AUGUST 2025

COUNTER-UNMANNED AERIAL SYSTEMS ARCHITECTURE

BRIG ANSHUMAN NARANG (RETD)

PRIMER

www.cenjows.in

CENTRE FOR JOINT WARFARE STUDIES

CENJOWS

PRIMER – COUNTER-UNMANNED AERIAL SYSTEMS ARCHITECTURE

Brigadier Anshuman Narang, Retired, is an alumnus of prestigious Rastriya Indian Military College. He holds the "Adani Defence Chair of Excellence" on UAS Warfare with Special Focus on Counter-UAS at CENJOWS.

Abstract

*The **Indian Prime Minister Modi's announcement on 15 August 2025 of India's indigenous "Sudarshan Chakra Mission'**, rivalling Israeli Iron Dome, for creating a defence wall against multi-domain threats **is the most needed defence capability enhancement in the next decade**. In a drones infested environment with tactical battle-space majorly dominated by Multi-Domain Unmanned Vehicles (MDUVs), Counter Unmanned Aerial Systems (C-UAS) architecture is the most essential component of the overall Rockets-Artillery-Air-Missiles-Drones (RAAMD) defensive shield "Sudarshan Chakra" to protect India's strategic, civilian and high value locations from attempted drone strikes by our adversaries and anti-national elements. The C-UAS kill chain primarily involves detection, identification, tracking and mitigation of all incoming drones, MDUVs and even swarms. With an ever-growing variety and continuous technological advancement in drones' domain, C-UAS solutions are*

already lagging behind and no single technique can provide a comprehensive anti-drone solution. Hence, the national multi-front C-UAS architecture requires multi-layered and multi-disciplinary detection systems spread across all levels, multi-tiered and multi-domain tracking and identification and most importantly a hybrid mix of soft-kill and hard-kill options to mitigate drones' threat without any collateral damage.

The easy accessibility of drones and its components has made the drones' threat ubiquitous internally and externally. Hence, the C-UAS concepts are applicable across the nation- central and state governments, military, border / coastal defence forces, para-military and police including CRPF and CAPF. This primer on "C-UAS" architecture has thus examined the current drones' threat, evolving drones and C-UAS technologies, tactical concepts, C-UAS structures, and then recommended the C-UAS conceptual contours, platforms and organisations for building a ***comprehensive C-UAS architecture as part of the national "Sudarshan Chakra Mission"****.*

Key Words

C-UAS, UVs, RAAMD, Kill-Chain, Unmanned Aerial Systems (UAS), Artificial Intelligence (AI), Electronic Warfare (EW), Radio Frequency (RF), Indigenisation

Basic Terminology. It's very important to simplify the key terms for a layman before progressing ahead with this primer as they have been used in this document.

- UV – Any vehicle in any domain which is unmanned.
- UAV – Any aerial vehicle which is unmanned. Also called drone.
- UGV – Any vehicle on land domain which is unmanned.
- USV / UUV – Any vehicle on sea surface / under water which is unmanned.
- UAS – A system which includes the UAV, a ground control station (GCS) to control the UAV and observe its mission information and the crew.
- sUAS – Small UAS or small drone. Also called Group 1 UAV with less than 9 kg weight.[1]
- MALE / HALE – Medium Altitude / High Altitude Long Endurance Drone.
- UCAV – Any UAV with a combat explosive payload on it. Also called weaponised UAV.
- Loitering Munition – Any UAV designed to search for a target while being airborne and strike the target once detected and trigger the integrated

payload to explode.[2] Iranian Shahed is an example. These are also called One Way Attack (OWA) or kamikaze drones.

- First Person View (FPV) Drone – A UAV with the target view being provided on the goggles of the pilot directly is called a FPV drone.
- C-UAS – An architecture to disrupt the functioning of adversarial UAS or any rogue drone.
- OFC – Optical Fibre Cable is a cable used to tether a drone and passing commands from the operator to the drone.
- Swarm Drones – Swarm of drones is the employment of two or more drones technically. Thus, two or more drones being launched together independently by different pilots but in the same area can be termed as a swarm. However, its claimed full form is 'Smart Warfighting Array of Reconfigured Module'. Thus, a mutually coordinated and functioning group of drones communicating amongst each other is actually a swarm.

Introduction

"*In the next ten years, by 2035, I want to expand, strengthen, and modernise this national security shield. Drawing inspiration from Lord Shri Krishna, we have chosen the path of the Sudarshan Chakra…**The nation will be launching the Sudarshan Chakra Mission. The entire system should be researched, developed and manufactured in India, harnessing the talent of our youth**. This powerful system will not only counter terrorist attacks but also strike back at the terrorists…**India aims to develop its own Iron Dome-like defence system, named Mission Sudarshan Chakra, designed to safeguard critical sites, including civilian areas**."*

-Indian Prime Minister Narendra Modi, 15 August 2025

The Indian Prime Minister's clarion call for "Sudarshan Chakra" defensive shield, from the Red Fort on 15 August 2025, is a clear indicator of the omnipresent drones' threat to our strategic sites whether military or civilian like dams, and even our national pride locations or high value targets. While India emerged victorious in Operation SINDOOR by leaving Pakistan military with no response options on the morning of 10 May 2025, the daily incursions of 300-500 Chinese and Turkish drones launched from Pakistan's

soil highlighted our vulnerabilities despite no significant damage in those 86-90 hours. A comprehensive C-UAS grid is thus a necessity today at all levels within military from a rifle company to HQ IDS and strategic sites, in civil from a border village to our Parliament and similarly across all other entities from dams on Indus waters to other High Value Objectives for the adversary.

Greek philosopher Plato's proverb "Necessity is the mother of Invention" is the most applicable proverb amidst the technology cat and mouse game between drones and C-UAS platforms. Drones were invented by technologically advanced nations to meet the critical necessity of minimising human casualties which were increasingly not acceptable in progressively transparent battlespace where every operation was watched world over. UVs were inducted to replace the human capital in performing the dangerous, difficult, destructive and dull tasks. Now that those drones have become extremely disruptive causing immense human casualties and destruction of civilian infrastructure, there is an inescapable necessity to protect the human capital by establishing a multi-layered C-UAS grid. The miniaturisation of drones under the latest combat proverb of "Big isn't Beautiful Anymore" has asymmetrically magnified the threat of disruptive cost impact wherein a low-cost small drone can destroy a much larger extremely costly platform. Myanmar's resistance group's targeting of military's Mi-17 Helicopter by OFC-controlled FPV drone, Ukraine's targeting of expensive Russian strategic bombers by cellular network controlled FPV drones and the targeting of Iranian SAM sites by Israel's Mossad agents by locally assembled drones amply prove this proverb and that C-UAS architecture is required across the length and breadth of the country and not only along the borders.

All recent and ongoing conflicts have highlighted that one single C-UAS solution will not solve the variety, quantum and density of drones infesting the modern battlespace. Whether be it Operation SINDOOR or Myanmar's ongoing civil war being fought by both sides having Chinese drones' fleet but adopting Ukrainian tactics, or the never-ending Russia-Ukraine war or the re-occurring Iran-Isreal-Houthis drones-missiles bouts, each side has attempted to innovatively saturate and exhaust the adversarial AD with least possible costs and outsmart the other in the technological field. Major strategic surprises and victories have been achieved by the smallest drones despite the existence of an effective C-UAS grid. Thus, it's clear that C-UAS architecture must

be dynamic, alert 24x7 detecting smallest of threats, warning all impacted, and most importantly mitigating the threat temporally and spatially with zero collateral damage.

