CENTRE FOR LAND WARFARE STUDIES

ISSUE BRIEF

No. 266 January 2021

Indian Armed Forces Must Prepare to Fight New Generation Wars

Brig Narender Kumar, SM, VSM (Retd), is a Visiting Fellow at the Centre for Land Warfare Studies (CLAWS) and former Distinguished Fellow, USI (New Delhi).

"War is a continuous interaction between opposing forces."[1]

—Carl von Clausewitz

Abstract: *Modern wars are much more than mobilisation of conventional armies for combat. The high-tech weaponry could determine how, where and when conflict will take place and who is likely to win. Although conventional armies are not yet outdated, however, total reliance on them may be counter-productive. Seeing the changing character of war, the adaptation of technology becomes significant. Thus, the suitable restructuring of combat units and formations with an eye on future is of utmost importance. Autonomous weapon systems are here to stay and they are becoming an important tool of intelligence gathering, target acquisition, reconnaissance and suppression of enemy ground and air defence systems. India needs to rethink its war fighting methodology so that future challenges by state and non-state actors can be dealt with and identified early. The recent wars and sensational attacks by non-state actors against economic and military targets have made great powers to re-think their doctrines, strategies and incorporation of technologies to secure their physical and cyber frontiers.*

Key Points

- Drones are becoming an integral part of modern armed forces for Intelligence, surveillance, target acquisition, and reconnaissance (ISTAR) missions and a potent platform for destruction of ground forces.
- Teaming up of human resource and technology is a battle winning combination to win new generation wars.
- Although the conventional forces still remain irreplaceable, however, there is a need to rethink the organisational structure of combat units to enhance their fighting and winning capabilities.
- The main battlespace in the future will be contested in the minds characterised by innovative employment of technology and information warfare.
- Integrated Theatre Commands is need of the hour, however, it would have to be future battle ready to be more effective.

The Centre for Land Warfare Studies (CLAWS), New Delhi, is an independent Think Tank dealing with national security and conceptual aspects of land warfare, including conventional & sub-conventional conflict and terrorism. CLAWS conducts research that is futuristic in outlook and policy-oriented in approach.
Website: www.claws.in **Contact us:** landwarfare@gmail.com

Introduction

The last one decade has seen some landmark turning points which are indicative of rapid changes in the character of new generation wars. The experience of recent military conflicts confirm that technology has taken the centre stage to fight and win modern conflicts. Drones have emerged as a lethal weapon system. Conflict in Syria and Azerbaijan's resounding victory over Armenia have shown that drones have become an integral part to execute intelligence, surveillance, target acquisition, and reconnaissance (ISTAR) missions for ground support operations and destruction of enemy ground forces. Correspondingly, cyber war is emerging as a new weapon of non-contact war, thus there is an urgent need to develop cyber shield and cyber spear to prevent the crippling of economy and military assets.

Turning Points in Evolving Trends in Warfare

The following attacks are strong examples of new generation warfare:

- ***Cyber Attack in Estonia.*** The cyber attack of 2007 in Estonia crippled their banking services, supply chains, air and rail travel, as a result of which Estonia was thrown into an 'artificially created' chaos. Large number of other functions of the state that were dependent on computer network for delivery of effective governance were also disrupted. This was one of the biggest cyber attack that lasted for weeks, and ultimately leading to Estonia reviewing its cyber security mechanism. This was a classic case of non-contact warfare that created lawlessness on the streets and triggered looting, arson and scarcity of essential goods and services. The attack showed how easily a hostile state can exploit potential tensions within another society.[2] The cyber attacks were so sophisticated that it took months for Estonia to restore its cyber network. Estonia had two options— first, to develop their own capabilities and suffer short term losses and second, to ask assistance from the NATO or fall back to Russia to bring it out of the chaos. It however, chose to develop its own cyber shield and cyber spear to defend and punish those who attempt to attack them. Today, Estonia is a leading cyber power in the world. Liisa Past a Cyber defence expert at Estonia's state Information System Authority remarked, "Cyber aggression is very different to kinetic warfare. It allows you to create confusion, while staying well below the level of an armed attack".[3] Estonia from victim of cyber aggression transformed itself to be an E-Estonia that is now able to secure its cyber space from rogue state and non-state cyber warriors.

