CENJOWS

ISSUE BRIEF

AUTONOMOUS DRONE THREAT AND COUNTER DRONE SYSTEMS FOR FUTURE

MAJ GAURAV KUMAR SINGH

CENTRE FOR JOINT WARFARE STUDIES

CENJOWS

AUTONOMOUS DRONE THREAT AND COUNTER DRONE SYSTEMS FOR FUTURE

Maj Gaurav Kumar Singh is an alumnus of National Defence Academy and a graduate of Defence Services Staff Course. He was awarded CDS Medal for Standing First in Critical Analytical and Innovative Thinking at DSSC.

"In the age of the almighty computers, drones are the perfect warriors. They kill without remorse, obey without kidding, and never reveal their masters."

- Eduardo Galeano

Abstract

The Indian Army promulgated its ***Policy Guidelines for Counter Drone Operations and Capability Development*** *in September 2022. This document delineates responsibility for counter drone operations, research and development (R&D) as also scaling of such systems to field formations. While the present generation of counter drone systems are designed to defeat drones based on employment lessons (both technological and operational) learnt from previous conflicts, it is imperative that the advancements in near future are catered ab-initio while countering the drone threat. This article analyses the autonomous drone development in Russia Ukraine War, its likely threat manifestation and prognosis of counter drone systems (both hard and soft kill). A salient comparison between hard and soft kill solution from operational perspective with focus on Indian R&D scenario is undertaken to avoid one size fits all solution.*

Operational Context – Autonomous Drones

The Russia Ukraine War is the first full scale conflict to witness widespread employment of drones by both sides. Russia has experimented with the Lancet and KUB kamikaze drones capable of operating autonomously while Ukraine is using US-designed Switchblade drones that are capable of identifying targets using algorithms. A slow integration of autonomous or AI-based technologies in drones has been observed, which is essentially just a software change to reduce human control.

The advent of autonomous drones is due to larger flying numbers which poses challenge of controlling numerous drones in flight, obstacle avoidance and precision targeting by these drones. Experts now caution that the proliferation of drones is driving militaries to hand over more and more control to artificial intelligence (AI), and ultimately moving toward systems that can operate on the battlefield without human involvement. This may entail an autonomous protection loop as it is less likely that humans can defend against autonomous drones without AI.

Autonomy in Drones

Before analysing the autonomy in drones, it is pertinent to understand two terms - AI and Automation that are often used interchangeably. Although both terms serve to operate smarter and more efficiently, yet, there remains few conceptual differences between the two terms. A common denominator for both AI and automation is data. While automated devices collate data, AI systems interpret it.

- **Automation -** Automation is about setting up devices to follow a set of pre-defined rules. The aim is to free humans from highly repetitive tasks that are tedious and error-prone. Automation supports human operators and frees up time for other types of tasks that require critical and creative thinking.

- **Artificial Intelligence (AI) -** AI is about setting up devices to make their own decisions (through human based input). AI is designed to mimic humans at an intellectual level, and perform tasks learnt by observing patterns and past results.

The so-called "autonomous" operation of a drone would mean that the system is able to modify its operating framework or its objectives (both initially defined by its algorithm and its designer) without human intervention.[1]

