with least cost and time. This means better situational awareness, real time sensor-shooter links to enable commanders to take decisions in almost real time frame. Looking from a field force commander's perspective the three critical components necessary to take fast decisions in a battlefield are time, space and force. In the quality of enablement, space, be it from a point of view of ISR, SATCOM or Position, Navigation and Timing (PNT) provides this capability to shorten the kill chain to find, fix, track, target and engage. So it is essential for nations to enjoy space superiority. It is equally important to have negation capabilities to deny the same to the adversary. In the digital battlefield six core functions can be related to space based capabilities.

Command & Control is the nerve centre of the digitised battlefield. Dissemination of information, assessment, reassessment and taking of requisite action in real-time is the requirement. Awareness of own & enemy situation by speedy decision making by integration of sensors, weapons and logistics. ISR and PNT are the two key capabilities to enable the aforesaid.

SATCOM provides battle space coverage and helps to maintain situational awareness by conveying intent to the tactical commander. It provides seamless interconnectivity from highest level to tactical level through digital video, data and audio.

Intelligence contributes to development of intelligence by recce and surveillance and through observation by visual, electronic and photographic means. Low earth orbit satellites give coverage of target on the order of minutes and geosynchronous satellites give persistent access to large portions of interest.

Movement and Manoeuver is the ability to bring about force manifestation at the desired time and place enables forces to achieve a position of advantage and bring desired effects.

Targeting in an era where standoff capabilities and effect based operations are taking dominance, targeting by operational fires, air & missile defence systems are gaining prominence. PNT capabilities enable precise 3D positioning capability, target location and guiding precision munitions.

Sustainment ensures freedom of action and extends reach of operational forces. This is enhanced by SATCOM and PNT capabilities.

Protection is becoming critical with proliferation of Anti-Ballistic systems, space based sensors and the need is to take deterrence and counter measures.

Summation – 2: Space operations give the decisive edge. We can see the battlefield with clarity, communicate with certainty, navigate with accuracy, strike with precision, operate with assurance, acquire with agility and at the same time deny all these to the enemy.

Part II: Indian space capabilities, opportunities and emerging military applications

Coming to Indian space capability, expanding horizons and emerging military applications, ISRO is a success story. From a modest beginning it has come a long way and is taking up exciting ventures. In the expanding horizon it is important for us not only to harness civil capabilities for military use but also develop certain capabilities peculiar to military use to attain high levels of force enhancement and defensive space control with integral military capability and desired satellite systems. They need to have certain redundancies and be fool proof to enemy measures. Sub meter resolution capabilities are currently available. But we desire resolution<0.2 m in future. We need operationally responsive space capability not only for military but also for disaster management to cover large area. We have SATCOM but bandwidth is a limitation. GAGAN is set to become operational in coming months. Space is a joint domain and a joint space command is necessary for which work is in progress.

Summation – 3: While convergence and dual use of space technology is essential and a must we need to look at specific military utilisation and military assets in space.

Part III: Future space mission trajectory, threats and challenges

India has multi front obligations with increasing threats and there is a diabolical nexus between our neighbors. As a nation who believes in strategic autonomy we need to maintain independent deterrence capability. Then we have certain regional and global responsibilities of a stable democracy & emerging power and so need to hone our deterrence and response capability for national security objectives. Looking at our neighbours, China certainly has a space capability though it is rudimentary in some aspects. China has demonstrated A-Sat capabilities and even launched micro satellites recently to repair satellites in orbit. Pakistan though doesn't have capabilities of its own but piggy backs on the Chinese. In this regard there is a space decision dilemma.

Option A: Maintain The Status Quo And Do Not Deploy Weapon Systems To Orbit. Continue the development of space-based force enhancement and information systems while developing ground- based space control negation systems.

Option B: Develop technologies for Offensive Space Control and ABM Systems to counter emerging threats to meet national security objectives. In conclusion:

- Space is central to network centric warfare and the digital battlefield.

- India must integrate Space capabilities at all levels of operational command, and expanding senior leaders' understanding of the utility of these forces relative to other tools available.
- Threat from our adversaries is real and we cannot ignore it. The nation has to decide to preserve space solely for peaceful purposes, or to protect our vital national interests through increasing convergence and if required in future, develop space control capabilities.

Enablers for Space Sensors in the Digital Battlefield - Air Vice Marshall (Retd) Dev Ganesh, Honeywell

In the digitalised battlefield we need to understand what components are required and for what purpose to achieve the big picture of the digitised battlefield. So we will discuss three or four sensors and the role they play.

