Counter-Unmanned Aircraft Systems (C-UAS)
Future of Warfare

Apratim Sharma[*]

The history of war is replete with instances where a nation that has effectively, and innovatively harnessed technology has been victorious. From innovations stem revolutions in military warfare, and the current world order is witnessing a very profound and rapid revolution through the employment of Unmanned Aircraft Systems (UAS), be it in conventional conflicts such as Nagorno–Karabakh (Azerbaijan–Armenia), the current Russia–Ukraine conflict or the unconventional 'Global War on Terror' in Afghanistan. The innovative and teamed employment of UAS has been the defining factor in modern conflicts. Thus, it is imperative for modern forces to possess counter-UAS capability, which shall redefine the future of warfare.

This article discusses the future roles of UAS, analyses its tactical, operational and strategic impact, assesses its vulnerabilities and having ascertained the need for counter-UAS (C-UAS) capabilities in future wars, suggests a C-UAS philosophy, methodology, kill chain and plausible approach in the Indian context.

Keywords: *Counter-UAS, C-UAS, Unmanned Aircraft Systems, Unmanned Aerial Warfare*

The last decade of the 21st century has witnessed a dramatic transformation in warfare, commonly termed 'Drone Warfare', wherein 'Armed Unmanned Aerial Platforms' have emerged as the next generation threat to combat forces in conventional as well as non-conventional domains.[1]

[*] Col Apratim Sharma is a serving Indian Army Officer and is presently posted with the Faculty of Studies at Army War College, Mhow.

ISSN 0976-1004 print
© 2022 Manohar Parrikar Institute for Defence Studies and Analyses
Journal of Defence Studies, Vol. 16, No. 4, October–December 2022, pp. 221–241

This increased optionality is particularly impactful in 'Hybrid' and 'Grey Zone' conflicts—the ambiguous interactions short of full-scale war that are typical in today's security environment.[2] This contemporary and technologically challenging threat has found easy access to many nation-states, non-state armed actors (NSAA) and terrorist organisations due to its cost-effectiveness, ease of operations and low-risk high visibility advantage. Already, more than 102 countries and non-state actors operate drones.[3]

The Nagorno–Karabakh and Russia–Ukraine conflicts have perhaps become the best examples of how small and comparatively inexpensive UAS can change the dimensions of conflict, once dominated by ground battles and traditional air power. Unmanned Aerial Warfare/UAS may have taken sophisticated Air Defence (AD) Systems by surprise and highlighted their operational limits but in this technology-driven 'Cat-and-Mouse game', AD Systems will have to evolve to adopt C-UAS platforms. As it is, low cost, rapid technology proliferation, capability to choose targets of choice, vulnerability of forces and critical assets (due to high cost and rapid technological advancement) will make C-UAS a ubiquitous choice in all future military operations. In the Indian context, there exists a reckonable UAS threat to Indian Armed Forces as our adversaries have witnessed an exponential rise in their armed UAS capabilities either through indigenous innovation or by friendly ties/covertness such as the procurement of the combat-proven Bayraktar TB2, which has extensively proven its might in the Russia–Ukraine conflict.

C-UAS capabilities include offensive and defensive security measures and processes meant to mitigate the risk of hostile UAS actions on own mobile, semi-static and static military assets.

Historical Perspective: Unmanned Aerial Warfare

In general, systems employing unmanned/pilotless technology are being called drones, Remotely Piloted Vehicles (RPVs), Unmanned Aerial Vehicles (UAVs), Unmanned Combat Aerial Vehicles (UCAVs), Unmanned Aircraft (UA), Unmanned Aircraft Systems (UAS) and small Unmanned Aircraft Systems (sUAS). Of all these, drones continue to be the favourite, garnering maximum attention. Technically, a 'drone' refers to any vehicle that can travel on its own in water, land or air.[4] Most of the military literature however use terms such as RPA, UAV, UCAV, etc., which reflect the way the technology has matured.

At present, the internationally accepted term in military operations is Unmanned Aircraft Systems (UAS), as promulgated by the US Federal Aviation Administration (FAA) in the 2000s. The term UAS includes everything that makes an unmanned aircraft work, such as its GPS module, ground control module, transmission systems, camera, all software and the person on the ground controlling it. In simple terms, an unmanned aircraft is a component of a UAS. The Indian government adopted UAS on 12 March 2021, as published vide official Gazette 'Unmanned Aircraft System Rules, 2021'.[5]

Genesis: Unmanned Operations

The use of explosive-filled balloons during the siege of Venice in 1849 is considered as the first of unmanned operations. These balloons were launched from an Austrian ship anchored near Venice. The wind was supposed to carry the balloons, which would be triggered by electromagnetism through a long copper wire.[6] In World War I (1918), Charles Kettering developed a gyroscope-controlled flying machine that fell and exploded after its propeller turned a pre-set number of times. In 1930s, pilotless aircraft started getting employed as aerial targets such as the 'DH 82B Queen Bee' employed by the Royal British Navy. US Admiral William H. Standley introduced the term 'Drone', correlating the behaviour of a 'Male Bee', which was identified as idler, could not function on its own and had a peculiar monotonous buzzing sound. During the 1930s, the term specifically referred to radio-controlled aerial targets. Once World War II broke out, it started to represent all remotely controlled pilotless aerial vehicles.[7]