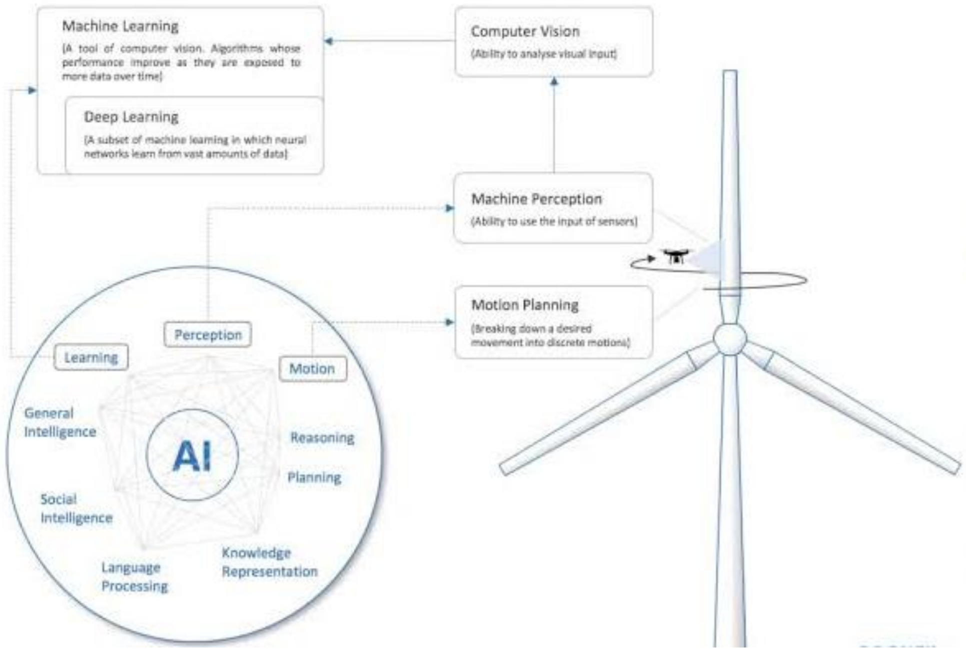

Figure 1 - Drones and AI (Source : https://droneii.com/wp-content/uploads/2018/08/Drones-and-AI-1024×768-1)

Autonomous Drone Technology

The so-called intelligent functions associated with drones are most often located on the ground. The drone sends data streams (usually images) that will be processed by algorithms and human operators on the ground. The information will then be verified, cross-referenced and analyzed by human decision-makers in order to establish the opportunity for concrete action on the ground. Thus, the information transits from the drone to the chain of command to determine an action to take. This action then goes back down to an operator and perhaps this same drone if it has the necessary effectors for the action. An order will be sent (or not) by the decision maker who will give his green light to the operator who will trigger the action through the drone. Once again, the human being keeps full control over the actions and movements of the drone, even if he delegates part of the execution of the actions to automated systems.[2]

Autonomous drones utilise a high-performance onboard image processing and a drone neural network for object detection, classification, and tracking during flight. The drone captures the data using the camera and sensors, which is analysed to extract useful information for a specific purpose. This process enables automatic extraction, analysis and understanding of meaningful information through one or more images processed through computer vision technology.[3] It can further use deep machine learning for self navigation, object detection, object tracking, obstacle detection and collision avoidances. For such tasks, the drone needs to be trained with variety of data sets and accurate data annotation to train the AI enabled autonomous flying.

Autonomous Drones in Russia Ukraine War

Ukraine is already using US-designed Switchblade drones—small, flying explosives that loiter over a vehicle before dropping on it—that are capable of identifying targets using algorithms. Russia has also been experimenting with autonomous weapons systems, according to Samuel Bendett, a Russia analyst at the Center for Naval Analyses, a think tank. Promotional materials for the Lancet and KUB kamikaze drones released by their manufacturer, Kalashnikov, suggests they are capable of operating autonomously.[4]

As the number of AI enabled drones increases, loitering munitions have emerged as the most suitable means to achieve cost effective results in battlefield. Israel has been exporting its radar killer Harpy, which can loiter over air defence radar for up to nine hours waiting for them to switch on and then crash to destroy the radar. Other such examples include Chinese Blowfish-3 and Iranian Shaheed-136. Shaheed-136 has proved to be game changer for Russia since it first appeared against Ukraine in September 2022.

Compared with initial phases of Russia's air war, the composition of Russian missile attacks has trended away from high-end missile systems like cruise missiles toward cheaper, less capable "low-end" systems like Shahed-136 one-way attack munitions (see below). In the first three months of 2023, during the tail end of Russia's strike campaign against Ukraine's electric grid, Shahed-136s accounted for around 40 percent of long-range projectiles fired at Ukraine. Since April, 61 percent of long-range munitions Russia has employed have been Shahed-136 one-way attack munitions. Compared to cruise and ballistic missiles, Shahed-136 are generally easier to shoot down and more vulnerable to cheaper defenses like the German-made Flakpanzer Gepard and other gun-based systems. The Shahed-136's warhead weight is also only between that of a cruise missile like Kh-101, and therefore causes less damage when they do make it through defenses.[5]