This primer will thus first describe the dynamics of the pervasive drones' threat, and then identify the key components and technologies within the drones which can be targeted to mitigate the threat. In the next part, the primer will analyse the various anti-drone / C-UAS technologies successfully tested globally and study India's prime indigenous C-UAS platforms. It will then describe the various C-UAS structures validated by the opposing sides in the ongoing conflicts. The major focus of the primer will then be to propose a comprehensive C-UAS architecture for the Indian, recommend certain essential concrete steps to be undertaken by all stakeholders and summarise time-based C-UAS essential steps.

Threat from Drones

"*The low cost, ease of availability, and increasing autonomy of drones have made them the weapon of choice for non-state actors and insurgent groups. From the smuggling of narcotics across the Punjab border to the airdropping of arms in Jammu & Kashmir, drones have proven to be effective tools for asymmetric warfare*. *The 2021 Jammu Air Force Station drone attack was a wake-up call. In under five minutes, two small drones dropped explosives on the station premises—no fighter pilot, no warning radar signature, no traditional engagement possible. It wasn't just a breach of physical space; it was a breach of perception. The enemy didn't need a missile—they just needed a drone with GPS and intent*."

- Group Captain MJ Augustine Vinod, Retired and COO, AutoMicroUAS, 23 March 2025[3]

Whether be it floods and earthquakes requiring disaster management assistance, or controlling fire mishaps, cleaning of railway trains, mapping of land by urban departments, spraying of pesticides by farmers, repair of electricity powerline, traffic control by police, delivery of blood urgently, aerial photography in a marriage or cricket match, or combat reconnaissance of enemy dispositions, drones are truly dual-purpose and replacing humans wherever possible to undertake a wide variety of tasks. On the combat battlespace, small drones have democratized precision strikes by

becoming “SECTION COMMANDER KA TOPKHANA”. sUAS have transformed the battlespace and enhanced the areas of interest and influence much beyond the areas of responsibility. Apropos, the commercial drone market is appreciated to witness a compound annual growth rate of 25.82% to expand from a market value of INR 74002 crores in 2022 to INR 462489 crores by 2030.[4]

This surge in drones’ industry has significantly enhanced the accessibility of drones and its components. Thus, rogue or adversary drones (and even own drones similarly against the enemy) can perform a wide variety of tasks which automatically span a wide variety of threat spectrum necessitating institutionalisation of C-UAS toolkit.

- **Persistent 24x7 Intelligence, Surveillance and Reconnaissance (ISR)**. Within the military, drones in conjunction with space-based satellites have transformed the ISR methodology making the battlespace truly transparent. The saying now goes “If you are still and uncovered, you are bound to get detected”.
- **Explosive payloads Delivery for Destruction**. The saying further continues that “If you are detected, you are bound to die” simply meaning “Destruction Equals Destruction”. Thus, a hunter-killer combination of two separate drones is being used to undertake maximum destruction.
- **Kamikaze / self-destruction by OWA / Kamikaze drones / Loitering Munition**. It’s simply a drone wherein the hunter goes looking out for its kill but doesn’t return as it carries out Japanese World-War II style kamikaze missions by destroying the target by self-destruction over it.
- **Bombing**. Like the much heavy strategic bomber aircrafts, the low-cost small drones are being adequately exploited to bomb targeted areas with mortar bombs, grenades or any locally improvised explosives.
- **Smuggling** of goods as regularly undertaken by Pakistan against India. Indian Border Security Force (BSF) had seized 107 Pakistani drones in 2023, neutralised 294 drones in 2024 and has shot down 175 drones from January to July 2025. With Pakistani smugglers now flying Chinese

drones[a] at more than 1 km altitude, they have now gradually increased the incursions to 4-5 km across IB.[5]

- **Electronic Warfare (EW) and Communication Disruption**. Drones carrying RF and GNSS jammers as payloads to disrupt communication and navigation signals. [6]
- **Communication Relay**. Drones carry communication relay equipment to establish an aerial relay station thereby extending the communication range. Ukrainians often loaded Starlink satellite terminals onboard the drones to extend communication.
- **Direction of Artillery Fire**. Drones are used to increase the precision of conventional unguided artillery by accurately guiding it on the target.
- **Raids or Ambushes**. Drones, particularly FPV variety, are increasingly being used for raids and ambushes as witnessed in attacks by Myanmar's resistance groups' raids of Myanmar Air Force's military airfields, during Operation SPIDER WEB by Ukraine against Russia and Operation RISING LION by Israel against Iran.
- Disruption or interference with enemy operations.
- Mine-laying and demining.
- **Gun platforms**. Turkish Songar drones have mounted MGs to engage troops on ground.
- **Interception of Enemy Drones / Helicopters**. This new mission was first tested when Ukrainians used Chinese DJI Mavic drones to ram Russian drones in end 2022. While Ukrainians targeted Russian helicopters with drones for the first time in July 2024, [7] Myanmar's resistance groups copied the same tactics to destroy Tatmadaw's Mi-17 helicopters.
- **Data Infiltration and Cyber Hacking**. Drones are now being planned for landing on rooftops of data centres for planting wireless intrusion devices. Ukrainians have effectively used them to hack into CCTV networks of Russian towns.

[a] The drones are mainly DJI Mavic series manufactured at Shenzhen in China. With maximum altitude capability of 6 km, and speed of 75kmph, they reach maximum range of 30 km with RF control and endurance of 40 minutes. Few claims are that these drones have even reached 20km across IB on few occasions.

- **Psychological Warfare**. Drones have been effectively employed by Myanmar's resistance groups to maintain continuous pressure on Myanmar military troops through fear and intimidation. Russians and Ukrainians have used drones for running their disinformation and propaganda campaigns. [8]
- Logistics.
- **Population Control**. Chinese effectively used drones for population control and broadcasting messages during COVID pandemic.
- **Decoys**. Drone decoys are being increasing employed by Russians to saturate Ukrainian AD thereby enhancing the penetration of their combat drones and missiles. [9]
- **Civil Tasks**. Logistics delivery, policing duties like VIP security, bomb-detection, traffic management and crowd control, agriculture etc. Indian MHA's Drones Study Report claims that "*Drones with digital dog nose sensors could replace actual dogs for sniffing of explosives for finding illegal drugs; detecting gas leaks; detecting viruses; detecting chemical weapon/toxic chemicals*".[10]
- **Counter Insurgency Operations**. Road opening, drones'-based cordon and convoy protection.
- Mapping and creating Digital Elevation Models especially with LiDAR.

In addition to adversarial drone threats, there is also a possibility of ant-national elements acquiring a NTPT[b] compliant drone[11] forcibly or of unintentional risky drones-

- Technical failures, loss of control in bad weather conditions or breakdowns due to unknown reasons.
- Inadequate knowledge of policies and rules leading to non-compliance / violations in high security areas

[b] "No Permission No Take-off" is a software which enables RPA / UAS except nano category to obtain flying permission in India through Digital Sky platform. More than 6 lakhs unregistered or non NTPT compliant drones were present in India as of 2019.