- ***Swarm Drone Attack on Russian Forces.*** The Swarm drone attack on the Russian forces in Syria (2018) was another turning point as to how future threats can manifest from proxies and non-state actors by using commercial drones to attack high value targets on the ground. Ten drones, rigged with explosive devices, descended over Russia's Khmeimim air base while a further three targeted the Russian Naval CSS point in the nearby city of Tartus.[4] The January 2018 drone attack is significant from the point of view that such drones are readily available in the market and can be misused by terrorists and rogue states. To keep anonymity, rogue states may use faceless organisations to avoid direct retaliation. This incident also highlighted that effective surveillance and air defence capabilities (electronic and kinetic) have the potential to neutralise such threats to a great extent.
- ***Aramco Drone Attack.*** The 'sophisticated' drone/ missile attack by Houthi rebels of Yemen on the Aramco oil refineries at Abqaiq and Khurais in Saudi Arabia is also indicative of the new generation warfare.. It was reported that the Houthi rebels were able to disrupt almost 50% of the oil export of Saudi Arabia with these twin attacks. It is a worrisome fact that few drones costing $15000 per piece could cripple 50% oil supply of Saudi Arabia. These drones were launched from Yemen almost 500 to 900 miles away from the target. These twin strikes exerted strategic restrain on Saudi Arabia as a result of which Saudi Arabia scaled down attacks on the Houthis in Yemen. The rebels were actually able to find gaps in the surveillance grid and manoeuvred the drones/missiles undetected. It is difficult to believe that non state actors can acquire such sophistication in Intelligence, Surveillance and Reconnaissance (ISR). It also shows that use of such sophisticated systems is no more restricted to the states as even the non-state actors can now lay hands on such lethal systems. The attacks indicate that, the state's monopoly over violence can weaken at any point of time and proxy fighters in the grey zone can assume greater role in fighting asymmetric wars.
- ***Azerbaijan-Armenia Conflict.*** The most important emerging trend was seen during Azerbaijan-Armenia conflict that has proved that autonomous weapon systems are future tools of war fighting. The war losses due to drone attacks were so heavy that Armenia ultimately signed the peace treaty on Azerbaijan's terms. Azerbaijan used Turkish armed drones and Israeli loitering drones that crashed into the target.

thereby, inflicting unacceptable damages on the Armenian Ground Forces. As per Azerbaijan, Armenian forces lost 185 T-72 tanks; 90 armoured fighting vehicles; 182 artillery pieces; 73 multiple rocket launchers; 26 surface-to-air missile systems, 14 radars or jammers; one SU-25 war plane; four drones and 451 military vehicles.[5] It also highlighted the use of sophisticated *ISR* systems to detect electronic emissions, underground emplacements by using combination of surveillance and reconnaissance tools such as thermal imaging, terrain synchronisation and electronic emission detection.

The above turning points highlighted the fact that smart and bold usage of technology will dominate the future battle field. Today's technology offers potential for quick, decisive and (comparatively) clean victories over larger but more technologically-backward adversaries.[6] Considering the above trends, there is a risk in complacency, assuming that existing structures and experiences in warfighting is adequate to inflict defeat on the adversary. However, what needs to be kept in mind is that technological change is one aspect but training, revision of doctrine, change in leadership ethos and transformation of military structures is another aspect—sticking to outdated doctrines, technology and fatigued concept of warfighting is counter-productive and at best can be called 'backwardness in prudence'.

What India needs to Learn from New Generation Wars

India's concern is as to how we could defend against traditional adversaries, proxies and non-state actors who may be in the process of acquiring autonomous weapon systems including commercial drones that were used by Syrian rebels against Russia, Houthis against Saudi Arabia and Azerbaijan against Armenia. Cyber attack is another potential threat that may be carried out by proxies making it difficult for the intelligence agencies and cyber warriors in India to identify and respond to the source of attack.

Time has come to study the emerging threats and there is a need to suitably restructure the combat units of the Indian Army so as to prepare themselves to face future emerging challenges. Current organisational structures especially field formations, appear vulnerable to autonomous weapon systems and cyber threats. Therefore, there is a need to rethink and break out from the conventional war fighting methodology. Today mechanised columns, artillery units, command and control centres, logistic areas and even field defences are vulnerable to the drone attacks and loitering smart bombs. Though conventional forces still remain irreplaceable to capture, hold and deny ground to the adversaries, but there is a need to rethink the organisational structure of combat units to fight and win ground campaigns. Few suggestions to trigger the debate on the subject are as given below: -