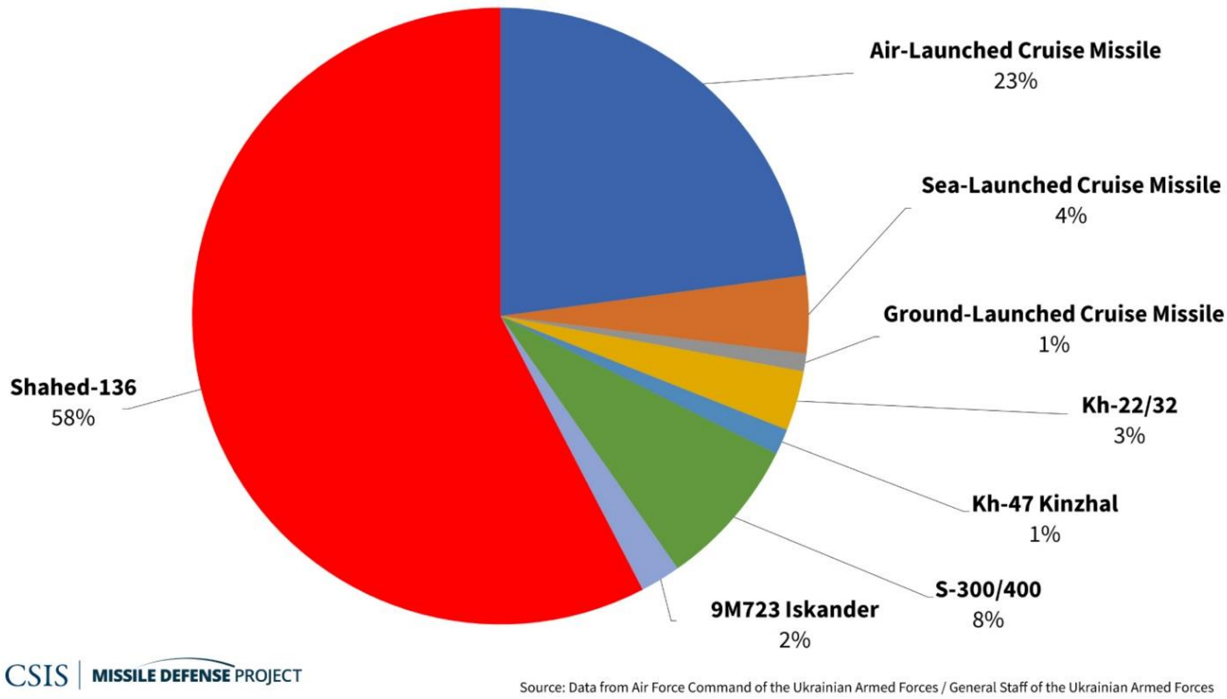

Figure 2 - Composition of Russian Kinetic Attacks on Ukraine (1 April to 22 June 2023) [6]

An analysis of Russia Ukraine Conflict indicates that the present generation of loitering munitions/ kamikaze drones have a high degree of autonomous operation and may also be incorporating AI for purpose of analysis. However, other than selected use of Artificial Intelligence Visual Identification (AIVI) technology in few drones no evidences of completely AI enabled drones were found. It can thus be safely assumed that the present generation of drones are in partial or conditional automation stage which will gradually enhance towards complete automation in future.