Having discussed the broad dynamics of drones' threat, it's important to understand the key components of drones and the major technological advancements. The next part of the primer will thus focus on those drones' components and technologies which can be targeted by C-UAS platforms to mitigate the threat.

Drones Technologies and Components

To understand the conceptual contours of C-UAS architecture, it's first important to understand the critical components of any drone / UV / UAV, the complete Unmanned Aerial System (UAS) and the latest technological advancements which can be effectively targeted.

Communication Systems. An UAV becomes part of UAS wherein the UAV communicates with the Ground Control System (GCS) to receive commands and transmit back target information / video. Thus, a command data and video transmission link between the GCS and the UAV is essential in any UAS. Many progressive technological developments have happened in this field.

- **Radio Frequency (RF)**. Allotment of two RFs from the existing electromagnetic (EM) spectrum– one for command and data communication and one for video transmission back were found essential in a basic UAS. However, these were fixed standard RF. The known drone communication bands are 433 MHz, 868 MHz, 915 MHz, 2.4 GHz and 5.8 GHz [12] within which FPV drones generally use 2.4 and 5.8 GHz bands.[13]
- **Frequency Hopping (FH)**. As the RF jammers started jamming the communication linkages between the GCS and the UAV, the UAS graduated to FH communication. By shifting to Software-defined radios (SDR), drone producers adopted spread-spectrum RF for overcoming fixed frequency jamming without any additional payload constraints.
- **Non-Standard Frequencies**. As the RF jammers also got enabled by SDR to undertake multiple RF jamming, the UAS graduated to frequency manipulation to work on non-standard frequencies outside the monitoring range of C-UAS platforms. Hamas, in their 07 October 2023 attack, most likely used RF in their drones beyond Israeli RF detection systems.[14]

- **Dual Band Radios**. Drones have also evolved to use two onboard dual band radios to maintain their communication link. Thus, while one band gets jammed, the drone can still communicate using the second band.

- **Cellular Mobiles**. With the desire of Russia and Ukraine both to use tactical small drones at strategic depths, cellular sim cards for internet-based communication were incorporated in drones to enhance the ranges of control by the drones' operators.
- **AI Enabled / Improvised Electronics**. With the advancements of SDR jammers to undertake multi-band jamming, drones' producers incorporated improvised electronics and AI algorithms onboard drones to evade EW jammers and spoofers. Russian Orlan-10 displayed advanced autonomous flight capabilities in 2023 thereby making Ukrainian EW ineffective. [15] Even Myanmar Junta thus went on to procure the Russian Orlan10 drones in 2024. Intelligentisation of drones has allowed it to identify jamming pattern, automatically classify threats and thereafter restore disrupted signals. Deep learning (DL), Machine Learning (ML) and Reinforcement Learning (RL) methods facilitate smart EM spectrum management and introduce waveform agility to evade detection. [16]
- **OFC**. With the progressive capability of jammers to undertake AI enabled jamming, drones graduated to OFC operated drones mainly OFC FPV drones. This concept then led to the evolution of Mother OFC drone or even a Unmanned Ground Vehicle (UGV) like Ukrainian Karakurt which can carry and further launch OFC FPV drones thereby achieving much longer ranges.
- **Quantum Proofing**. Quantum chips are now being developed to quantum proof the communication of drones making it hacking proof.

Electronic Components. The electronic components are generally dominated by the Chinese including the microchips and transistors. [17]

Motors. Although many Chinese drones' motors are defective as seen in the Turkish Yiha-III drone also, the vast majority of motors, whether complete or in components for later assembly, are still primarily imported from China. [18]

Navigation. Classically, most drones have used Global Navigation Satellite System (GNSS) signals for navigation from various constellations like the American GPS, Russian GLONASS, European Galileo and Chinese Beidou. However, GPS signal jamming and spoofing are the new norms to interfere with the drones. Hence, the drones' manufacturers are now adapting AI enabled alternate navigation technologies. Quantum navigation is the next technology advancement being attempted to end reliance on GNSS chips.

AI Modules. With more battlespace data being generated with every conflict, AI modules on board drones, are becoming more powerful in evading C-UAS measures, automatically identifying targets and engaging them. Chinese made AI modules are extremely cheap today. An Automatic Target Recognition (ATR) and autonomous flight module for FPV drone costs less than 500 USD on Alibaba. A post by "Autonomous Warfare" on LinkedIn on 15 August 2025 amplified that AI-enablement or Intelligentisation in drones, called 'Autonomous Warfare Ontology' encompasses "*Unmanned systems across air, land, maritime, space, and cyber domains; Levels of autonomy and control modes; Human–machine interaction paradigms; Mission types undertaken by autonomous systems; AI capabilities enabling autonomy; and the operational domains in which these systems function*". With a diagram below, the LinkedIn account explains the same in case of loitering munition as: -[19]

"*Loitering Munition (1.1.1) — Operating at Autonomy Level 3 (2.3) with Human-on-the-Loop (3.2) oversight, conducting a Strike Mission – Kinetic (4.2.1) using AI-based*

Target Recognition (5.5) in a Contested Urban Environment (7.7, 7.8)."