- Integration of land-based fire-support and drones is becoming a necessity of modern warfare i.e. should an artillery regiment have three gun batteries or it should have two gun batteries and one squadron of armed and surveillance drones including kamikaze drones (also called loitering munitions, designed to hover in an area before diving on a target) for fire support operations. Surveillance drones will help artillery guns and drones to provide fire support to the troops in contact. Thus, artillery must now think ahead to incorporate drones as part of their armoury.
- Should armoured regiment have three squadrons of armour or it should have two squadrons of armour and one squadron of drones? Mechanised columns would require armed and surveillance drones to cover manoeuvre in the battlefield. Anti-drone systems, both ground and hovering, could be considered at the armoured brigade level. A Recce squadron at the armoured brigade level could be restructured to provide aerial surveillance and anti-drone cover. This will give armoured formations greater flexibility and ability to manoeuvre in the battlefield. Although the era of main battle tank is not yet over, however, the survival of tanks is dependent on taking on the incoming drone, anti-tank missiles and enemy ground forces. Therefore, tanks would be required to deal with ground and hovering drone threat. DRDO and even the defence industries need to look at viable systems that can be mounted on tanks or on tracked vehicles to ensure survival against ground and drone threats.
- There is no option but to reorganise Surveillance and Target Acquisition (SATA) and air defence regiments to ensure effective ISR over tactical battlefield areas to provide air defence against drone and air attacks. Drones are also emerging as good and potent system to suppress enemy air defence assets on the ground. Thus, the army air defence formations/ units will have to look at both defensive and offensive capabilities against drones.
- Hybrid warfare division is a necessity at each theatre command. Cyber, electronic and information warriors should be part of this division to fight day- to- day battle in order to ensure that the military capabilities are not disabled during peace and war. The creation of this division can no more be delayed or deferred since cyber and information war has become everyday war and there is no ceasefire in such wars. Till

integrated theatre commands are raised, these hybrid divisions could be part of nominated command headquarters of three services.[7]

- New generation wars have the potential to overthrow 'a stable and predictable' military balance by innovative doctrines and hybrid strategies.[8] Hence, the limiting factor is lack of operational experience of fighting innovative wars. It will also require visionary generals, ready to experiment and innovate war fighting strategies, such as General Valery Gerasimov of Russia, General Qasem Soleimani of Iran and General Yaşar Güler of Turkey.[9]
- Without adequate sensors, the electronic warfare cover, counter-drone weaponry, and traditional ground units, are in trouble.[10] Future army units should be equipped with composite systems to deal with electronic, air, drone, cyber and ground attacks.

Indian Army therefore, needs to realise that the actual battlespace is in the mind and future wars will be contestation of innovative ideas. As a result, new generation wars will be dominated by information and psychological warfare. The objective is to reduce the necessity for deploying hard military power to the minimum possible level.[11]

Way Ahead for India

Some of the suggested way aheads for India are as follows:

- ***Establishment of Integrated Theatre Commands***. Restructuring and transformation of armed forces is need of the hour to fight new generation wars. Establishment of Integrated Theatre Commands (ITC) is a good initiative, but the future battle ready nature of these Theatre Commands will make it more effective. Focus must be laid on conventional as well as new generation wars. Therefore, structures so designed must cater for contact and non-contact wars. Indigenisation of technology is a must since India cannot depend for long on foreign technology that could be compromised.
- ***Human Resource Development.*** Human resource development and technology adaptation is the key to fight future wars. There is a need to train, develop skill & aptitude of the officers and men to prepare themselves to fight grey zone conflicts, cyber wars and digitised wars as no matter how much technology is improved, ultimately there is going to be the human in the loop. Thus, we are looking at teaming up of men and machines or autonomous systems controlled and guided by humans.

- ***C3 Centres.*** Communication and command &control centres will be at great risk i.e. they will be always vulnerable to enemy drone strikes. Hence, there is a need to either provide digital camouflage or maintain airborne communication hubs to avoid targeting by drones.
- ***Securitisation of Cyber Space.*** The securitisation of cyber space is a necessity. It would require cyber intelligence, sharing of information, monitoring of cyber space and identification of possible exposed flanks that needs immediate attention to prevent attacks. The Computer Emergency Response Teams (CERTs) would play an important part and the CERT teams need to be ahead of inimical forces —both in technology and response actions. Integrated theatre commands would require to deploy such assets on land, sea and even in aerospace (manned and unmanned).
- ***Increased Cooperation.*** Increased cooperation and information sharing at both the technical and political level could also help to solve one of the most challenging issues in the cyber security realm i.e. the problem of attribution.[12] This would require proactive approach to build cooperation and shared response through defence diplomacy. Role of defence diplomacy is vital to build capabilities and capacities to respond to non-contact wars.