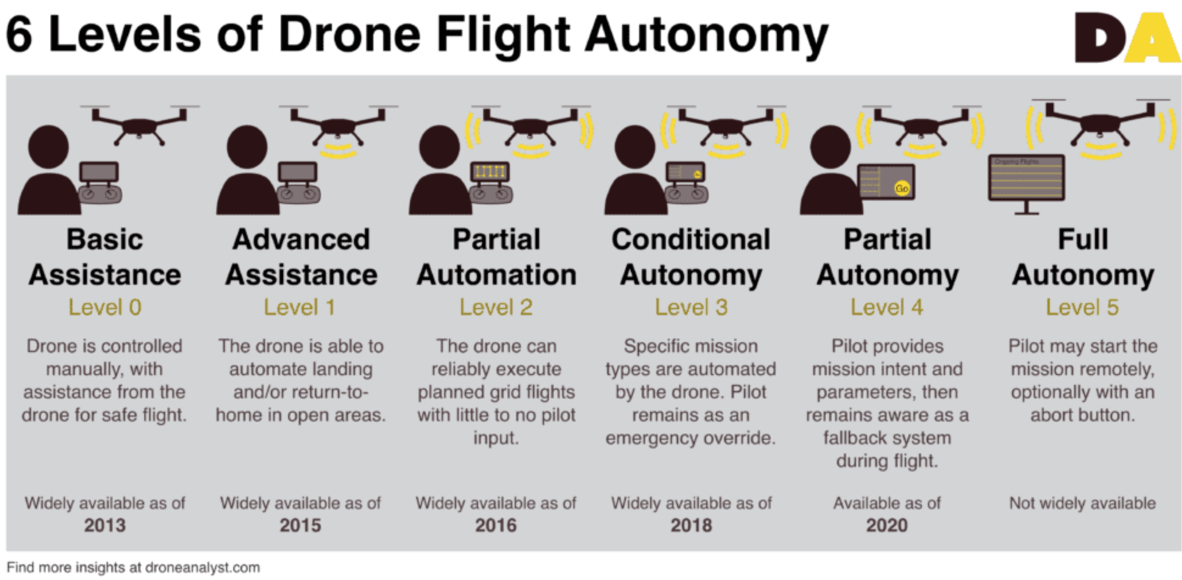

Figure 3 - Six Levels of Drone Flight Autonomy [7]

Threat Manifestation – Autonomous Drones

Autonomous drones are suitably poised to occupy significant airspace as compared to manned air missions due to cost effectiveness, versatility, endurance and human life factor. Manned air missions will in future be used mainly to control drone swarms or to augment the efficiency of unmanned autonomous missions in scenarios where survivability chances are high.

Increase of autonomy in drones has made it a weapon of choice in modern warfare. Its employment is gradually occupying the vacant space in kinetic battlespace which is not covered by rockets, missiles or aircrafts due to factors like cost to effect ratio, cost of human lives and deniability. In such threat scenarios, autonomous and AI enabled drones present different employability options based on its capability and suitability of mission. These can be utilised in battlefield based on dividends accrued from its employment.

- **Tactical Battle Area (TBA)** - In TBA, mobile strike and static holding forces with supporting eco-system are likely targets for drones. These targets vary in inter-se targeting priority based on phase of operations and own objectives. Thus, selections of targets is based on specific effect desired at the target end. To cater for such specificity, autonomous drones are better suited for employment wherein human based control ensures that the designated target is neutralised before triggering a force based event in the battlefield. AI-enabled drones may also be used in TBA, albeit in limited manner, to cater for tasks which autonomous drones may fail to achieve due to its counter like GPS and communication jammers/ spoofers employed by adversary.

- **Areas in Depth** - AI enabled drones are better suited to engage targets in depth which are of strategic importance and static nature. Longer flight distances requires self navigation, obstacle detection and collision avoidance till arrival at the target. AI is better suited to undertake such task while ensuring precision at the target end without fatigue and plausible deniability for desired destruction.

- **Swarm Threat** - Swarm threat will saturate the present vintage of counter drone measures and cause significant attrition to conventional defence. These are likely to be used in various stages of battle to achieve suppression/ destruction of enemy air defence whenever other manned/ unmanned platform will fail to do so.

Threat Mitigation Solutions for Autonomous Drones

Russia Ukraine War showcased that during the initial phase, hard kill or kinetic options impose high cost penalty when employed against drones thereby leading to non kinetic or soft kill options gaining currency. However, having learned its lessons on effectiveness of soft kill options on drones, in subsequent phases of the war, new generation drones were relatively more autonomous (with AI) to reduce dependency on communication from control centers and navigation from satellites using GPS. Some trends observed during the Russia Ukraine war are :-

- **Electronic Hardening of Drones** - A trend in electronic hardening of drones was noticed as seen in Shahed-136 which has an alternate navigation sys wherein its external antennas acts as receivers for LORAN navigation signals. LORAN is less accurate than GPS, but relies on ground-based transmitters which are more difficult to jam.