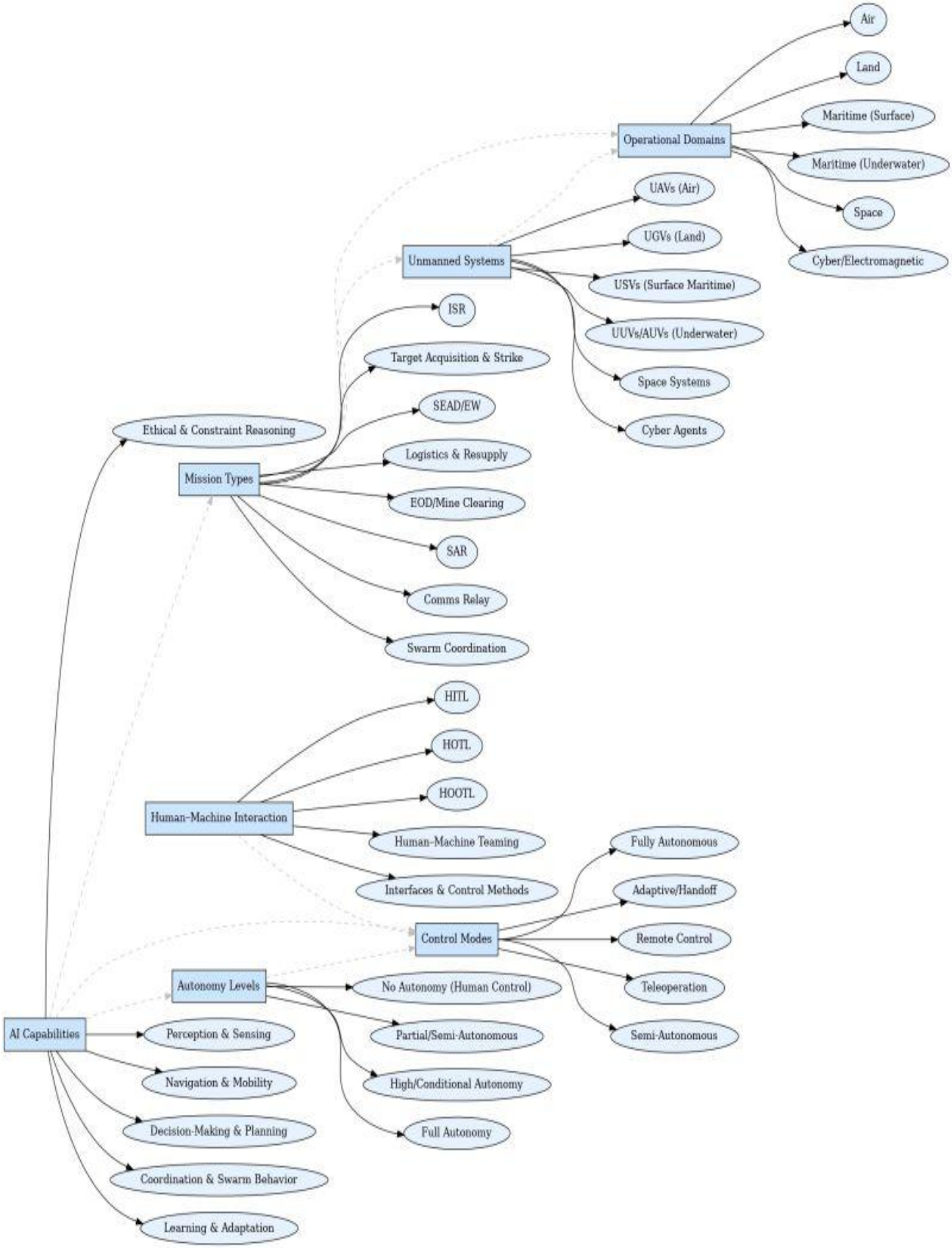

Figure 1: AI Capabilities for Drones
(Source- Autonomous Warfare[20])

AI has enhanced the drone threat manifold by making drones autonomous or semi-autonomous through variety of ML algorithms for Automatic Target Recognition (ATR), near real-time decision making at tactical level and swarm drones' decentralised coordination; enhancing ISR or situational awareness through computer vision, automatic flight planning, obstacle avoidance and autonomous navigation in GNSS denied environment; facilitate edge computing for real-time data processing; and though natural language processing for enhanced machine-machine and human-machine interaction. [21]

Quantum Technology. In addition to Quantum navigation, Quantum technology is being developed for drones at advanced stages for establishing quantum communication links[22], having quantum sensors as ISR payloads and also use Quantum AI (QAI) for advanced drones' management.

Payloads. With a variety of payloads like ISR, Synthetic Aperture Radars (SAR), communication, logistics and most importantly the explosive payloads, the varieties of drones are gradually increasing to undertake the multitude of missions to perform the disruptive, dull, dangerous, difficult and destructive tasks.

Future Developments. The Chinese and few other countries are now fielding biologically inspired drones which are replicating birds or insects and simultaneously working on cyber-autonomous drones which operate completely independently without any C2 links. [23]

C-UAS Technologies

While the first two parts of the primer focussed on the drones' threat and the drones' components and technologies, this part shall undertake a detailed analysis of the C-UAS technologies available globally, the successful technical advancements and will identify the strengths and weaknesses of each of them.

As per the main components of any UAS developed discussed above, a C-UAS grid should thus first detect the UAS as adversarial and target the constituent systems to disrupt their functioning. Thus, the basic building blocks of any C-UAS kill-chain or

even better kill-web are- a detection platform to detect any UAV nearby; a Command and Control (C2) system to positively identify the UAV as adversarial; and then an engagement system to either destroy it termed as hard kill or disable it termed as soft kill.

Detection. Detection of drones can mainly be undertaken by radars both passive and active variety systems, visually, thermal systems- electro-optic (EO) and Infrared (IR) both long-wave IR (LWIR) and medium-wave IS (MWIR), RF detectors, LiDAR and acoustic sensors. However, the biggest challenge for wide array of available modernised detection sensors is the detection of small drones (sUAS). These are covered in the succeeding paragraphs.

EO / IR Optical Cameras. EO cameras display the reflected / emitted thermal signals of the drone in various bands- Near IR (NIR), Short-wave IR (SWIR), MWIR and LWIR[c]. Usually mounted with pan and tilt control for automation, they have a maximum range varying from 500 m to 15 km depending on the available line of sight (LOS). The cost range of EO cameras varies from 20,000 to 500,000 USD.[24]

- **Strengths**. The biggest advantage of EO/IR cameras as a detection platform are that they are very useful for visual classification and then classifying detected drone by employing image recognition VLMs.[25]
    - Effective in non-RF environment too like for detecting OFC FPV drones.
    - Facilitate Multispectral fusion i.e. NIR, SWIR, MWIR and LWIR.
    - Allows low-cost ML / RL.
    - Post confirmation of enemy drone, its digital tracking is easy.
- **Weaknesses**. The major weakness is the adverse impact of bad weather and fog [26] particularly for the visible and NIR cameras.
    - Dependent on LOS and cannot function beyond visual range (BVR). Higher zoom is required for sUAS and bigger drones at longer ranges.

[c] Visible band, most suitable for daylight conditions provides horizontal resolution from 1280 to 3840 pixels; NIR is most apt for low light conditions and provides a resolution from 704 to 2560 pixels; both visible and NIR are not suitable for foggy / rainy conditions. SWIR is ideal for high humidity with resolution ranging from 640 to 1920 pixels; finally, MWIR and LWIR are best employed in zero light conditions with resolution ranging from 640 to 1280 pixels.

- Multi-spectral camouflage can beat EO/IR devices. As it is, it's slightly difficult to detect drones amidst stress and clutter.
- They can be blinded by reflective decoys.
- IR cameras are not fully effective in low temperatures and rain / high humidity conditions.

Lidar. These systems employ lasers to detect any incoming drones by measuring distances. [27]

Radars. AD radars have been the most famous platforms for detecting aerial threats with claimed ranges of drone detection varying from 500m to more than 20 km depending on the radar cross-section (RCS) of the incoming drone. The cost range of radars varies from 20,000 to more than 10,00,000 USD. [28] However, in case of C-UAS operations, they suffer from key disadvantage of active emissions giving away their positions, small radar cross-section of drones which are nearly negligible in case of small drones, and doppler frequency shifts of drones and birds are nearly similar. Significant technological advancements have been made in the domain of radars too.

- **Active Radars**. While the L and S band radars are generally used for detecting UAS, X-band is found suitable for UGVs. K and W bands are more suitable for detecting short range ground movement.[29] Active radars are of two types – pulse type and continuous wave (CW). While pulse type emits short pulses, CW emits illumination signal continuously. The data provided is very reliable and accurate. [30]
- **Passive Radars**. Passive radars do not emit and use the emissions of nearby cellular tower or some other similar platform to detect drones or other aerial threats. Drone Shield's 8th edition of C-UAS factbook emphasises that "*Potential illumination signals that could be used for UAS detection include Frequency Modulation (FM), Digital Video Broadcasting (DVB), Global System for Mobile Communications (GSM), Global Navigation Satellite System (GNSS), or Wireless Fidelity (Wi-Fi)*". [31]
- Miniaturization of Solid-state Active Electronically Steered Array (AESA) radars. [32]

- **3D Radars**. Israel has effectively used 3D radars in its C-UAS platforms Elbit systems ReDrone and the Rafael Advanced Systems Drone Dome to detect adversarial drones. [33]
- **AI Enablement**. AI enablement of drones is facilitating adaptive signal processing, real-time clutter suppression, adaptive waveform generation, enhanced phased array antennas by optimised beam steering, enhanced data fusion for AI-driven target prioritisation, autonomous threat detection and target recognition, predictive maintenance and fault detection.[34]

The strengths and weaknesses of radar-based detection are listed below:

- **Strengths**. The major advantage of radars is long-range all-weather detection capabilities over a wider area comparatively.[35]These are most suited when:
  - The target volume capacity is high.
  - Target classification algorithms have matured.
  - There is no interference with military or civilian signals.
- **Weaknesses**. Apart from being active emitters, the cluttering of low-altitude returns, and resultant higher detection threshold results in low efficiency against low-RCS drones. [36]
  - They require EM spectrum deconfliction for allotment of additional RF.
  - Many of them require fixed gimbaled mounts.
  - Low-altitude drone flight routes facilitate terrain masking.
  - Swarm drones and tactics cause saturation.