During the Vietnam War (1960s), UAVs were employed for stealth surveillance, however technological progress (electronics, computers, miniaturisation) and change of human mindset brought about the combat adaptation of UAVs, which used precision weapons in real-time for destroying 'Time Sensitive Targets'.[8] These were called Uninhabited Combat Aerial Vehicles (UCAVs). During the Yom Kippur War (1973), Israel lofted drones to draw Egyptian fire, then sent manned planes to destroy the identified Egyptian missile batteries. Israel also used them during the Lebanon War, in 1982, to scout for targets; it sold its Pioneer Drone to the US for aerial surveillance during the 1991–92 Persian Gulf War.[9] It was one of Israel's leading drone designers, Abraham Karem, who designed the Predator Drone after he emigrated to the United States.[10]

UAS Operations

UAS comprises a number of sub-systems, usually the same elements as in manned aircraft but without a pilot. The aircrew is replaced with an electronic intelligence and control sub-system. Other elements such as launch, landing, recovery, communication, support, etc., are the same in both manned and unmanned systems.

UAS: Threat and Risk Conundrum

A study of hostile UAS (2016) by the Remote Control Project, Oxford Research Group[11] defines threat as:

$$\text{Threat} = \text{Capability} \times \text{Intent}$$
$$\text{Risk} = \text{Likelihood (Threat} + \text{Vulnerability)} \times \text{Impact}$$

A threat is an actor possessing both capability and intent to attack. A risk is a function of a threat, a vulnerability, the likelihood of the threat attacking the vulnerability, and the potential impact of the attack. This definition signifies that threat from unmanned operations have risen exponentially and there are huge risks if this threat is not countered effectively. The current Russia–Ukraine conflict exemplifies this equation the best when Ukraine acquired UAS capability with an intent to thwart another misadventure by Russia, as in 2014. And, when the Russian vulnerabilities were exploited, the impact was detrimental for Russian AD and Air Force.

Over the last decade, US, China, Russia, Turkey and even Iran have considerably advanced the development of UAS and possess a huge inventory and range of UAS. UAS threat manifestation and its impact can be deduced from the quote by the United States Secretary of the Navy Ray Mabus, which reads: "F-35 Joint Strike Fighter will likely be the last manned strike fighter aircraft, the Department will ever buy or fly, and that autonomous unmanned vehicles will be the new normal in ever-increasing areas". A unique challenge in countering UAS is the wide number of ways it can be employed and the different conditions faced in each potential scenario. A UAS threat is the strongest multi-domain battlefield weapon of present time.

Future Roles/Exploitation

Next-generation UAS will execute complex roles as under:

- Autonomy: Automatic Target Detection, Recognition and Destruction

- Electronic Attack
- Nuclear Payload Delivery
- Aerial Delivery/Resupply of Ammunition and Medicines
- Combat Search and Rescue
- Refuelling: Large UAS could eventually take on the aerial refuelling
- Offensive and Defensive Counter Air
- Swarms in WMD Role: Swarms consist of multiple unmanned platforms and/or weapons deployed to accomplish a shared objective, with the platforms and/or weapons autonomously altering their behaviour based on communication with one another. These swarms could be highly effective as mass casualty weapons, especially against soft targets. Swarms of sUAS can be successfully used to distract, disorient and disrupt military operations.

Threat Matrix

A UAS threat is likely to manifest in three military domains:

- *Strategic*: Threat manifestation in this domain is still distant and requires extreme technological skill. The objective though shall be to strategically disrupt the enemy forces and impact their cognitive domain to disrupt application of forces. This domain will be primarily dominated by sophisticated UAS using communication links from satellites. However, a possible leverage of disruptive technology, namely robotics, expert systems, artificial and collective (cloud-like based) intelligence, network communications, IoT, etc., in future may manifest this future-projected threat into reality. Use of UAS in this domain will primarily be carried out by state actors.
- *Operational*: Threat manifestation in this domain is primarily by human-controlled and semi-autonomous UAS. This domain will mainly be dominated by sophisticated UAS using communication links from relay communication links or satellites, and primarily be carried out by state actors. Non-state actors would take some more years to acquire such technology, it being a niche technology and most nations still trying to acquire them as well as the cost factor.
- *Tactical*: UAS employment in this domain is an imminent threat and has to be addressed at priority. This threat may manifest from sUAS/improvised hobby drones as swarms, exploiting weaponised devices against service personnel, specialised equipment, ammunition dumps, attack on senior leadership, etc., by NSAA and terrorists.