- **Higher Autonomy in Drones** - Initial phase of Russia Ukraine War demonstrated vulnerability of drones due to navigation signal from satellites. Thus, a higher degree of autonomy was added to the drones thereby rendering them more difficult to knock out of the sky due to far less reliance on communication link for navigation, thus insulating them, to an extent, against electronic warfare threats. The push towards autonomy served as a direct attempt to evade the Electronic Warfare threat thereby forcing higher reliance towards hard kill or kinetic solution to counter this evolution in drone warfare.

- **Cost Effective Target of Drones** - The old-fashioned radar-laid guns like the German Gepard are now being supplied to Ukraine to provide effective defence against drones along with shoulder-launched missiles like Stinger to render the more cost effective. This also reduces the chances of electronic fratricide of own drones in flight.

- **Directed Energy Weapons -** Many countries have increased pace of research in Laser and High Powe Microwave (HPM). India is also testing its KALI and DURGA systems to mitigate the drone threat.

<u>Counter Drone System – Drone Threat Mitigation</u>

- **Hard Kill Prominence in TBA** - The change in philosophy to counter drones can be witnessed from the development in drones during the Russia Ukraine War. It can be easily surmised that with the electronic hardening, lesser reliance on communications and navigation signals by drones as also chances of electronic fratricide, the likelihood of employment of soft kill measures (less laser and HPM) against drones will reduce in future.

- **Guns as Cost- Effective Counter Drone Solution** - Unfavourable cost effectiveness of engagement of drones by SAMs is likely to make guns duly integrated with advanced radars capable of detecting low Radar Cross Section (RCS) targets as the most prudent system against drones.

- **Development of Advance Ammunition** - Major lesson from Russia Ukraine War is the need to develop low- cost option against drones. It is anticipated to spur development of lesser cost ammunitions/ missiles like 3P ammunition and micro missiles to neutralise the drone threat in future.

- **Lack of Aerial Counter Drone Solutions** - After the Armenia Azerbaijan Conflict, the counter drone solutions have primarily depended upon ground based EW/ Soft Kill or Hard Kill System. However, no means to counter drones from aerial vectors have emerged. It was only on 14 Mar 23, when a Russia Su-27 reportedly downed a US MQ-9 Reaper but apart from this no air to air engagement of drones has been witnessed.

<u>Qualitative Comparison - Hard & Soft Kill System</u>

Hard Kill System - The hard kill counter drone system include gun sys and SAMs. The advantages and disadvantages of these sys are: -

- **Advantages**
  - ✓ **Cost Effectiveness** - The hard kill system especially gun sys are cost effective while due to its relatively cheap ammunition. SAM system are not cost effective however, development of micro missiles provide cost effective options for their emp. SAMs can be cost effective while targeting sophisticated drones.

  - ✓ **Shoot to Kill Options** - The pelletised ammunition with fragmentation warhead provides high sure shot kill probability (SSKP). The proximity fuze feature further increases the effect at target end.

  - ✓

- **Disadvantages**

  - ✓ **Engagement Accuracy** - The hard kill sys rely on line of sight of firer and/ or tracking capability of radar. The tracking capability of radar is further dependent on size, range, flight altitude and other features of the target. Thus, the engagement accuracy reduces in Built Up Areas (BUAs) or whenever the above requirements are not met.

  - ✓ **Collateral Damage** - The hard kill sys is suitable for emp in TBA where settlements and assets are limited. However, in BUA these sys is likely to be relatively less effective due to chances of collateral damages.

<u>Soft Kill System</u> - The advantages and disadvantages of these sys are: -

- **Advantages**

- ✓ **Cost Effective as compared to SAMs -** The soft kill system is cost effective as compared to SAMs as these sys relies on RF to cause disruption.