RF Detection. Detection of RF emissions is the most basic C-UAS task with maximum range achievable from 300m to 15km and cost ranging from 20,000 to 500,000 USD. RF sensors normally operate in the known drone communication bands of 433 MHz, 868 MHz, 915 MHz, 2.4 GHz and 5.8 GHz and depend on the library of known signals. [37] RF detectors can also detect the drone crews generating the radio control emissions.[38]

- **Strengths**. The biggest advantage of RF detection is that it's a passive method which is employable in all meteorological conditions and thereby facilitates stealthy detection. Additionally, it facilitates RF fingerprinting for

creating independent ID for each drone; early warning via telemetry sniffing; can be easily integrated with 5G; and provides multipronged detection mesh. [39]

- **Weaknesses**. The primary weakness is its absolute ineffectiveness to detect autonomous, 5G enabled and OFC FPV drones. Additionally, many false targets appear in dense RF environments caused by legitimate wireless communications in urban areas. In addition to masking of drone communications by Wi-Fi, Bluetooth and other signals, RF detection is also prone to electronic deception. It is unable to intercept encrypted links, satellite-based commands and burst communications. [40] Additionally, the library needs regular updates.

Multi-Band RF Detection. As the drones have advanced from fixed frequency to FH, the RF detection systems have also advanced to multi-band spectrum analysers.

Acoustic Sensors. Due to high level of noise in acoustic environment, maximal range of acoustic microphones varies from just 200m to 1 km with most small and medium drones producing acoustic signatures range of 200-5000 Hz. The cost of acoustic sensors generally ranges from 20,000 to 100,000 USD. As seen in Sound Ranging systems for detecting enemy guns and mortars earlier, acoustic drone detection systems can provide multiple detections simultaneously. Although the biggest advantage is that it's a passive system, it requires very careful deployment. [41] BSF has gone to exploit the natural hearing capabilities of K9 dogs to pick up the auditory signatures of drones to alert the BSF troops about the incoming Pakistani smuggling drones. [42]

- **Strengths**. The strength of the acoustic systems is that apart from being purely passive and comparatively low-cost, they don't depend on LOS. [43]

- **Weaknesses**. Apart from very high false alarm rate, their range is very limited. While they are ineffective against muffled propulsion and stealth blades, the acoustic libraries are also limited. [44]

Quantum Sensing. In order to overcome limitations of various detection techniques and to ensure greater precision of detection, quantum sensing technology is now being researched and developed to employ Quantum Sensors for detection of drones. This technique is likely to be more effective against AI enabled drones evading other detection methods. [45]

Having discussed the first aspect of the C-UAS kill chain – detection, it's now important to talk about the various other mitigation techniques against drone threats both soft kill and hard kill variety. The next sub-part shall thus first focus on soft kill aspect.

Electronic Warfare (EW). The simplest C-UAS solution is to detect any EM transmission and disrupt the same particularly the data link between the GCS and the UAV for C2 or jam the GNSS signals. The standard jamming sequence has been to jam the drone's command link. The drone may then either gain height to regain communication by evading jammer or may adopt an AI enabled route to follow pre-designated flight route. The adversary will then ideally jam the GNSS signals of the incoming drone or may even spoof them to mislead the drone.[46] The EW, in the C-UAS domain has advanced significantly despite lagging behind drones EW hardening advancements: -

- **Fixed Frequency EW**. This was an old concept wherein the jammers focussed their power on a single RF to jam it. RF jammers typically jam the RF link between the drone and its operator / GCS. On being effectively jammed, the drone can either hover at same place, fall down or undertake pre-planned "Return to Home" move.
    - **Strengths**. In addition to being non-lethal and low-cost, they cause immediate loss of control and can achieve wide area GPS lock. [47]
    - **Weaknesses**. The most important limitation is the imposition of legal restrictions in civil airspace particularly near airports. They are ineffective against GPS-independent drones, encrypted and FH communication links, cellular communication links, AI enabled jamming evasive and OFC drones. [48] Jamming of drone's transmission signal is always more difficult than jamming the drone's command signal from the GCS.

- **C2 Spoofing**. The spoofing of drone's C2 signal aims to force land it a place of choice or force the drone to 'return to home".
- **SDR EW**. The jammers have graduated to software-defined multi-band jamming.
- **AI Enabled Jamming**. Like drones, the jammers were also AI enabled to prevent Intelligentised and advanced electronic drones from evading EW.
- **GNSS Jamming and Spoofing**. The basic concept was to jam GNSS signals (GPS and Galileo are in the ~1,100 to 1,700 M Hz spectrum) to ensure that the drone lost its geospatial orientation. As the technology progressed, GNSS spoofers were developed to give fake targeted GNSS signals thereby altering the drones' geographical coordinates away from the actual location. However, the employment of C-UAS spoofers[d] including GNSS receiver lock ups, at airports has significant collateral impact on own aircrafts. [49] As the hardened drones overcame spoofing through encrypted military grade precise GNSS signals or through hardening, the C-UAS engineers particularly in Russia are aiming to jam the GNSS satellites themselves. However, the alternate navigation techniques like Quantum navigation may overcome EW constraints altogether till another quantum counter is developed. Chinese have now designed TDXL-KGR 1101 anti-jamming array antenna for receiving Beidou and GLONASS signals and transmitting BDS L-band signals.

Net Drone. These drones carry net as a payload to capture the threat or rogue drone. [50] Nets are also fired by few shotguns.

Cyber Takeover. The enhanced number of computing devices on any advanced drones have made them that much more vulnerable to cyber takeover. The cyber takeover involves firstly interception of the drone C2 signal and then overriding it. [51] Drone hacking has evolved significantly during the Russia-Ukraine war. The hackers aim to steal data, or hijack the drone from the pilot to take over physical control and land the adversarial drone at a location of hacker's choice.

[d] Many C-UAS companies advertise than their spoofers have "Selective of Targeted" RF Interference capabilities. However, the truth is collateral impact will happen on own aircrafts when used near airports.

- **Strengths**. They facilitate precise takeover of adversarial drones without any collateral RF effect and exploit OEM[e]-provided backdoors.[52]
- **Weaknesses**. The major challenge is the time, normally around 30 seconds or more, which it takes to decrypt a single drone. [53] The technique is ineffective against satellite communication enabled UAS, cellular communication links-based drones and encrypted C2 links. [54]

The Russian-Ukraine and Iran-Israel wars and even Operation SINDOOR have shown limited impact of soft kill EW methods of jamming and spoofing. The Myanmar's resistance groups advancement to OFC FPV drones made military junta's procurement of jammers less impactful. Thus, the next sub-part shall discuss the hard kill options for mitigating drones' threat.