Threat to Combat Forces

Unmanned platforms have the capability to collect detailed intelligence or pose a kinetic threat to critical assets by state/NSAA/terrorists. The following Vulnerable Areas (VA) or Vulnerable Points (VP) are directly threatened by UAS/sUAS/drones:

- ***Offensive and Defensive Ops***: Near real-time intelligence improves target location accuracy, counter fire response time and fire mission lethality, thus enhancing the threat to field forces. Russia destroyed four Ukrainian army brigades preparing to conduct a cross-border attack in July 2014 through UAS surveillance.
- ***Threat from NSAA***: Strong offensive and defensive air power has always been with nations having robust financial might and technological superiority. Easy availability, proliferation and local innovation of UAS by NSAA have changed that equation in the last decade. A range of non-state groups, including ISIS, Hezbollah, Hamas, the Kurdistan Workers' Party, Jabhat al-Nusra, Donetsk People's Republic and Ansar-Allah (commonly known as the Houthi Movement) have demonstrated the capability to use sUAS/drones for a wide range of operations, including aerial strikes, surveillance and reconnaissance and propaganda. Currently, multiple groups are operating in Africa, Middle East, Arabian Peninsula, Southeast Asia, Eastern Europe and South America. Few instances for reference are:
    - *Hezbollah attacks*: Hezbollah for the first time ever employed a Mirsad-1 drone in November 2004 for reconnaissance and to carry explosives over Israel.
    - *Attacks by Al-Qaida*: Al-Qaida operatives in Pakistan built small attack drones, which were discovered by the police in 2013.
    - *Attacks by Islamic State*: In 2014, ISIS employed over 300 commercial off-the-shelf (COTS) and homemade drones during Iraq and Syria operations, with one-third being armed strike missions.
    - *Attack on Russian base*: In January 2018, 13 homemade drones attacked two Russian military bases in Syria.
    - *Attack by Houthis*: Houthis successfully guided artillery fire and missiles with their sUAS, hitting targets with a level of precision credited to regular armed forces only. In January 2019, a Houthi drone detonated 80 kgs of explosives at a Yemeni military parade, killing six soldiers. Eight months later, they used armed drones at

Aden Military Camp, killing 36. Later, a small swarm of attack drones damaged critical Saudi oil processing facilities in Abqaiq and Khurais.[12]

Lethal UAS Operations: The Kill Chain

The battle of UAS shall comprise integrated attack incorporating multiple threat capabilities in a well-coordinated and synchronised manner, such as a mix of armed UAS, cruise missiles, fighter aircraft and artillery in coordination with electronic and cyber attacks.

The 'Kill Chain' is a military concept which identifies the *structure of an attack* by the identification of target, dispatching of forces to target, initiation of attack on target and destruction of target.[13] In case of lethal UAS operations, it shall entail the following sequence to neutralise defensive capabilities and jeopardise critical assets employing 'Manned Unmanned Teaming':

- Launch Intense ISR Activities: To locate critical offensive and defensive assets and forces
- Force AD Sensors to Transmit
- Employ EW Assets Offensively. Turkey tested indigenous KORAL EW equipment in sync with Byaraktar TB2 UAS (Operation Springfield)
- Saturate AD Systems
- Attrition Battle
- Punch a Hole in AD Grid. Precision targeting of FC radars and the Command and Control Centre (C2) of a sophisticated AD System will render a void/gap in the overall AD cover, which can be easily exploited by the adversary as was amply demonstrated by the Israeli Air Force during the 1973 Yom Kippur War.
- Employ Mix Use of UAS and Fighter Aircraft
- Achieve Overall Air Dominance
- Engage Piecemeal and Create Psychological Havoc

UAS Vulnerability

AD Systems are meant to protect airspace and are thus designed taking manned aircraft into consideration. However, having assessed the modern threat of UAS to battlefield, it is critical to evaluate the vulnerabilities of UAS in order to counter them. The most significant vulnerabilities are:

- *Slow Moving Targets*: UAS have a unique design with high aspect ratio wings, affecting flight manoeuvrability and making them vulnerable to kinetic and non-kinetic targeting. For example, the average speed of Bayraktar TB2 is 60 m/s and 130 m/s for MQ1 Predator.

- *Susceptible to Weather Conditions*
- *Easy RF Visibility*: Modern AD radars capable of tracking artillery shells, with minor threshold modifications can easily detect UAS.
- *Reliance on Ground Control Station (GCS) and Communication Link*: The GCS uses separate bi-directional antennas to communicate with UAS and satellites. The GCS and communication links are prone to cyber and electronic attacks. Spurious signals can be used to disrupt geostationary communication satellites.
- *Dependency on Positioning Systems*: Most UAS use a dedicated positioning downward data link to determine its precise location, which can easily be jammed by a stronger power transmission in a similar frequency. During Operation Iraqi Freedom, Iraq employed Russian GPS jammers against coalition forces to disrupt coalition navigation and targeting.[14]
- *Vulnerable Mission Payloads*: Effective countermeasures can be executed against the payloads being carried by a UAS, that is, by blinding the on-board sensor/weapon by employing kinetic or non-kinetic means.
- *Vulnerable Control Elements*: The physical control element can be subjected to kinetic countermeasures while the non-physical can be subjected to electronic domain[15] countermeasures.
- *Dependency on Associated Infrastructures*: UAS operations depend on huge infrastructure with a large footprint, which can be easily targeted in the initial phases of operations.

UAS Countermeasures

One of the unique challenges in countering UAS (C-UAS) is its applications and the different conditions faced in each potential scenario. *The appropriate countermeasure differs in a peacetime versus combat scenario; even between that faced in a terrorist incident, insurgency and peer-on-peer warfare*.[16] For example, response to an UAS attack in peacetime shall primarily attract a non-kinetic response to avoid escalation, while in a conflict situation a kinetic response shall be prudent.

C-UAS Methodology[17]

There is no silver bullet for the UAS problem, hence there is no single comprehensive solution. The best approach is to employ a hierarchy of countermeasures that encompass regulatory, preventive and reactive countermeasures.

