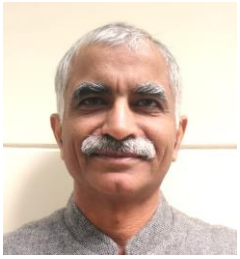
CENTRE FOR JOINT WARFARE STUDIES

CENJOWS

COUNTERING UNMANNED AERIAL SYSTEMS THREAT



Gp Capt Kishore Kumar Khera, VM (Retd) is an independent analyst. He has served as a fighter pilot in the Indian Air Force and was a Research Fellow at Manohar Parrikar Institute for Defence Studies and Analyses (MP-IDSA), New Delhi.

An attack by over two dozen unmanned aerial systems (UAS) on Abqaiq-Khurais refineries in September 2019,[i] assassination of Maj Gen Qasem Soleimani in an Unmanned Combat Aerial Vehicle (UCAV) attack in January this year[ii], the Indian Border Security Force (BSF) shooting down a Pakistani quadcopter carrying arms and ammunition in Indian air space in June [iii] and in the past one month, extensive use of unmanned aerial systems for attacking combat elements in the ongoing conflict between Armenia and Azerbaijan[iv] have showcased the changing battlespace scenario and application of unmanned aerial systems in the entire spectrum. In these four sperate applications of UAS, the entire current battle spectrum of hybrid warfare is captured and includes use by non-state actors, a state carrying out targeted killings, a state using these in propagating terrorism as a state policy and finally in a conventional conflict between opposing militaries. These events exemplify that the UAS has come a long way from its initial large-scale military application over three decades back and has created a niche place in the kinetic force application matrix. This transition is highlighted by the sole superpower, the US, that used a manned mission to kill Osama bin Laden in May 2011 in Pakistan, and a decade later, it resorted to an unmanned system to kill Iranian Maj Gen Qasem Soleimani in Iraq. These recent examples indicate the effective use of unmanned

aerial combat systems in different parts of the world by diverse players for varied objectives.

There are two prime reasons for such a rapid role expansion of UAS in kinetic force application or its support. First is the availability of such systems. With expanding use in the commercial arena from package delivery to filming, a number of UAS are based on Commercially of the Shelf Technology (COTS) and have a relatively low cost.[v] Add to this the negligible risk to the operator who could be at a safe distance from the scene of action. And based on the operating system, this distance could vary from a few kilometers to thousands of kilometers. The third aspect is the low vulnerability of the majority of small systems owing to their very small Radar Cross Section (RCS), thermal, visual and audio signature. These small signatures make UAS detection difficult and even more problematic to intercept. Additionally, the very high cost of modern air defence systems makes targeting UAS a very costly affair. Lastly, a majority of UAS can be mastered with a couple of days of hands-on training. This compresses the time between acquisition of a system and its operational deployment, an ideal facet for non-state actors.

The UAS have their inherent limitations also.[vi] A majority of UAS have low speed and very limited maneuverability. But the most crucial aspect is about their communication links with the base station that guides its operations. Normally, a UAS has multiple channels for communication. The channel for flight control is the most crucial and therefore invariably has inbuilt redundancy and large bandwidth. Communication regarding the operation of on-board sensors is limited and normally uses discrete inputs. The sensor output, in terms of video or data, is transmitted to the base station directly or via a satellite link and this can rarely be interfered with as that necessitates accurate knowledge of the receiver system and direct line of sight to it. The most vulnerable part of UAS communication set up is its satellite-based navigation system receiver. These generally operate in L band and can easily be saturated. Loss of location input makes the UAS lose their effectiveness.

The threat of an attack by a UAS has forced researchers to look for systems and techniques to counter it. Shooting down a UAS is an ideal solution but this requires a potent air defence system that can detect, track and intercept small RCS aerial vehicles. Use of surface to air missiles and air to air missiles against UAS has had limited success. Even when such interceptions have succeeded, the cost matrix still favours the UAS except

in a case of interception of a high-value high-end UAS. A classic case of this engagement was in June 2019 in the Strait of Hormuzwhere a US Navy Broad Area Maritime Surveillance (BAMS-D) RQ-4A Global Hawk High-Altitude, Long, Endurance (HALE) drone was shot down by Iranian surface-to-air missile system for violating the Iranian airspace near Kuhmobarak in the southern province of Hormozgan. This was a week after a US MQ-9 Reaper was shot over Yemen by a surface-to-air missile fired by the Houthi movement and Iran's failure to shoot another US MQ9 Reaper with a surface-to-air missile in the Persian Gulf area.[vii]

Small UAS that operate within the range of small arms fire can be targeted but it requires very high skill level to shoot a small target operating in three dimensions. With small arms, the Indian BSF has managed to down a number of small UAS trying to drop weapons and drugs from Pakistan into Indian territory. However, with UAS operating at a higher altitude, this system cannot produce desired results. In such a case, LASER or Electro-Magnetic Pulse (EMP)[viii]as a tool to target the UAS has also been explored as an option. But its limited range and high-power requirement limit its application in case of a multiple UAS attack. Practically, the most viable option to tackle a UAS threat is through electronic warfare to disrupt its navigation and communication systems. A high-power multiband transmitter that saturates UAS communication receivers can make the UAS redundant. In February 2020, Russia defended its Hmeymim airbase in Syria from a UAS swarm attack withits EW system Krasukha-4, a broad band multifunctional jamming station. Originally, Krakushka was designed to protect areas in and around Russia's military bases against airborne radars. However, it proved to be useful in counteracting armed drones as well. The truck-mounted radio emitter is capable of jamming radar signals and control channels for UAS with an estimated range of up to 300 km.[ix] A similar event was replicated last month with the same Russian electronic warfare system,also called Belladonna, operating from Russian military base at Gyumri in Armenia to knock out at least nine Turkish Bayraktar armed drones used by Azerbaijan to target Armenia.[x]However, the flip side of this methodology of using EW to counter UAS is that friendly or neutral missions in the range of the jammer will be equally affected. For example, a GPS jammer to disrupt a UAS can also disrupt the civil airlines' aircraft in its line of sight.

