Impact of Technology on Warfare

Lieutenant General PC Katoch, PVSM, UYSM, AVSM, SC (Retd)*

Introduction

Advancements in technology have revolutionised warfare already. By 2025, technology would have gone to the next step or perhaps the next to next step. With continuing volatility in India's neighbourhood, we may be faced with heightened threats in future through the spectrum of conflict particularly; in the asymmetric spheres, along with militarisation of space and heightened hostile activity in cyberspace. There is a need to examine how technology will impact future warfare, what our voids and weaknesses are with respect to technology and what initiatives we need to take in order to enable India gain its rightful place in the comity of nations.

Present Impact of Technology on Warfare

Technology enables hi-tech wars that are short and swift. Ranges, accuracy and lethality of weapons have increased very considerably. Concurrently, the space and time continuum has been greatly compressed. There is exponential increase in situational awareness and battlefield transparency as forces are shifting from platform centric to network centric capabilities. Simultaneous handling of the strategic, operational and tactical levels is possible. Improved battlefield transparency in turn has increased the importance of dispersion of forces and need for deception. Technology has ushered the advent of offensive cyber warfare, information dominance, space wars and Effect Based Operations (EBOs). Ironically, technology has also empowered the terrorist to cause more severe damage.

Future Scenario

The regional security environment surrounding India today includes failed and failing states. We are faced with nuclear threat, missile threat, cyber threat, cross border terrorism, infiltration, demographic assault, conventional threat and insurgencies. Besides, we are battling continuing asymmetric wars waged by both, China and Pakistan. The 27 odd terrorist organizations operating in India including the Maoist insurgency are open to exploitation by our adversaries. The US thin out from Af-Pak Region and increased Chinese forays into POK, Pakistan, South Asia and the Indian Ocean Region (IOR) will enhance collusive threat from China and Pakistan.

Pakistan's obsession to control Afghanistan and get the Indians out is unlikely to recede. India should, therefore, be prepared to continue to battle asymmetric war with overlaps of conventional war (both with China and Pakistan) under the nuclear shadow. Insurgencies in India are likely to continue with burgeoning population unless we can manage the social change very well, of which the signs at present are not very encouraging. Cross border terror may escalate with ISI's tail up, Pakistan's *jihadi* policy, tacit support by China and expanding globalization of terror outfits like the Lashkar-e-Toiba (LeT). Existing LeT footprints in Maldives, Kerala and efforts to link-up with the Maoists spell more danger, especially for South India. The current Opposition in Bangladesh is known for its links with anti-India terrorist organizations and change of guard in Bangladesh could increase our problems. Space and cyber space will be active battlegrounds, particularly because of credible capabilities of China. Militaries alone cannot cope with new threats, courtesy globalization. Ability to conduct integrated operations with other components of Security Sector is necessary. The entire Security Sector will need to integrate to cope with 21st Century challenges. The Security Sector will encompass the Armed Forces, Special Forces, Para Military Forces, Central Armed Police Forces, Coast Guard, Intelligence Services, Private Security Services, Customs and Immigration Services, concerned Government Ministries / Departments and the like. Therefore, while developing and planning future defence related technologies, it would be prudent to look at the entire Security Sector.

Cyber warfare may emerge more dangerous than even nuclear threat due to ambiguity in the source of attack and the potential to cripple critical infrastructure of a country, bringing it to a standstill. Internet has increased vulnerability to cyber attacks. Prevention is being replaced by pre-emption and the cyber race is becoming endlessly vicious in the absence of any international norms. 25 million strains of malware were created in 2009 alone1, whereas, 286 malware variants were detected in 2010 – average of one every 0.79 seconds2. Offensive information dominance is the new buzzword. Under threat are national security and our economic well being. Cyber security is talked more in terms of "cyber insecurity"; courtesy hackers, phishing, malware, viruses, automated internet tools, e-bombs, logic bombs, electro-magnetic pulse (EMP) and high pressure microwave (HPM) attacks. Critical infrastructure and distribution systems are highly vulnerable. Geographical distribution of networks and sheer size of devices and networks is a challenge, especially with the use of different interoperable protocols and diverse equipment and largely untutored work force with little interest in IT security. Effects of errors and omissions are increasingly catastrophic. Attacks are organized, disciplined, aggressive, well resourced and sophisticated. Adversaries are nation states, terrorist groups, criminals, hackers, non-state actors, latter largely a misnomer. Significant exfiltration of critical, sensitive information, planting malicious software occurs on regular basis. Major cyber attacks on critical infrastructure and control systems have occurred since 1982 involving oil / gas pipelines, emergency alert systems, floodgates of dams, communications and power of airports, sewage system, nuclear monitoring system, power grids, train signaling system, canal system, nuclear power plants, hospital communication system – to the power blackout in Hong Kong Stock Exchange in 2011. The prolonged power blackout at Terminal 3 of Indira Gandhi international Airport on 06 Aug 2011 could well have been caused by a cyber attack.