- ***Regulatory Countermeasures***: This requires a 'Whole of Government Approach' since multiple departments of government and law enforcement agencies are the stakeholders. These countermeasures can restrict the capabilities of COTS sUAS and limit their access to hostile groups and rogue individuals. These measures have no connotation on the hostile application of a UAS by an adversary. Some issues that merit attention as part of regulatory countermeasures against UAS exploitation by NSAA are as follows:
  - *Remote ID*: Mandatory remote IDs should be imposed on all COTS UAS to provide in-flight identification information to an electronic interrogation platform.
  - *Mandatory No-Fly Firmware*: UAS manufacturers should install India-specific firmware that includes the GPS coordinates of no-fly zones around sensitive fixed locations and limits carrying capacity and controller range.
  - *Harsh Penalties*: Civil aviation rules and licensing regimes to regulate the use of UAS with irrevocable harsh penalties such as blacklisting and cancellation of pilot license in case of violation impacting national security.
  - *Legal Framework*: Legal protection and authority to security forces to shoot down or jam suspicious UAS should be promulgated.
- ***Preventive Countermeasures***: The following countermeasures should be the first ones to be applied to avoid application of reactive countermeasures:
  - *Deterrence*: Deterrence is the best preventive action against UAS,[18] however, it requires own capability building in terms of effective C-UAS platforms and the will to take immediate punitive actions against an adversary UAS. Effective deterrence has the potential to minimise the use of UAS by an adversary and NSAA/terrorists.
  - *Suppression*: If deterrence doesn't ensue, the UAS should be interfered by using effective EW, interdiction and cyber-attacks. This should be done even against UAS ground installations and networks.

  - *Avoidance*: A UAS can only target once a human operator identifies the target and physically designates a weapon for destruction. Traditional measures such as camouflage, dispersion of troops may be sufficient to counter an electro-optical (EO) camera. Reportedly, the Taliban in Afghanistan mitigated their risk of detection by the US Predator and Reaper UAS by simply parking their trucks below trees and covering them with mattresses to suppress IR radiation from the hot engine.[19] Similarly, modern sensor technology was countered by Ukraine by fielding newer materials in the current Ukraine–Russia conflict.
- ***Reactive Countermeasures***: Reactive countermeasures come into play once preventive countermeasures fail to deter a determined adversary.
  - *Detection*: The C-UAS Kill Chain starts from early and farthest detection of a UAS. Varied sensors employing different technologies should be incorporated to detect the aerial threat and integrate it into the overall Control and Reporting (C&R) system.
  - *Decision-making*: UASs with small Radar Cross Section (RCS) and low speeds will invariably be detected at the last moment, thus a fully automated C&R system and speedy decision-making processes are mandatory.
  - *Neutralisation*: State-of-the-art technology, intensive and cost-effective C-UAS non-kinetic and kinetic means are required to neutralise the UAS threat.

C-UAS Kill Chain

A C-UAS platform is defined as a system capable of lawfully and safely disabling, disrupting or seizing control of a UAS.[20] C-UAS technology is primarily used for securing the airspace around critical VAs, VPs and HVTs. The C-UAS kill chain primarily involves the seamless use of C-UAS technology in three distinct phases (DT-ID-I Cycle):

- ***Detection and Tracking (DT) Phase***: A sensor system detects, locates, and tracks the incoming UAS threat in relation to the distance and direction from the VA/VP. Detection alerts the operator of unidentified objects based on system capabilities and configuration. The primary sensor (could be RF Detector) detects the presence and cues secondary sensors, such as cameras or electronic identification elements, which in coordination with the primary sensor confirm the precise location and IFF status.

- ***Identification and Decision (ID) Phase***: A probable threat must then be positively identified and classified prior to counteraction as the C-UAS operator will have a limited window to make the interdiction decision. Experience has demonstrated that the radar must be complemented with EO and electronic RF monitoring to acquire and confirm target identity.[21]
- ***Interdiction (I) Phase***: Depending on the technique used, this could result in a range of effects, including the UAS landing on the ground or activating the 'return to home' mode (in case of jamming or spoofing), capture or complete/partial destruction of the UAS (lasers, projectiles, impact drones, high-powered microwaves, etc.).

C-UAS Kill Chain: Execution

- ***'DT' Phase***:
  - Radar: Doppler radars function on the principal of differentiating the frequency shift of the return signal from the original transmitted frequency to acquire a target UAS. However, many radar systems generate false positives as well, degrading the capability to distinguish between a signal from a bird and a UAS, thus making the process complex and necessitating high sensitivity radar systems.
  - Passive RF Sensor: Passive RF sensors analyse the radio signatures and modulations specific to UAS signals.
  - EO/ IR Sensor: While EO identify and track UAS based on their visual signature, IR uses their heat signature. EO/IR cameras are an important sensor component of C-UAS platforms and on many occasions are the only way to confirm an actual UAS detection.
  - Acoustic Sensor: Acoustic sensors detect UAS by recognising the unique sounds produced by their motors. Acoustic systems rely on a library of sounds produced by known UAS, which are correlated with the target UAS to derive the identity.
- '***ID' Phase***: A ground-based C2 system with redundant and robust software can make or break C-UAS platforms. All the data from different sensors and technologies need to be collected, processed, synthesised and displayed in a user-friendly and actionable manner.