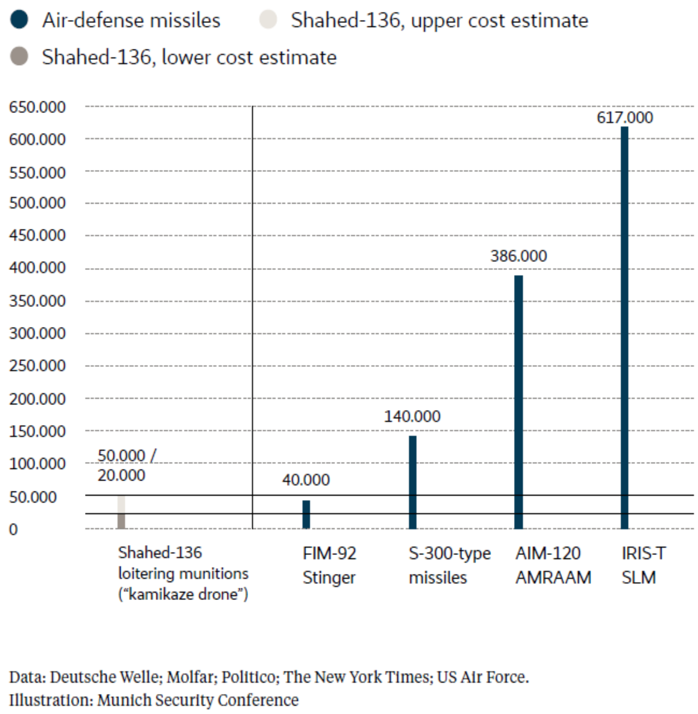

Figure 4 - Cost (in USD) per Unit of Shahed-136 and Selected Air Defence Missiles [8]

- ✓ **Employment in BUA -** These system cause disruption at the target end as compared to hard kill sys which cause destruction/ damage. Thus, in BUAs these are better suited as chances of collateral damage are minimal.

- **Disadvantages**

  - ✓ **Electronic Fratricide -** The soft kill system produces strong EM waves to cause disruption. However, as the range of these system increases from the source, the area covered at target end increases exponentially (πr^2 where at every 1000m 1º subtends 17 meter as diameter). Thus, at desired range of 5 km for any soft kill system large air space is rendered as No Fly Zone and thus chances of electronic fratricide increases substantially.

  - ✓ **Vulnerability -** Soft Kill Sys come in configuration of several vehicle mounted/ portable system (less RF guns). These sys function on transmission of energy to search, locate, analyse, record and subsequently jam or disrupt the target. The electronic transmission by these system makes them vulnerable to Anti- Radiation Missiles, loitering munitions Kamikaze Drones etc.

  - ✓ **Electronic Hardening -** Theses system rely primarily on the satellite (for navigation) and communication links (for control from distant Ground Control Stations) of the drones to carry out jamming/ spoofing so as to gain control or disrupt. However, with the increase in autonomy and inclusion of AI based features it is likely that future drones will have minimal or no reliance on satellite links and communication links thereby rendering soft kill system limited to low end drones.

Prognosis – Counter Drone System

Hard Kill System - These systems are likely to emerge as primary counter drone means in TBA where chances of electronic fratricide and collateral damage is limited. However, these sys due to their inherent dependence on radar sys for Beyond Visual Range engagement are likely to be vulnerable to c by ARMs/ loitering munitions, thus an integrated deployment of short range soft kill/ HPM/ DEW system is imperative to provide dedicated protection to assets in TBA. Also, Hard Kill system due to chances of collateral damage in BUAs are less suitable for deployment in hinterland.

Soft Kill System - Such system have an intrinsic spread of large area in air space as range increases which renders that airspace as No Go for own aircrafts. Any flight in this air space is likely to cause electronic fratricide in TBA. These sys are suitable for emp in BUAs and hinterland.

Analysis of Indian Counter Drone Scenario

- **Indigenous Counter Drone Development -** The Indian counter drone development has largely focused on development of capability to detect commercial drones at a distance of 3-5 km. The development curve in mitigation means is also inadequate due to primary reliance on soft kill especially RF guns which have limited ranges.

- **Hard Kill –Primary UAS Engagement Method** - Russia Ukraine War has demonstrated that present gun sys are both cost effective and assured means to mitigate drone threat. Thus major R&D push in this sphere is desired.

- **Focused R&D in Ammunition** - Development in field of ammunition would provide both desired lethality and accuracy to mitigate counter drone threat. Thus, indigenous development in this field needs necessary thrust to evolve into a cost effective solution.