With Russians induction of Chinese made OFC drones evading Ukraine's advanced EW, the Ukrainian solution evolved was "**When you can't jam, you hunt**".[55] Apropos, guided missiles, radar-guided AD guns, helicopter engagements[56] and drone interceptors have proven to be more impactful in mitigating the drones' threat. However, both guided missiles and helicopters are expensive engagements of low-cost drones and thus are restricted in scale.

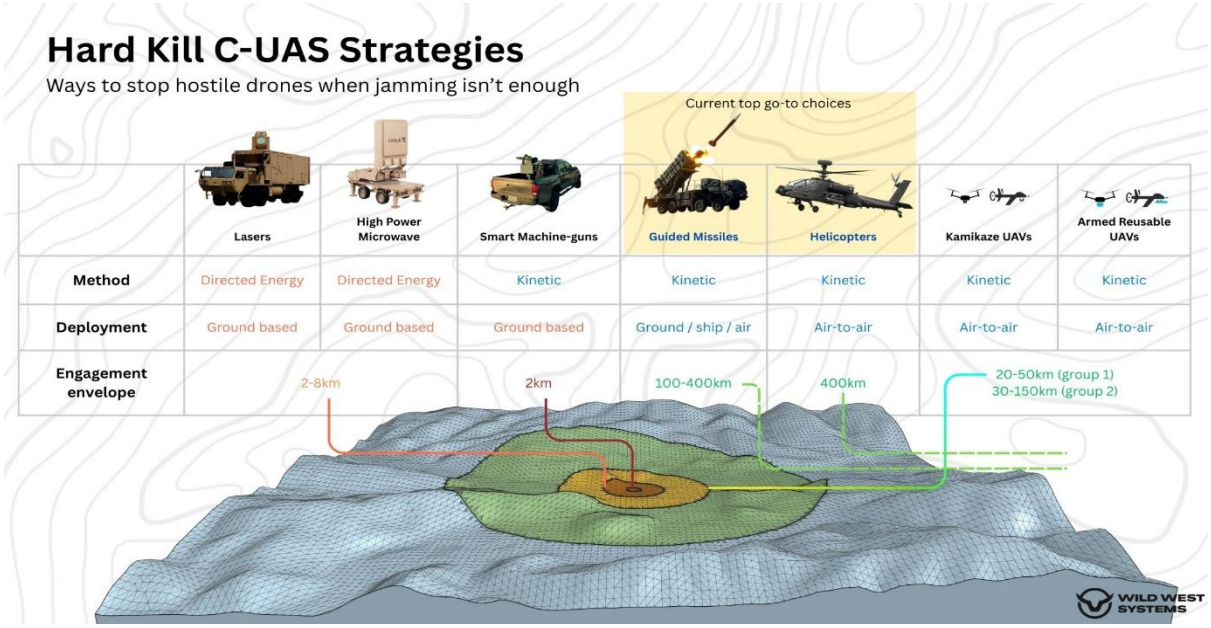

Figure 2: Hard-Kill C-UAS Strategies
(Source-Moshe Baum[57])

[e] Original Equipment Manufacturer.

Ground-Based Directed Energy Weapons (DEWs). Lasers and High-power Microwaves (HPMs) are DEWs which have supposedly achieved ranges of up to 10 km while claims are for 20-25 km. While lasers target critical components of the drones by using directed energy, the HPMs direct high intensity electromagnetic pulses (EMP) to destroy the electronic system onboard the unmanned aircrafts. While the initial procurement and induction costs are extremely high, the cost per shot in C-UAS missions is very low.

- **Lasers**. The single biggest advantage is precise targeting. However, they are adversely impacted by sensitive weather and fog conditions. [58] Newer versions of Rafael Drone Dome use lasers to destroy incoming drones. [59] The cost of lasers depends on the quantum of power and hence a low-powered system would be cheaper but achieve lesser range. In any case, lasers have to be aimed preferably at the drone's weak point- the propellers for several seconds to cause destruction. **This kind of aiming on high-speed drones is very difficult which thus requires significant training of laser operators.** [60]
- **HPM**. With a wide field area coverage, they are most suitable for neutralization of swarms. However, they are ineffective against EM-shielded drones and have the risk of collateral damage / fratricide. [61]

Chinese are claimed to have developed a handheld AM-500 DEW for a range of 1 km and Sheng-1 DEW with a range of 2-25 km for intercepting drones and missiles.[62] Russians have most probably used the Chinese DEW Shennong Shield 3000 successfully to intercept Ukrainian drones.

AI Turrets. The first few AI turrets like Ukrainian Sky Sentinel turret, seen on the Ukrainian battlefield, are claimed to have targeted four Russian Geran OWA drones with mounted machine guns. Its major feature is autonomy in target detection, trajectory calculation and prediction, and then engagement of incoming drones without any human intervention. [63] Autonomous Warfare LinkedIn account, in its post of 15 August discussed earlier above, describes AI enablement of C-UAS turret as: -[64]

> "*At Autonomy Level 3 (2.3), with Human-on-the-Loop (3.2) engagement approval, executing Defensive Strike – Kinetic (4.2.1) using Perception (5.1) and Target Recognition (5.5) in Urban Base Defence (7.7)*."

Small Guns. A large variety of small hand-held guns and machine guns are being used for intercepting drones.

- The AI enablement of machine guns and provision of AI-enabled turrets has enhanced the precision and strike rates for engaging drones up to a close range of 2 km.
- Net guns have been designed to entangle drone or its rotors by firing nets.
- Shot guns have been designed to fire specialised anti-drone cartridges. Russians effectively used Stupor C-UAS gun to intercept Ukrainian drones. [65]
    - Ukrainians have now started mounting six-barrel shotguns on FPV drones to engage adversarial drones in an aerial battle. An Instagram account "drone wars_", stating from X-account handle "RoyCA@GrandpaRoy2" describes its capabilities as: -

      "*It has three firing modes - single, burst, and salvo. But the main advantage of the system is that it has no recoil - Its shot power can be compared to a 12-gauge shotgun*."[66]

Figure 3: 6 Barrel Shotgun FPV Drone

(Source-RoyCA@GrandpaRoy2 and drone_wars_[67])

Interceptor Drones. Amidst surging Russian drones' production capacity, declining availability of Ukrainian combat manpower, and depleting US aid, the cheapest and most effective option for Ukraine to minimise own casualties was to use low-cost drones as interceptors against Russian OFC FPV drones which couldn't be jammed

electronically. As these interceptor drones succeeded more than other C-UAS options, they enhanced the speed of these drones to make it faster than Russian Geran drones for intercepting them. Being locally produced, the Ukrainians improved the radar sensing coverage and organised extensive pilots' training to start successfully intercepting Shahed variety drones from March 2025 onwards. While they have graduated from slower reconnaissance to Shahed / Geran series drones, the drone interceptors' performance does reduce in bad weather conditions like fog and thunderstorms. At an approximate cost ranging between 5,000 to 10,000 US dollars, it's much cheaper than Shahed kamikaze drones.