Identifying the threat and taking immediate decision is the main task of the C2 system.

- ***'I' Phase***: The interdiction phase involves the use of non-kinetic (non-physical means such as the use of electromagnetic spectrum, spurious signals, offensive cyber action, etc.) or kinetic effectors (physical means such as projectiles, missiles, nets, etc.). Both types of effectors can be used to achieve either Hard Kill (i.e. physical destruction of UAS/drone) or Soft Kill (disruption of UAS/drone). Non-kinetic means are not 100 per cent effective and have low technological shelf-life as future UAS/drone technology will easily outdate them, whereas kinetic effectors will always remain relevant. Ideally, on an integrated platform, there has to be a mix of non-kinetic and kinetic effectors to ensure 100 per cent neutralisation of unmanned aerial threat. This can be achieved by:
    - *Soft Kill*: This is achieved by using non-kinetic effector/techniques, thereby making a UAS operationally ineffective. A UAS can be hijacked, captured, forced to go out of control or return to base without fulfilling its mission by employing the following means
        - RF Jamming: It disrupts the RF link between the UAS and its operator by generating large volumes of RF interference. Once the RF link is severed, a UAS may either descend to the ground, return back or go rogue. The exact frequency to jam can be determined via RF detection. The advantages of this technology are medium cost and non-kinetic neutralisation. The disadvantages are short range, requirement of direct LOS, likely interference to friendly systems, jamming of other radio communications and the possibility of unpredictable behaviour of UAS.
        - RF Hijacking: It involves electronically taking over a UAS. This approach requires high skill and extensive knowledge of the data-link protocols of different types of UAS and an advanced software to break into secure 256-bit encryption.[22]
        - GPS Jamming: It involves disrupting the UAS satellite navigation link, such as GPS or GLONASS, by specialised jammers. For example, GPS jamming was used to thwart the OSCE Special Monitoring Mission to Ukraine in 2018.[23] However, this technique leads to collateral damage as a plethora of other military technologies in combat rely

upon the GPS/GNSS for precision, navigation and timing functions.

  - Spoofing: It involves feeding spurious communications or navigation links to take control of or misdirect a UAS. This can be difficult to implement especially if the data link is encrypted. It is, however, achievable with focused technological capability. In 2011, Iran successfully captured a completely intact highly sensitive American RQ-170 Sentinel stealth UAS[24] by using the spoofing technique.
- *Hard Kill*: This can be achieved by both non-kinetic and kinetic effectors.
  - High Energy Laser Effector: It involves destroying or burning critical components thereby leading to physical destruction. It is a cost-effective technology but has short range, and affects other radio communications. For example, Rheinmetall's High-Energy Laser Effectors range is 3,000 meters only. Also, UAS' surfaces can be modified to bounce the laser beam off the target, negating this effector's efficacy.
  - High Power Microwave (HPM) Effector: HPM is one of the best non-kinetic solutions. HPM effectors use high-intensity microwave energy to damage the internal electronics of a UAS within seconds. The advantages of this technology is that a UAS, if in range, can be effectively stopped and that it is very effective against swarms. However, it is expensive and risks unintentional disruption of own communications or destroying other electronic devices in the area. Also, as the UAS switches off and instantly falls uncontrolled, it may cause collateral damage.
  - Nets/Projectiles: Nets are designed to entangle the targeted UAS and to destroy or physically disable it by firing a net from an aerial platform.
  - Impact UAS: A UAS is guided to intentionally collide with the adversary UAS. A number of C-UAS systems can be employed in combinations of interdiction elements to increase the likelihood of a successful interdiction. For example, many jamming systems have both RF jamming and GPS/GLONASS jamming capabilities in the same package. A single integrated platform can have an electronic

system as the first line of defence and a kinetic system as a backup measure.

Approach to C-UAS: Indian Context

C-UAS Philosophy: Recommended Structure

- Follow Combined Arms Defence Concept.
- Incorporate highly adaptable and flexible autonomous C-UAS technology and processes to provide operational advantages over adversary's UAS capability.
- Adopt increasingly interoperable systems and platforms having modularity, which results in the evolution of effective, sustainable and efficient C-UAS systems that can adapt with the changing threat spectrum of UAS.
- Ensure seamless integration of C-UAS systems into operations across all domains and levels of warfare (strategic, operational and tactical) during conflict.
- Provide 24 × 7 C-UAS solutions during peacetime to all critical infrastructures against sUAS attacks by NSAA and terrorists.
- Encourage teaming across departments and agencies, academia and industry to drive innovation, technology and efficient use of research and development (R&D) investments to evolve indigenous C-UAS platforms.

C-UAS Strategy

Countering UAS threat will require synchronised, simultaneous and cohesive approaches at different levels as mentioned below:

- ***National Level***: A 'Whole of Government Approach' is essential to cope with the threat essentially pertaining to regulations, indigenous effort, innovation and Transfer of Technology (ToT). The imperatives will be:
  - Make comprehensive UAS guidelines and enforce strong and punitive regulations against illegal use of UAS.
  - Build strong relationships with C-UAS industry who comprehend the threats and technological requirements based on the 'Qualitative Requirements' to meet the highest security standards. Incentivise and facilitate the C-UAS industry to meet our requirements.