Way Ahead/ Recommendations

- **Joint Counter Drone Operational Philosophy-** A Joint Philosophy at Armed Forces level is essential prepared to synergise efforts for identification of threats, listing out assets, evolving threat mitigation strategy and above all to prepare a road map for future procurement by incorporating best practices from sister services. This will streamline the overall procurement towards a common objective based on common employment philosophy.

- **Integrated Counter Drone System** - Globally integrated hard kill and soft kill options are being developed to optimize and give best cost-effective solutions for neutralising the drone threat. Thus, counter drone system based on EM spectrum (less laser & HPM) must be under single service and arm which may be declared the lead agency for developments and procurements.

- **C2 Architecture** - The C2 structure needs to be decentralised, flexible and encompass all services. The integration of sensors will provide timely early warning to enable prompt mitigation of the drone threat.

- **Electronic Emission Policy (EEP)** - Employment of soft kill counter drone system will involve EM transmissions which may be violate to existing EEP status. The existing policy may need review and clarity on activation of emitters, especially in TBA.

- **Countering Swarm Threat** - Swarms by sheer number will saturate air defence. A focused approach to mitigate this threat by development of HPM, DEW, High Intensity Laser, etc is desired.

- **Civil Military Fusion in R&D** - The R&D effort at national level must be channelised through military agencies to focus on specific system as listed:-

  - ✓ Development of vehicle mounted **HPM sys** against swarms at ranges of 2 to 10 km.

  - ✓ Development of high power **LASER** for drone threat up to 5 km.

  - ✓ Development of **power efficient and broad spectrum jammer** to counter both military and civil grade drones.

  - ✓ Development of **long range radars** to detect drones and stealth platforms at long ranges upto 20 to 50 km.

  - ✓ Development of **AI enabled smart sights** to enable acquisition, tracking & engagement of drones by small arms and vehicle mounted weapons.

Conclusion

In future warfare, positive identification of a state drone strike and swarm from terrorist drone strike will be difficult as states engage in deliberate grey zone operations for plausible deniability. Non state actors will cater for lapses in state supply by combining military hardware with commercially available drones. Such trend will make drone threat landscape increasingly complex, congested, ambiguous and volatile to counter.

The counter drone solution requires multiple parallel systems approach to cater for individual drawbacks and defeat drone threat. Simultaneously, interoperability between various counter drone systems and modularity in parts of the same system needs to be ensured to enable speedy evolution to mitigate ever evolving drone improvements. Emphasis on shortened R&D and reduced technology gestation period is essential to keep pace with technology enhancements in drone systems.

DISCLAIMER

The paper is author's individual scholastic articulation and does not necessarily reflect the views of CENJOWS. The author certifies that the article is original in content, unpublished and it has not been submitted for publication/ web upload elsewhere and that the facts and figures quoted are duly referenced, as needed and are believed to be correct.

Endnotes

1. Arnault Ioualalen, 'Autonomous military drones soon equipped with ai, reality or fiction?', 12 May 2021, https://www.linkedin.com/pulse/autonomous-military-drones-soon-equipped-ai-reality-arnault-ioualalen, accessed 14 July 2023
2. Ibid
3. Vikram Singh Bisen, 'How AI-Based Drone Works : Artificial Intelligence Drone Use Cases', 5 February 2020, https://medium.com/vsinghbisen/how-ai-based-drone-works-artificial-intelligence-drone-use-cases-7f3d44b8abe3, accessed 14 July 2023
4. Morgan Meaker, 'Ukraine's War Brings Autonomous Weapons to the Front Lines', 24 February 2023, https://www.wired.com/story/ukraine-war-autonomous-weapons-frontlines, accessed 12 July 2023
5. Ian Williams, 'Russia Isn't Going to Run Out of Missiles', 28 June 2023, https://www.csis.org/analysis/russia-isnt-going-run-out-missiles, accessed 12 July 2023
6. Ibid
7. David Benowitz. 'As Talk of Automated Drones Increase, We Separate Fact from Fiction', 21 October 2020, https://droneanalyst.com/2020/10/21/breaking-down-the-drone-autonomy-hype, accessed 14 July 2023
8. Report of Munich Security Conference 'Defense Sitters — Transforming European Militaries in Times of War', 01 June 2023, https://securityconference.org, accessed 12 July 2023