In the next stage of development, American company Swift Beat plans to collaborate with Ukraine to design drones capable of intercepting missiles. Since specialist interception training particularly for operation in conjunction with radars takes time, and Ukraine is facing manpower shortfalls, the response of interceptor drones is being automated by AI.[68] Rheinmetall has introduced an autonomous interceptor drone for precise for engagement of rogue drones as shown in the figure below.

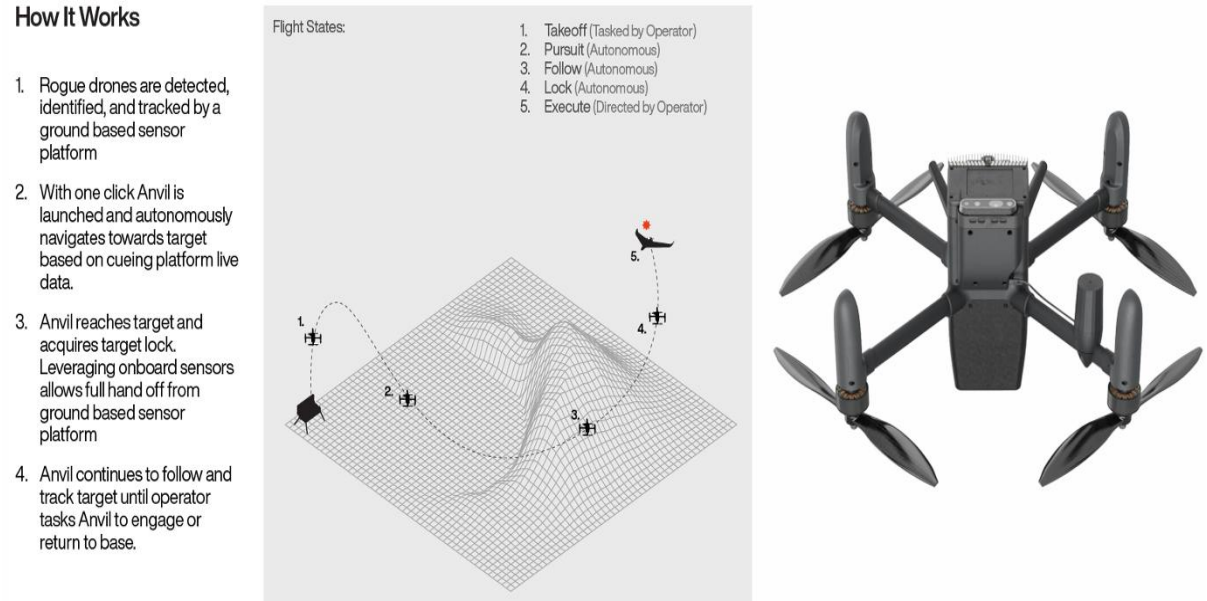

Figure 4: Rheinmetall's Autonomous Interceptor Drone

(Source- Rheinmetall[69])

Kinetic interceptors, despite having many advantages, have few challenges too. The biggest challenge is that it's a one-on-one engagement and thus swarm intercept tactics would need equal numbers of interceptor drones. Flight dynamics stress is another challenge during adverse wind conditions. Most importantly, decoy drones can overwhelm interceptors.[70]

Swarm Defence. In order to neutralise enemy swarms of drones, swarm drones are another good mitigation option. Automated decentralised swarms allow faster response required to handle large numbers of drones simultaneously. [71] The US engineers at its Naval Air Warfare Centre Aircraft Division have developed an AI module called the Optimized Cross Domain Swarm Sensing (OCDSS) to rapidly generate swarms mission plans. It simulates numerous scenarios to identify the most suitable combination of ISR sensors, platforms, explosives and drones' formations to achieve the desired objectives from swarm drones.[72]

Legal and Administrative Measures. Various legal and administrative measures also facilitate protection against rogue drones. [73]

- **Geofencing**. Chinese DJI geofencing software is a prime example of how the drone's GNSS-based software prevents it from entering zones defined as restricted. However, in Indian context as seen in Ukraine too, the Chinese OEM can exploit this to limit DJI drones (whatever procured by Indians) from attacking certain areas. **Indian government needs to promulgate indigenous software defined geofences which must be compulsorily installed on all drones registered within India**.
- **Registration**. All drones, except nano category (<250 grams as per Indian Drones Regulations 2021), are compulsorily registered and given a Unique Identification Number (UIN). However, this becomes very difficult in case of locally assembled drones.
- **No-Fly Zones / Restricted Areas**. This has already been done under various Indian policies. DGCA has restricted that drones in India cannot fly above 120 metres altitude vertically. Furthermore, night drone operations are restricted except for government, emergencies or when permitted by the DGCA.

Drone Forensics. Drone forensics is a method of conducting detailed investigations of captured / downed adversarial drones to identify vulnerabilities and develop counter measures. It requires convergence of both drones and C-UAS experts in uniform and outside- talented and passionate drones engineers.

Justin Nerdrum, a US Marine Corps veteran, in his LinkedIn post summarised that in a recent test of 30 Counter-drone systems, only 3 passed the “Ukraine Test”. He amplified that: -[74]

> “*Project Flytrap 4.0 revealed that most C-UAS tech fails against real drone tactics… FPV drones with fibre-optic control laugh at your RF jammers. 30-50 km range. Zero emissions. Unstoppable with traditional tech.*
>
> ***What worked -*** *Autonomous hunter-killers that match drone speeds; Passive sensors are invisible to enemy EW; Squad-portable jammers under 20 lbs.*
>
> ***What failed -*** *Anything requiring perfect weather; Systems needing 5+ operators; Solutions costing more than targets.*”

A comparison of various C-UAS technical systems is summarised in the table below.

Detection System	**Range**	**Detection Method**	**Effectiveness Against Swarms**	**Efficiency in Bad Weather**
Radar	High – BVR	Active (except passive radars)	Capable	Yes
RF Sensing	High - BVR	Passive	Limited	Yes
EO / IR	Medium – LOS based	Passive	Limited	No
Acoustic	Low, but not LOS dependent	Passive	No	No
LiDAR	Medium	Active	Capable	
Mitigation Method	**Legality**	**Collateral Impact**	**Cost per mission**	**Versatility**
EW - RF Jammers / Spoofer	Restricted, particularly near Airports	Moderate, Severe near airports	Low	Medium
Cyber Takeover	Restricted	Low	Medium	Limited
Interceptor	Legal for combat	Low	Medium	High
Laser	Legal for combat	Low	Low	Medium
HPM	Legal for combat	High	Medium	Low
AD Guns	Legal for combat	Very low	Medium	Medium
SAMs	Legal for combat	Negligible	Very high	High

Shotguns / Net guns / AI enabled MGs	Legal for combat	Negligible	Low – Medium	High
Geofencing	Legal	Nil	Negligible	Limited

Table 1: Comparison of C-UAS Platforms

(Source-Author's Research)

C-UAS Solutions. Having identified and analysed the various C-UAS technologies, it's important to understand the various C-UAS solutions- individual soldier wearable, portable, mobile, static and large-scale types.