- ○ Explore ways and make it easier for MSMEs with novel approaches and technologies to collaborate in the development of new C-UAS platforms. Explore and encourage innovative endeavours for C-UAS solutions.
- ○ Organise C-UAS conclaves for better conception, ideation and sharing of vision and thus pursue technology as well as system development.
- ○ Fund science research and technology, push investments in emerging technologies that can benefit C-UAS endeavour.
- ○ Work with overseas partners and arrive at technology solutions through ToT.
- ○ Increase collaboration with international partners, DRDO, academia, industry, technical colleges and start-ups for C-UAS research and testing.

- ***Operational and Strategic Level***: Seamless integration of C-UAS assets in the operational and strategic domain will be a challenge and will require deliberate and protracted efforts. First, parameters need to be identified, based on which the framework for integration can be articulated.
- ***Tactical Level***: Evolve immediate and effective countermeasures against the sUAS threat in the tactical domain as priority. The forces should be trained on handling the sUAS threat by preventive and available reactive countermeasures till C-UAS technology is made available. Immediate procurement of low-cost EO/IR sensors should be done followed by non-kinetic effectors (both soft and hard kill) in Phase-1 and kinetic effectors (hard kill) in Phase-2.

C-UAS Developments: Review and Recommendations

Several nations have developed C-UAV systems and are in various stages of operationalisation and deployment. C-UAS capability of developing countries is highlighted with recommendation for procuring and pursue R&D along with international partners, DRDO, academia and industry.

- ***Israel***: Israel's 'Drone Dome System'[25] is a counter-UAV system that incorporates a laser weapon system.
- ***USA***:
  - ○ The US has developed a laser-based anti-drone system called the Advanced Test High Energy Asset (ATHENA)[26] with a range of approximately 5 kms.

  - *Marine AD Integrated System (MADIS)*:[27] MADIS is being employed by US Marines to meet evolving and future threats. It has two variants. The MADIS Mk1 includes a turret-launched Stinger missile, multi-functional EW capability, direct fire weapon, EO/IR sensor and a shoulder-fired Stinger missile for dismounted operations. The MADIS Mk2 (C-UAS variant) includes a multi-function EW capability, 360-degree radar, direct fire weapon, EO/IR optic and supporting C2 communications suite.
  - *DE M-SHORAD, Weapon System*:[28] Directed Energy Manoeuvre-Short Range AD Weapon System is a US Army programme to integrate a 50-kW class HEL weapon system on the Stryker A1 8x8 armoured vehicle. The integration of a 50 kW laser on a Stryker A1 is part of the MMHEL (Multi-Mission HEL) programme. The MMHEL is a technology integration and demonstration effort with a solid-state laser system, agile beam control system and supporting laser sub-systems integrated into a combat platform.
  - *Interim Manoeuvre Short-Range Air Defence (IM-SHORAD)*:[29] The IM-SHORAD system represents a major boost in firepower for Stryker vehicles, consisting primarily of a 360-degree Avenger AD turret loaded up with Stinger and AGM-114 Longbow Hellfire missiles, an XM914 30mm cannon and a 7.62mm machine gun.
- ***China***: It has recently developed an anti-drone system called the 'Silent Hunter',[30] which has a laser gun to engage low-flying UAVs.
- ***Russia***: Russia has recently come out with an improved version of their C-UAV system called Rex-2,[31] an anti-drone hand gun.
- ***Indigenous Context***:
  - *Anti-Drone System*:[32] DRDO has developed an Anti-Drone System, which was deployed for the Independence Day event at the Red Fort on 15 August 2020. The system is said to detect and jam micro drones up to 3 kms and use lasers to bring down a target up to 1–2.5 kms, depending on the wattage of the laser weapon.
  - *Drone Guard System*:[33] Bharat Electronics has developed a C-UAV system called Drone Guard System that has been configured to detect, track and neutralise intruding drones. The system utilises RF spectrum to detect a drone and a EO-IR sensor to track it

continuously and thereafter generate a RF jamming signal to neutralise the target. This system is capable of bringing down a drone by hampering its communication link as well as by blinding its GPS source. This portable and agile system can also be configured to be vehicle mounted as per requirement.

Way Forward: Enabling Forces

To counter the UAS threat and develop C-UAS capability, there is a need to prepare a comprehensive roadmap involving all stakeholders, including the government machinery, lawmakers, security forces, scientific community and industrial workforce in conjunction with citizen participation. A timed roll-on plan needs to be charted for the enablement of this novel yet pertinent domain. Exploitation of existing indigenous systems will allow us to identify the desired improvements alongside capability demonstration.