With gradual adaptation of Artificial Intelligence in UAS, their dependency on communication network will reduce. This will call for a fresh approach to neutralise AI dominated UAS and an AI operated counter UAS may be an

effective solution. The killer UAS needs to be of very small size and with low range but with high quality sensors and fast processing speed to converge on to the incoming UAS and hit it to disrupt its operation. Overall, a well-crafted plan is required to disrupt a UAS attack that combines and employs all possible methodologies based on the threat assessment.

In our context, all three wings of the armed forces operate UAS and more systems, imported and indigenous, armed and unarmed, are on the offing. With China as the manufacturing hub of UAS in the world, and Pakistan too manufacturing and operating multiple types of UAS, there is a real threat of UAS attacks. However, very little capability exists to effectively counter a drone swarm attack. A multi-pronged strategy needs to be in place to develop an effective counter to an UAS threat.

As exemplified by the Russian case, EW is the way forward in current context. As the threat exists, all three services are developing expertise in the EW domain along with other methods to develop a viable counter. An ideal solution will be to pool in EW resources of all three services to device and evolve a comprehensive system to counter a UAS threat. With resource availability under strain, the current approach of individual service developing service-specific solutions may prove to be sub-optimal. In any case, policy, strategy and operational plan for a ubiquitous Electronic Warfare needs to controlled and managed by a single entity for best results. And the integration can start with a counter UAS project.On the research and development front, the Indian Air Force attempt to tap the talented Indian youth by organizing an open contest in UAS category was a welcome step. But the nodal agency for such projects, DRDO, needs to support the military plan for EW and also provide more options from its talent pool by exploring LASER, EMP and AI operated Counter UAS. The research and development in this field needs to be given the required impetus.
Indian armed forces are gradually developing an integrated model for warfighting and the first Chief of Defence Staff set the ball rolling on January 1, 2020. However, the transition process is yet to take off for establishment of the Air Defence Command and integrated logistics at the station level.[xi] While that process is on, it will be prudent to initiate a parallel process for the integration of Electronic Warfare capability that will practically define the battlespace dynamics in the coming decade.

[i] David Reid, CNBC, September 20, 2019, available at https://www.cnbc.com/2019/09/20/oil-drone-attack-damage-revealed-at-saudi-aramco-facility.html(Accessed on November 1, 2020)
[ii]Who was Major General Qassem Soleimani, Iran's regional point man, The Indian Express, January 3, 2020, available athttps://indianexpress.com/article/explained/who-was-major-general-qassim-suleimani-6197535/ (Accessed on November 1, 2020)
[iii] Pakistan drone loaded with arms shot down by BSF along IB in J&K, The Times of India, June 20, 2020, available at https://timesofindia.indiatimes.com/india/bsf-shoots-down-drone-that-entered-jks-kathua-from-pakistan/articleshow/76476385.cms(Accessed on November 1, 2020)
[iv] Lt Gen HS Panag, High-tech drones could have neutralised Chinese intrusions at LAC but India didn't have them, The Print, October 29, 2020, available at https://theprint.in/opinion/high-tech-drones-could-have-neutralised-chinese-intrusions-at-lac-but-india-didnt-have-them/532979/(Accessed on November 1, 2020)
[v]Turkish Bayraktar used in the ongoing conflict between Armenia and Azerbaijan is a fairly conventional armed drone that is navigated to the target area using GPS. The drone's Wescam MX-15D multispectral camera system is made in Canada while its BRP-Rotax engine that generates about 100 horse-power is produced in Austria.
[vi] For more on comparison of UAS with a manned aircraft see Kishore Kumar Khera, Has the Time Come to Replace Manned Combat Aircraft With Armed Unmanned Aerial Vehicles? IDSA, New Delhi, August 16, 2017 available on https://idsa.in/idsacomments/replace-manned-combat-aircraft-with-armed-unmanned-aerial-vehicles_kkkhera_160817/(Accessed on November 2, 2020)
[vii]Strait of Hormuz: US confirms drone shot down by Iran, BBC News, June 20, 2019, available on https://www.bbc.com/news/world-middle-east-48700965(Accessed on November 1, 2020)
[viii] For more on EMP weapons see Atul Pant, EMP Weapons and the New Equation of War, IDSA, New Delhi, October 13, 2017 available at https://idsa.in/idsacomments/emp-weapons-new-equation-of-war_apant_131017/(Accessed on November 2, 2020)
[ix]Russian Electronic Warfare System Brings Down Hostile Drones in Syria, Defence World.Net February 3, 2020, available at https://www.defenseworld.net/news/26265/Russian_Electronic_Warfare_System_Brings_Down_Hostile_Drones_in_Syria(Accessed on November 1, 2020)
[x] Stephen Bryan, Russia knocking Turkish drones from Armenian skies, Asia times, October 26, 2020, available at https://asiatimes.com/2020/10/russia-knocking-turkish-drones-from-armenian-skies/(Accessed on November 1, 2020)
[xi]Govt working on setting up a new air defence command by October: Report, Business Standard, August 28, 2020, available at https://www.business-standard.com/article/defence/govt-working-on-setting-up-a-new-air-defence-command-by-october-report-120082800008_1.html(Accessed on November 1, 2020)