Future Technological Developments

Listing out all the likely technological advancements with military applications by say year 2025 would require many pages but existing improved assault rifles will perhaps include phased plasma guns. Plasma weapons already reported in Russia, focus beams of electromagnetic energy produced by laser or microwave radiation into upper layers of atmosphere to defeat targets flying at supersonic or near-sonic speeds, bumping the targets out of trajectory. Laser weapons would be fielded on land, sea and air. Our DRDO is developing a Laser Dazzler for police forces that will impair vision temporarily to control unruly crowds. DRDO's Laser Science & Technology Centre (LASTEC) is developing

a vehicle mounted gas dynamic laser-based Directed Energy Weapons (DEW) system, named 'Aditya' as a technology demonstrator. A 25-kilowatt laser system is also under development for hitting a missile in terminal phase at a distance of 5-7 kms. DRDO identifies DEWs, along with space security, cyber-security and hypersonic vehicles as future projects. MoD's "Technology Perspective & Capability Roadmap" identifies DEWs and anti-satellite (ASAT) weapons as thrust areas over the next 15 years. However, given the track record of DRDO, how much they will actually deliver by 2025 is anybody's guess.

While there was much talk of stealth helicopters in the recent US Navy Seals raid in Pakistan to kill Osama bin Laden, the US has already developed a Reusable Space Plane (X-37B) – another step in weaponising Space. In addition, a powerful conventional weapon (Prompt Global Strike), as alternative to nuclear warhead, is under development, which can travel halfway around the world from launch to target in less than 30 minutes, using missile launch, release of hypersonic gliders and eventual release of 1000 pound deep penetration bombs. The revolution in communications equipment is already visible in commercialized products. The narrative of technological advancements can go on endlessly. China's indigenous aircraft carrier could be twice the speed of existing carriers with a catamaran type of hull greatly reducing pitching, yawing, swaying and capacity for simultaneous launch and landing of aircraft from twin flight decks. India's Space Vision 2025 envisages satellite based communication and navigation systems for rural connectivity, security needs and mobile services. Imaging capability is to be enhanced for natural resource management, weather and climate change studies. Indian Regional Navigational Satellite System (IRNSS) with seven satellites is to be up by 2012, enabling deployment of indigenous GPS. Space missions and planetary exploration are planned to understand the solar system and the universe. Development of a heavy lift launcher, Reusable Launch Vehicles as Technology Demonstrator missions leading to Two Stages To Orbit (TSTO) and human space flight are also planned.

Technological Transformation

Considering the rapid rate at which technology is progressing, 2025 should actually see a quantum jump. Fully Networked Centric Warfare (NCW) capable forces would be operationalised. Better PGMs would be available including High Energy Lasers, Plasma, Electro Magnetic, Ultra Sonic and DEWs. ISR and communications would be revolutionalised. Long range strategic Aero-Space Platforms would be in play. Stealth and Smart Technologies and Artificial intelligence would be optimized. Improved nukes would be more compact and lethal. Nano weapons and equipment, including Micro UAVs, Ant Robots and the like would come in. Cyber Warriors, Worms, Viruses, CyBugs would be common. ASATs would be in use. Considerable progress can also be expected in the ongoing research of mind control, albeit this too can have adverse effects for mankind, should it fall into wrong hands. Most of these technologies, as mentioned above, would have come in China by 2025 and some of them by extension in Pakistan.

Impact on Future Warfare

Technological advancements, as mentioned above, will greatly affect the manner in which wars will be fought. Conflict will be five dimensional to include Aero-Space, Land, Sea, Electro-Magnetic and Cyber. Information Warfare will include Network Centric Warfare (NCW), C4I2 Warfare, Electronic Warfare, Cyber Warfare and all other forms of operationalized Cyber Space. Space Combat, Cyber Space Combat, Radiation Combat, Robotic Combat, Nano-technology Combat will add to the forms of Combat. Operations will be increasingly inter-agency involving greater application of all elements of national power. States like Pakistan will continue to employ hi-tech irregular forces. Asymmetric wars will be an ongoing affair. Information superiority will be as important as land, sea and aero-space superiority. The central feature of 21st Century warfare will be that force application must include all domains of diplomacy, information technology (offensive and defensive), military operations and economic activities (DIME). India must invest in all aspects of DIME in areas of our strategic interest. At national level, there would be requirement of constant synergy. De-conflicting actions are required to achieve a united national front. Military jointness is an absolute imperative in the Armed Forces. Ability to conduct integrated operations with other components of Security Sector is necessary.

Technology Related Requirements

Considering the threats to our national security by 2025 coupled with technological advancements, our wish list should be as under, which should also be the focus for DRDO, PSUs and Private industry for development of technologies:-

(a) Networked elements of national power.

(b) Information dominance and information assurance.

(c) Ability to paralyse enemy C4I2 infrastructure.

(d) Credible deterrence against state sponsored terrorism.

(e) Long range expeditionary strategic forces.

(f) Stand off weapons to pre-empt enemy attack.

(g) Mix of DEW, PGMS, ASATS etc.

(h) Ability to disrupt enemy logistics / sustenance.

(j) Mix of hard kill and soft kill options.