- ***Organisational Restructuring***: There is a need to reorganise AD setup, train and equip for C-UAS operations and integrate with defence forces and the police.
- ***Asset Allocation***: A UAS threat is omnidirectional, thus there is need to detect and interdict along the entire border, which is an expensive preposition. Apropos, a surveillance and engagement grid needs to be evolved to cater for high-threat areas initially, with options of sidestepping if the situation demands. Therefore, asset allocation should be based on a short warning period, in proximity to HVTs and in anticipation of faster pace of operations.
- ***Capability Development***: Presently, C-UAS technology is niche and unlikely to be shared by C-UAS enabled countries. Apropos, focussed R&D needs to be carried out indigenously as per 'Atmanirbhar Bharat Abhiyan', to enable our defence and civil industries to manufacture such equipment. This further needs to be supported by the government in terms of assured demand and material and monetary support, with targeted time periods.
    - *Short Term*: Based on recent experiences and developments, it should be endeavoured to procure detection-cum-interdiction systems that are tried and tested in modern-day battles (Ukraine, Syria, etc.) with ToT as part of the deal.
    - *Long-Term*: In addition to own R&D, based on technical know-how gained from the inductions, a focused development roadmap with high level of integration between the DRDO,

relevant civil industry and users should be kick-started. This will also improve our reliance on home-grown defence production and subsequently act as a driver for growth for exporting defence hardware to an extremely thirsty market.

Conclusion

Rapid proliferation and innovative use of sUAS by states, NSAA and terrorists pose a significant threat to frontline combat units. The forces are facing sUAS/drone threats but there is no effective C-UAS platform. However, in future, as demonstrated in recent conflicts such as Russia–Ukraine conflict, UAS will play a significant role and thus an effective C-UAS is the need of the hour.

Research efforts and incorporation of highly adaptable and flexible autonomous C-UAS technology and processes to provide significant operational advantages over adversaries is what future wars will characterise. Adoption of increasingly interoperable systems and platforms having open architecture standards and modularity which results in the evolution of effective, sustainable and efficient C-UAS systems that can adapt with the changing threat spectrum of UAS is desired. During conflict, there is a need to ensure seamless integration of C-UAS systems into operations across all domains and levels of warfare (strategic, operational and tactical) to deter and deny critical space and strategic advantage to the adversary, while at the same time ensure the same for own forces. An efficient C-UAS in the short-term and an indigenous product line in the long-term, under 'Atmanirbhar Bharat', is the way forward for ensuring peace by ensuing deterrence and in case of any misadventure, ensuring victory.

Notes

1. Andrea Bertolini, 'Artificial Intelligence and Civil Law; Liability Rules for Drones', European Parliament, 13 December 2018, available athttps://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2018)608848, accessed on 15 July 2022.
2. 'Game of Drones', Center for A New American Security Wargame Report, 2016, available at http://drones.cnas.org/wpcontent/uploads/ 2016 /06/ Game-of-Drones-Proliferated-Drones.pdf, accessed on 17 July 2022.
3. Dan Gettinger, *The Drone Databook,* Bard College: Center for the Study of the Drone, 25 September 2019, available at https://dronecenter.bard.edu/projects/drone-proliferation/databook/, accessed on 17 July 2022.

4. ‘What’s the Difference Between Drones, UAV, and UAS? Definitions and Terms’, Pilot Institute, 22 March 2020, available at https://pilotinstitute.com/drones-vs-uav-vs-uas/, accessed on 17 July 2022.
5. ‘Unmanned Aircraft System Rules, 2021’, *Digitalsky.dgca.gov.in*, available at https://digitalsky.dgca.gov.in/assets/files/UAS Rules, accessed on 20 July 2022.
6. Nikola Budanovic, ‘The Early Days of Drones – Unmanned Aircraft from WWI & WWII’, *Warhistory*, 12 May 2018, available at https://www.warhistoryonline.com/military-vehicle-news/short-history-dronesaircraft.html?chrome=1l, accessed on 20 July 2022.
7. Zoran Miličević and Zoran Bojković, ‘From the Early Days of 962 Unmanned Aerial Vehicles (UAVS) to their Integration into Wireless Networks’, *Military Technical Courier*, Vol. 69. No. 4, October 2021, pp. 941–62, available at https://www.researchgate.net/publication/355974188_From_the_early_days_of_962_unmanned_aerial_vehicles_UAVs_to_their_integration_into_wireless_networks, Vojnotehnicki Glasnik,.10.5937/vojtehg69-33571.
8. T. Gugała, ‘Unmanned Aircraft Vehicle, Unmanned Aircraft Systems: The Use Of Unmanned Aircraft Systems (UAS) in Combat Operations’, *Transport Problems*, Vol. 6, No. 4, 2011, available at http://transportproblems.polsl.pl/pl/Archiwum/2011/zeszyt4/2011t6z4_15.pdf, accessed on 20 July 2022.
9. Chamayou Gregoire, *A Theory of the Drone*, New York: The New Press, 2015, p. 27; Adam Rothstein, *Drone*, New Delhi: Bloomsbury Academic India, 2017, p. 31.
10. ‘The Dronefather’, *The Economist*, 1 December 2012, available at https://www.economist.com/technology-quarterly/2012/12/01/the-dronefather, accessed on 20 July 2022.
11. ‘Hostile Drones: The Hostile Use of Drones by Non-State Actors Against British Targets’, Remote Control Project, Oxford Research Group, January 2016, available at https://www.files.ethz.ch/isn/195685/Hostile%20use%20of%20drones%20report_open%20briefing_0.pdf, accessed on 20 July 2022.
12. Mohammed al-Kibis, ‘Houthi Drone Targets Senior Yemini Officers, Kills Five Soldiers’, *Al Jazeera*, 10 January 2019, available at https://www.aljazeera.com/news/2019/1/10/houthi-drone-targets-senior-yemeni-officers-kills-five-soldiers, accessed on 20 July 2022.
13. ‘Kill Chain Approach’, Chief of Naval Operations, 23 April 2013, available at http://cno.navylive.dodlive.mil/2013/04/23/kill-chain-approach-4/, accessed on 20 July 2022.
14. Tegg Westbrook, ‘The Global Positioning System and Military Jamming: The Geographies of Electronic Warfare’, *Journal of Strategic Security*, Vol.