There is a need to put in place robust strategy of denial by technology, structural organisations and doctrine. Threat can be minimised by denial of exposed flank and minimising vulnerabilities. There is no panacea for dissuasion and deterrence but what is needed is continuous review of strategy, technology and doctrinal approach.

Conclusion

We are already in an era of “non-linear warfare” due to simultaneous deployment of multiple complimentary military and non-military strategies against the adversary. It is high time that the Indian Armed Forces carefully examines the new trends in war fighting. Technology is changing the contours of conflict and fatigued ideologies & traditional methods of war fighting are fast becoming obsolete. Today, ground forces are vulnerable and ineffective against loitering drones that are ready to strike troops, mechanised columns and artillery emplacements. A shield against autonomous weapon systems is an urgent requirement. Cyber and autonomous systems are available with the proxies and non-state actors, and can cause heavy damage to the economy and war waging capabilities. Therefore, it can be safely assumed that drones have now become an integral part of modern combined arms warfare.

End Notes

[1] Octavian Manea, “The Need to Compete on Multiple Battlegrounds: An Interview with Lt. Gen. H.R. McMaster”, *Small War Journal*, 17 November 2020. Accessible at https://smallwarsjournal.com/index.php/jrnl/art/need-compete-multiple-battlegrounds-interview-lt-gen-hr-mcmaster. Accessed on 16 Dec 2020.

[2] Damien McGuinness, “How a cyberattack transformed Estonia” , *BBC News*, 27 April 2017. Acceesible at https://www.bbc.com/news/39655415#:~:text=It%20is%20an%20event%20that%20still%20shapes%20the%20country%20today.&text=But%20in%20April%202007%20a,a%20cyber%20security%20hotshot%20today. Accessed on 16 Dec 2020.

[3] Ibid.

[4] David Reid, “A swarm of armed drones attacked a Russian military base in Syria”, *CNBC News*, 11 January 2018. Accessible at https://www.cnbc.com/2018/01/11/swarm-of-armed-diy-drones-attacks-russian-military-base-in-syria.html. Accessed on 16 Dec 2020.

[5] Robyn Dixon, “Azerbaijan’s drones owned the battlefield in Nagorno-Karabakh — and showed future of warfare”, *The Washington Post*, 12 November 2020. Accessible at https://www.washingtonpost.com/world/europe/nagorno-karabkah-drones-azerbaijan-aremenia/2020/11/11/441bcbd2-193d-11eb-8bda-814ca56e138b_story.html Accessed on 16 Dec 2020.

[6] Geraint Hughes,” Predicting future trends in warfare”, Defence Studies Department, King's College London, 21 February,2018. Accessible at https://defenceindepth.co/2018/02/21/predicting-future-trends-in-warfare/. Accessed on 17 Dec 2020.

[7] Narender Kumar, “Hybrid Warfare Division: An Urgent Operational Requirement for India”, *Journal of The United Service Institute of India (USI),* Vol. CL, No. 620, April-June 2020. Accessible at https://usiofindia.org/publication/usi-journal/hybrid-warfare-division-an-urgent-operational-requirement-for-india/. Accessed on 17 Dec 2020.

[8] N.6.

[9] Narender Kumar, “Visionary Generals – shaping modern warfare”, *Indian Defence Industries,* 17 Oct 2020. Accessible on https://indiandefenceindustries.in/visionary-generals-modern-warfare. Accessed on 17 Dec 2020.

[10] Can Kasapoglu, “Analysis - Five key military takeaways from Azerbaijani-Armenian war”, Anadolu Agency, 30 October 2020. Accessible at https://www.aa.com.tr/en/analysis/analysis-five-key-military-takeaways-from-azerbaijani-armenian-war/2024430. Accessed on 18 Dec 2020.

[11] Shahzada Rahim, “ New-generation warfare and the future of state security”, *The Jerusalem Post*, 03 September 2018. Accessible at https://www.jpost.com/opinion/new-generation-warfare-and-the-future-of-state-security-566421. Accessed on 18 Dec 2020.

[12] Alberto Muti and Katherine Tajer with Larry Macfaul, “Cyberspace: An Assessment of Current Threats, Real Consequences and Potential Solutions” *Network for Social Change Project by the Oxford Research Group*.,. Accessible at http://www.vertic.org/media/assets/Publications/CS1.pdf. Accessed on 18 Dec 2020.

The views expressed and suggestions made in the article are solely of the author in his personal capacity and do not have any official endorsement. Attributability of the contents lies purely with author.