- Surveillance by Panchromatic, IR, SAR, Multi & Hyper spectral Imaging sensors
- Electronic Intelligence and analyses of voice and data transmissions
- Communications: Data & Voice over very wide distances. - Controlled Transmissions through Beam Forming Networks. For instance to restrict the footprint of a geostationary satellite at 36,000 km which has a huge footprint, it is possible to limit the beam of the satellite to a limits space. To jam the transmission from a satellite it is necessary to be within the footprint of it. All of the above depend to a large extent on accurate Positioning, Pointing or Beam Shaping of the satellite, sensor or beam.
- Air & land vehicle Management by Sky Connect, Osprey Wings, through satellite networks.

The AVM talked about Miniature Inertial Measurement Unit (MIMU), Space IFOG IMU, Integrated Stellar-Inertial Attitude Determination System (STARMU), produced by Honeywell, highly accurate and robust units that help satellites maintain their position in space. This in turn contributes to accurate ISR inputs from the satellite. The Reaction Wheel Assembly Family, works on the principle of precession and helps control the satellite to point it at the desired place. The Sky Connect Air Craft Tracking System uses the Iridium constellation and has the following capabilities:

- Tracking of all airborne assets in all types of terrain with 66 satellites in Low Earth Orbit (LEO).
- Automated position reporting plus urgent notifications.
- Voice calling using dedicated dialler direct to Operation Centres for fast response to hostile action.
- Pin Point rescues after shoot downs.
- Iridium set to enter India, in talks with BSNL/MTNL

The Osprey main features are as follows

- Worldwide Tracking, messaging and alerting

- Alerts to multiple contacts via SMS and email as well as systems messaging
- Effective for ground as well as air vehicles
- Up to 450 customisable pre-defined messages
- Stealth mode for silent and low backlight operations
- Customise views using Points of Interest.
- It is already in use with several state and central police forces in India.

Discussion

- Importing critical software is a concern and indigenisation is the key. We cannot afford to be left behind.
- Indian Space cell is looking into all space requirements including mobile SATCOM and orbital intelligence.
- India is planning to launch a constellation of 3-5 ELINT (electronic intelligence) satellites to monitor of communications.

Closing remarks by the Chairperson - Lt Gen (Retd) SP Kochhar, AVSM & Bar, SM, VSM, former SO-in-C

The discussions bring out how critical battle space is getting for the military warfighter and how much emphasis is on to the space, but at the end of it we must remember that finally it is all about defeating the enemy in time and space. All efforts need to be made to disrupt the enemy's decision cycle.

Discussion

- Because of the acquisition process it's easy to buy the hardware but software is a different ballgame. Software for a networking system needs the concerned people to sit and determine the output. This has to be then translated to the industry to build the appropriate one. In all this transparency is needed.
- The role of IT in refurbishing old systems is limited. It can only be used where there is a software component involved but not in standalone military systems.
- Recently a system called Shakti has been fielded as part of artillery networking which is an IT command control system. It has reached the field formations and lot of feedback has been received. Certain software glitches have been identified which are been addressed.
- India has reasonable capabilities in satellite communication. The army has the capabilities but not at the field formation level.
- There is a basic flow in the relationship model between the developer and the user. Culturally there is a trust deficit. Money making is the incentive for innovation. The other problem is systemic. There has to be a working relationship.
- There is a need for basic integration between basic science and applied science. Technology has a cycle - develop, produce, field, exploit, maintain and then upgrade. The entire cycle is about 15 years.

SESSION III: OPERATIONS AND TRAINING ASPECTS

Chairperson: Lt Gen Aditya Singh, PVSM, AVSM (Retd), Former GOC-in-C Southern Command**

Training and Operations are the most important aspects inspite of the dependence and rise of technologies. In this age of digitisation, technology has acquired a new dimension. In the digitised battlefield, scope for damage or advantage is immense. The kind of vulnerability that grows with the situational awareness and reach over a wide area are tremendous. Therefore, training and operational aspects becomes crucial. With digitisation, there is also the aspect of insider threat. Instances of Wikileaks, Manning and Snowden leaks speaks for itself when it comes to insider threat in the realm of digitisation of battlefield. Digitisation of battlefield provides democratisation of battlefield. It provides tremendous advantages but also provides scope for tremendous disaster. Disaster comes from the weakest links; therefore, implementing it in the Indian scenario is vital.