12, No. 2, available at https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=1720&context=jss, accessed on 20 July 2022.

15. Karl Ginter, 'Space Technology and Network Centric Warfare: A Strategic Paradox', USAWC Strategy Research Project, available at https://apps. dtic.mil/sti/pdfs/ ADA469763.pdf, accessed on 20 July 2022.
16. Stephen W. Miller, 'Fighting Back Against UAS', *Asian Military Review*, 30 July 2020, available at https://www.asianmilitaryreview.com/2020/07/fighting-back-against-uas/, accessed on 30 July 2022.
17. Andre Haider, 'A Methodology for Countering Unmanned Aircraft Systems – Comprehensive Approach to Countering Unmanned Aircraft Systems', Joint Air Power Competence Centre, 21 January 2021, available at https://www.japcc.org/a-methodology-for-countering-unmanned-aircraft-systems/, accessed on 25 July 2022.
18. M. Mazarr, 'Perspective Understanding Deterrence', RAND Corporation, available at https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE295/ RAND_PE295.pdf, accessed on 25 July 2022.
19. Andre Haider, 'The Vulnerabilities of Unmanned Aircraft System Components', Joint Air Power Competence Centre, 18 December 2020, available at https://www.japcc.org/the-vulnerabilities-of-unmanned-aircraft-system-components/, accessed on 25 July 2022.
20. Jian Wang , Yongxin Liu and Houbing Song, 'Counter-Unmanned Aircraft System(s) (C-UAS): State of the Art, Challenges, and Future Trends', *IEEE Aerospace and Electronic Systems Magazine*, Vol. 36, No. 3, March 2021, pp. 4–29, available at https://doi.org/10.110/maes.2020.3015537, accessed on 29 July 2022.
21. *Countering Threats from Unmanned Aerial Systems (C-UAS) – IEEE,* available at https://www.gov.uk/government/publications/crowded-places-guidance/, accessed on 29 July 2022.
22. Tegg Westbrook, 'The Global Positioning System and Military Jamming: The Geographies of Electronic Warfare', no. 14.
23. Ibid.
24. Scott Peterson, 'Downed US Drone: How Iran Caught the "Beast"', *Christian Science Monitor*, 9 December 2011, available at https://www.csmonitor.com/World/Middle-East/2011/1209/Downed-US-drone-How-Iran-caught-the-beast, accessed on 29 July 2022.
25. 'Israeli Laser Defense System Successfully Intercepts Multiple Drone Targets', *The Times of Israel*, 12 January 2020, available at https://www.timesofisrael.com/israeli-laser-defense-system-successfully-intercepts-multiple-drone-targets/, accessed on 29 July 2022.

26. 'USAF Tests Lockheed Martin's Athena Laser Weapon System', *Global Defence Technology*, 11 November 2019, available at https://www.airforce-technology.com/news/usaf-lockheed-athena-laser-weapon/, accessed on 6 August 2022.
27. 'Marine Air Defense Integrated System (MADIS)', Missile Defense Advocacy Alliance, 8 July 2020, available at https://missiledefenseadvocacy.org/defense-systems/marine-air-defense-integrated-system-madis/, accessed on 6 August 2022.
28. 'DE M-SHORAD Guardian Stryker A1 50 kW-Class Laser Weapon', *armyrecognition.com*, 29 January 2022, available at https://www.armyrecognition.com/us_army_wheeled_and_armoured_vehicle_uk/de_m-shorad_guardian_stryker_50_kw-class_laser_weapon_data_fact_sheet.html, accessed on 06 August 2022.
29. 'M-SHORAD', Missile Defense Advocacy Alliance, available at https://missiledefenseadvocacy.org/defense-systems/m-shorad/, accessed on 6 August 2022.
30. 'Anti-Drone Laser System: Silent Hunter Laser Weapon', *China Military Drone Alliance*, available at https://www.militarydrones.org.cn/silent-uunter-anti-drone-laser-weapon-developed-p00193p1.html, accessed on 6 August 2022.
31. H. Hrachya, 'ZALA Aero REX-2 Anti-Drone Gun', *Daily News, Defense, Russia*, 27 June 2019, available at https://www.overtdefense.com/2019/06/27/zala-aero-rex-2-anti-drone-gun/, accessed on 6 August 2022.
32. 'Independence Day: DRDO's Anti-Drone System Was Part of PM Modi's Security at Red Fort', *The Economic Times*, 15 August 2020, available at https://economictimes.indiatimes.com/news/defence/independence-day-drdos-anti-drone-system-was-part-of-pm-modis-security-at-red-fort/drdos-anti-drone- system/slideshow/77558751.cms, accessed on 8 August 2022.
33. 'BEL's Drone Guard System on Display at DefExpo 2018', *Aviation & Defence Universe*, 12 April 2018, available at https://www.aviation-defence-universe.com/bels-drone-guard-system-on-display-at-defexpo-2018/, accessed on 8 August 2022.