(k) Layered strategic air and theatre missile defence.

(l) Competitive cyber warfare capability.

(m) Ability to exploit space and cyber space.

(n) Conventional forces capable of winning high tech wars.

Leave aside the Security Sector, even the Military presently does not even have common data structures, symbology and interoperable protocols. A true "System of Systems" approach has yet to come. The Military must accelerate establishment of Integrated C4I2SR system. Integrated communications must be established to provide seamless communications vertically and horizontally. All platforms must be network enabled. Cyber security must graduate to information assurance and information dominance. A holistic review should be done to ascertain requirements of stand off PGMs, DEWs, ASATs. Technologies like Steerable Beam Technology, Wide Band / Software Defined Radios, Network Security, Common GIS, Data Fusion and Analysis, Alternatives to GPS, Dynamic Bandwidth Management, Lasers to shoot UAVs, Camouflage and Concealment etc should be exploited.

We should not lose focus on equipping the soldier at the cutting edge who is constantly engaged in the sub conventional conflicts. This also applies to the cutting edge of the entire Security Sector including the PMF, CPOs and Police. The Government must focus on indigenous production of critical hardware, software, telecom equipment and chip manufacture. The Defence Procurement Procedure (DPP) with the cosmetic annual review does not meet present day requirements. Its review should be outsourced incorporating academia, think tanks and private industry. Both the civil and military leadership should lend themselves to attitudinal change to accommodate the concept of NCW. The Military Leadership must adapt to the changing nature of war. With respect to intelligence, technology should be exploited for real time / near real time dissemination of the Common Operational Picture (COP) and incorporation of a Decision Support System (DSS) to assist analysis, assessment and decision making. The Military should undertake holistic examination of its ISR and Intelligence requirements. Networking of Services Intelligence with "all sources" intelligence and real time / near real time dissemination should be ensured.

The Government must identify focus areas for R&D. Unveiling of our LCA with 40 per cent imported parts including the engine concurrent to China unveiling its Stealth Fighter, indicates the pathetic state of our R&D. Mr Anil Manibhai Naik, Chairman L&T laments in his letter to the Prime Minister3, *"Defence Production (MoD) Joint Secretaries and Secretaries of Defence Ministry are on the Boards of all PSUs — sickest of sick units you can think of who cannot take out one conventional submarine in 15 years now with the result that the gap is widening between us and China and bulk of the time we resort to imports out of no choice. The defence industry which could have really flowered around very high technological development and taken India to the next and next level of technological achievement and excellence is not happening"*. There is a positive requirement to slash the business empires of the DRDO and make them focus on critical areas. DRDO's recent announcement of having produced a mosquito repellent indicates how unfocused this elephantine organization is. We must truly open defence sector to the private industry, instead of the current practice of "through DRDO and PSUs." The DRDO and PSUs need to be made accountable and responsible. Groups of private industry should be identified for focused requirements. R&D allocations should be reviewed and appropriate share must go to private industry / group (s) of private industry tasked for defence requirements. The DRDO /and PSUs should learn the art of 'reverse engineering' to cut short development time, as is being done by China.

Information revolution and networked environment give rise to various entities. Services must retain core competency and have ability to integrate with other domain specialists. Concept Development Centres (CDCs) should be established involving modelling, simulation and synthetic environment that will provide a powerful aid to visualisation analysis, test, evaluation, training and rehearsal throughout acquisition lifecycle. Simulation is the best way to understand and optimize dynamics of manufacturing processes and support chains. CDCs require networking with knowledge entities. In year 2005, China already had 90 laboratories for chip manufacture. We have yet to establish the first such facility, which proves how unfocussed we are as a nation.

Conclusion

By all indications, India will have to face heightened threats from its immediate neighbourhood by 2025, particularly from China and Pakistan. Technological advancements will activate the domains of space and cyberspace. The widening military gap between China and India will magnify these threats, which need to be taken seriously. We urgently need a revolution in military affairs (RMA) to take us into the next level of military capabilities to meet future challenges. A draft national cyber policy has been prepared, and comments and recommendations have been invited by the Government. The crux will be its speedy implementation and layered cyber protection for security and critical infrastructure protection, leading thereon to information dominance. It is possible if the Government and the Military take various initiatives and pursue them vigorously to ensure speedy execution. We have to act consciously and speedily.

Endnotes

1. Symantec Report 2010.

2. Symantec Report 2010.

3. Anil Manibhai Naik, Chairman of L&T wrote a letter to the Prime Minister, details of which appeared in <rediff.com> on 8 March 2011, 18.58 IST.

***Lieutenant General PC Katoch, PVSM, UYSM, AVSM, SC (Retd)** was commissioned into the Parachute Regiment in December 1969. He superannuated as Director General Information Systems. Post retirement, he has authored articles on military cum security issues. He is an elected member of the USI Council. Currently, he holds the Field Marshal KM Cariappa Chair of Excellence at USI Centre for Strategic Studies and Simulation (CS3).

Journal of the United Service Institution of India, Vol. CXLI, No. 585, July-September 2011.