Battle Command Systems: User's Perspective I: Mr Michael O'Hara Kelley, Senior Programme Manager, DRS Technologies

Battle Command Systems (BCS) is all about the user. The complaints about equipment not working properly is because the user are not being consulted at the development stage. The most important aspect of BCS is to provide right information to the right person at the right time in the right format to make the right decision. When a deluge of information is obtained, it is important that this information is converted into data for confidently executing the Commander's intent. For information to be transmitted in the right format through a military formation right from the soldier level to the brigade level, user interface becomes important in the realm of BCS.

In order to understand the information being transmitted from the battlefield, there is a need for a single ubiquitous BCS from the lowest to the highest level while tailoring to the users needs. Critical thinking is also necessary to understand the essence of the battle and the essence of the mission. Exclusion of all the things that do not

matter and focus on the things that matters is vital to act on the information obtained from the battlefield.

What is being done to understand the Commander's intent and to instill trust on the command by creating a trustworthy BCS. For BCS to be working efficiently, it is important to consider the user in the BCS because every individual has their own unique capabilities. Therefore, for the optimum functioning of the BCS, there is a need for tailoring the BCS equipment to the specific needs of the user. In other words, it is important how users need the BCS. One of the ways of tailoring the BCS to user's specific needs is to simplify the whole system by integrating the already existent user interfaces. For example, for a seamless transmitting of information, BCS can be integrated to the likes of Microsoft Office, which everyone is familiar with.

What is important to note here is how the legacy of today is being taken forward so that it works together with future technologies in the coming times. This is so because if old and new technologies are not tied together, it becomes a very expensive affair to get hold of completely new technology. In other words, technologies becomes obsolete is a very short span of time. Technology to be efficient in battlefield should be taken to the tactical level of the soldier.

However, what is really preferred is a common hardware right from the soldier to the highest level that does the same mission command and battle command operations. Common hardware makes it easy because it can be replaced easily with a common software suit. Last but not the least, the most important aspect is working with the user as they are the ones who will use the equipment, trust the equipment and provide feedback of the equipment.

Battle Command Systems: User's Perspective II: Mr Jayesh Shah, Sr Principal Engineer, DRS Technologies

There has been a lot of debate over exportability of equipment provided from overseas. DRS Technologies has been working with the US government and as such, DRS Technologies equipment and technologies are very much exportable. Since DRS Technologies' involvement with the Indian Army for digitisation, the company is fully aware of the ToT requirements among other such requirements.

Configuring a system is the most challenging task in a battlefield. One cannot configure a system that suits the user. Further, the mission does not have to suit what the user has in his platform. In order to do that there is a need to minimise the size, weight and power for integrating into a system. There is also a need to integrate new systems into the old equipment and the only way to do that by trying to minimise the impact of the new technology in the existing platform.

DRS Technologies works towards providing the best C4ISR system not only to the United States and UK Army but also for the Indian Army. DRS systems are designed specifically for the Army. The design are designed primarily to meet Battle Command needs and not for any other purpose.

Over the years there has been tremendous improvement in the quality of the equipment used in BCS and at the same time, there has been tremendous decrease in the cost of the same. Though there has been huge advancement, the footprint of these equipment remains the same so that the overall system does not get affected.

In the Indian Army there is a need for convergence of equipment between the old and the new ones. However, what is important in this context is that the introduction of new equipment does not mean discarding of the old one, rather their coexistence. Further, integrating new and old technology is important to have a seamless network in the digitised battle space.

A BCS is not just buying computers and displaying GPS, rather it is important to integrate different parts into the system, which addresses the weight, portability, power and footprint issues. Herein, it is important to use technology that the young soldiers are already familiar with and which does not require training.

Expectation from Net-Centricity in the Battlefield: Maj Gen RP Bhadran, ADG IS, DGIS

Net-Centricity evolved from a simple theory of networking, which has proved itself in management and marketing. Taking forward the same concept, networking has been delimited in the military forces. It has been believed that war-fighting ability will improve with networking.

In the backdrop of the First Gulf War, several steps have been taken towards net-centricity. The classic case of technology and operations moving hand in hand is that technology has opened up new vistas for war fighting.

In broad terms, there is a need for real time operational picture, real time intelligence picture, and facilitating fast decision-making. Net-centricity lightens the fog of war and then it will manifest into decision making dominance, collaborative achievement and search missions. Besides, warfare facilitated by powerful computers and smart applications on one side and stable network and communication on the other hand facilitates digitisation of battlefield.

In addition, high tech sensors and their integration into weapons has aided the net-centricity of battlefield. However, the expectations are availability of the real time operational picture, rapid deployment of forces, status of deployment of equipment and arms requirement. Further, there is a need for real time status of enemy movements. This is where the sensors come in. More the number of sensors, more information is being obtained. At the same time, net-centricity does not suggest that the battlefield be littered with sensors, rather what is expected is that it will facilitate focusing on the available sensors.

Net-centricity is also expected to provide with a computer assisted planning of the battlefield. In other words, net-centricity is expected to provide assisted terrain analysis with high-resolution maps with obstacles, corridors, killing areas etc. drawn up. Similarly, anything which is purely mathematics is expected to be fully automated especially the logistical aspects – stocking, build-up, replenishment, mobilisation etc.

Cyber security system is an important aspect of net-centricism. Application should be the main constituent in this realm. Computers should be power efficient and portable because footprint of the system is required to be kept as low as possible so as to avoid giving its signatures to the enemies. There is a need for different form factors with full- fledged servers for all platforms and integrated units where there are no illuminated displays.

As far as communication devices are concerned, the focus should be on non-emitting media so that it is not prone to be interfered. It should be complimented with

short-range configured radio sets and work in low bandwidth. All networks should be secured so that the enemy does not gain an advantage through unsecured networks.

The application software has to be lean and mean so that the associated hardware can be lean as well. Bare essential features should be given to the system. Middleware should be avoided or modified for usage to consume less resource. To stabilise network in technical battlefield, applications should be able to determine the peacetime usage and wartime usage automatically. Finally, the important aspect of geographical systems is that it should have common across all applications to avoid problems during exchange of information.

Making of a Digital Warrior: Col Sameer Chauhan, Senior Fellow, CLAWS

Every citizen is a warrior when one dwells on digital warrior in today's scenario. Conventional conflicts will have high tech content. So combatant will be required to have high tech equipment. Warfare will be more mental than physical contest. Education on technical skills among military personnel will be required more than what is present today. Therefore, in a nutshell, the future will have technologies related to surveillance, observations, navigation, reduced time for decision, increased decision taking at a junior leader level, increased precision weaponry, multi-media electronics, even part of soldier's kit. Similarly, digitisation of the in-service equipment, increased media and coherence with other services and other departments. The soldiers will need to imbibe technology such as augmented reality technology, brain-computer interface etc.

Some recommendations include – Human resource management and awareness training. Over the years, average threshold of the Indian combatants have increased. This has to be taken into consideration in the discourse of digitisation of battlefield in the Indian perspective. At the same time, there is need for identification of specialist within the Force for usage, and up-gradation of the systems.

The first stage is to identify those who have a technical frame of mind. Thereafter, nurture and train and retain the identified resources. There is a need for institutional process to identify such specialist. Incentives are also important in the process of nurturing and retaining such specialist. There is a need to structure short or medium courses in Military Institute of Technology so that the identified specialist gets their

training there. Continuity of such specialist in a project is also the need of the hour. There is a need for realignment of policies in the Indian Army for the purpose of continuity. The officers involved in project development programmes should be allowed freedom to enhance their wisdom through various mediums.

Further, e-learning has to become a norm rather than an exception not only for learning but also for information exploitation. Training the digital warrior in virtual world including simulations, virtual training has to be a culture and a habit. There is also a need for awareness of the technology that has been planned for induction into the Army. One possible way is to update it in the Indian Army website. There is also a need to inculcate faith in the indigenous systems. In house system will have flaws but it is only when they are used that a credible feedback will build up which will lead to further development.

Interaction – During the interaction of the session there were queries about digital maps in India, for which the response stated that there are digital maps in Indian no doubt, but digital data is inadequate. In a question on ways of enabling the Indian soldier, the respondent replied by saying that Indian soldiers can be enabled by indigenous systems for which there wouldn't be any need of outsourcing. On the question about the software on handheld devices, the answer was that the hand held devices at the moment are scaled-down version of the desktop. Finally, on the question of how to ensure right information at the right time to the right person without overload, the respondent stated that right information at the right time to the right person without overload can be achieved by having the right type of systems in the battlefield. The same can also be achieved through hardware and software sychronisation and role-based configuration.

Concluding Remarks: Maj Gen Dhruv C Katoch, SM, VSM (Retd), Director, CLAWS – The seminar was interesting and has contributed to the learning experience on the battlefield use of technology. Enabling winning capabilities in future conflicts and Digitisation is the way to move forward for the Indian Army. The seminar has taken a look at platforms, sensors, cyber, space based issues and also operational and training aspects. India still has a long way and the bottom line is that India need to expedite its indigenisation programme.