- **Man-portable / Wearable**. These are for frontline soldiers for immediate response for our troops' survivability. The portable and wearable drone jammers or shot guns are prime example.[75]
- **Transportable Solutions**. Employing hybrid convergence of various C-UAS platforms, a vehicle generally mounts few sensors and mitigation platforms. These systems are modular and can also be moved and made operational in a new location even if not permanently mounted on a vehicle. [76]
- **Maritime Solutions**. These are tailor-made for maritime domain integrating detection and mitigation platforms for conditions applicable on a naval vessel. [77]
- **Hybrid AD and C-UAS**. The drones' threat is integrated in the overall aerial threat and thus the AD system of detection and mitigation includes coverage of drones too.[78] During Operation SINDOOR, Indian military in a manner had adopted this solution.
- **RAAMD**. The handling of all aerial threats is the ideal solution. Israeli Iron dome is the ideal example which has tailor-made its sensors, EW, interception missiles and DEWs in a fused manner to handle threats from rockets, artillery, air, missiles and drones. America is trying to replicate it over a much larger area through the ambitious Golden Dome plan. Indian Prime Minister's announcement of 'Sudarshan Chakra' shield takes it one step ahead by including both defensive and offensive missions.

After analysing the C-UAS technologies and solutions available globally, the next short part of the primer will look at India's key indigenous C-UAS platforms.

Indian Indigenisation

It's well established now that with rapid evolution of drones' technologies, C-UAS technology is undoubtedly lagging behind. Russian drones, with Iranian and Chinese assistance, have repeatedly outwitted Ukrainian C-UAS platforms. Thus, with China's domination of evolving drones' market, the Indian "Sudarshan Chakra" defensive shield mission requires complete indigenisation of RAAMD architecture. Operation SINDOOR showed the prowess of the RAAMD efficiency of Indian military to minimise the damage of Pakistan's drones, missiles, aircrafts, rockets and artillery. However, much more needs to be done urgently. One indigenous system which amalgamates most C-UAS techniques discussed above and proved successful in Operation SINDOOR was the **BEL and DRDO's D4 (Drone Detect, Deter, Destroy)** C-UAS platform.

D4 System. India's Integrated Drone Detection and Interdiction System (IDD&IS MK1, also called D4) is an indigenous C-UAS platform costing approximately Rs 20 crores. As per BEL, *"To address the malicious threats posed by rogue Drones, a Counter Drone System has been developed by DRDO & Productionized by BEL which has been operationally proven. The Counter Drone System (D4 System) is capable of performing real time search, detection, tracking and neutralization (Soft/ Hard Kill) of the flying drones (Micro/Small UAVs) and will provide object details (Optical / Thermal) and RF spectrum display on GUI (Guided User Interface)*." The vehicle-based system has a detection range of 5-8 km, soft kill interception range of 2-5 km and hard-kill range over 800m.[79] BEL states "*Counter Drone system (D4 System) is configured with the following systems*"[80]

- *"RADAR System – Drone detection and tracking".* Employs X-band radar to get precise bearing and range even for sUAS's low RCS. [81]
- *"EO System – CCD, IR camera with LRF for detection and tracking of Drone target".* Employs EO/IR sensors to mitigate false positives from other detection methods. [82]
- *"DF Counter Drone System- Drone communication channel RF Detection & Jamming, GPS Jamming / Spoofing System (Soft Kill)."* It has the capability to

scan most commercial drones. The system also has Wi-Fi de-authentication capabilities. [83]

- *"Laser Directed Energy Weapon System (Hard Kill)".*
- *"Command & Control Centre (C3) with Power Source for complete Syste*m". An integrated AI module differentiates between drones and false targets to classify the target drone as quadcopter, fixed-wing or hybrid. [84]
- Some models may also have interceptor drones, net-based entrapments and projectile launchers too. [85]

One of the designers of D4 C-UAS platform, Group Captain MJ Augustine Vinod, Retired and COO, AutoMicroUAS, in his article of March 2025, two months before Operation SINDOOR states that

> "*In 2024, after multiple test cycles, the D4 system was declared operational. The Ministry of Home Affairs and the Indian Army began trials at select locations—particularly in Punjab, Jammu, and the Northeast, where drone intrusions had surged. Today, D4 is being deployed in layers: Forward bases to monitor infiltration and drone drops; Strategic installations like ammunition dumps, airbases, and communication hubs; Border Outposts (BOPs) to detect cross-border smuggling and recon drones… In at least three reported incidents, the D4's interceptor drone brought down a rogue UAV before it could cross the border—making this not just a defensive system but a* ***proactive countermeasure***…*D4 is being constantly upgraded: Integration with facial and payload recognition; 5G jamming modules; Portable D4 Lite versions for VIP protection and convoys; Naval variants with maritime radar integration. AMOS Aerospace, AutoMicroUAS, and others are working parallelly to make this ecosystem modular, mobile, and interoperable*."

Indigenous DEW. In early 2025 before Operation SINDOOR, India's DRDO successfully demonstrated a 30 kilowatts Laser-based weapon system with a 5 km range for neutralising swarm drones, missiles and aircrafts.[86] DRDO has also announced its plans to build the **300-kilowatts laser system 'Surya' with 20 km range by 2027**. Raghav Patel claimed that the key components of the system would

be mounted on two 8x8 vehicles and will include an Advanced Laser Generator, Long Range 60 cm aperture beam director and an Integrated Control System.[87]

With a broad understanding of drones' threat and the various C-UAS technologies and platforms including few indigenous systems, there is a need to understand the force structuring of various C-UAS platforms to optimise their effectiveness. Thus, the next part of this primer shall discuss the various C-UAS structures fielded in the various ongoing conflicts with major focus on the Russia-Ukraine war.

C-UAS Combat Groups

The advancements in drones' employment techniques and doctrinal evolution have simultaneously led to the evolution of C-UAS combat groups at various levels. The major C-UAS concepts of combat structuring as witnessed in various conflicts are discussed in this section.

Mobile Fire Groups. Comprised of variety of mobile AD weapon detachments like machine guns[f], Man-packed AD systems (MANPADS) like IGLA, radar-guided AD systems, thermal imaging (TI) devices, laser target designators (LTDs) and advanced optical sensors, these mobile detachments have been used by Ukrainian military to counter drones in the ongoing war with Russia. As per various estimates, Ukraine's approximately one thousand mobile fire teams have caused just 1% confirmed drone kills. They have been able to successfully intercept 80% Russian Shahed drones strikes at their peak. The efficacy of such groups has become questionable as their effectiveness is now between 20 to 40%. [88]

Surface to Air Defence Groups. The Surface to Air Defence Groups primarily comprise Surface to Air Missiles (SAMs). SAMs are mainly of three types- short range (SR-SAM) like Akash; medium range (MR-SAM) like Barak-8 and long range (LR-SAM) like S400 and Chinese HQ9. The high costs of SAMs prevent its usage against low-cost drones. Hence, SAMs particularly MR-SAM and LR-SAM variety are

[f] A successful machine gun interception of a drone ideally requires the machine gun to be along the drone path.

generally deployed to protect high-value critical infrastructure and are prioritised for missile-threats and not drones. SHORAD (Short Range AD) groups mainly include SR-SAMs, and anti-aircraft guns (AAGs) of various varieties- towed (generally obsolete now), wheeled and self-propelled (SPAAG) and generally have a range up to 10-25 km.

EW Groups. EW groups have been deployed by all conflicting sides India-Pakistan, Russia-Ukraine, Myanmar's Tatmadaw and resistance groups to jam adversarial drones' signals but have limited short-to-medium range. Pakistan has been exploiting these limitations very effectively to fly its smuggling drones at altitudes above 1 km across Indian border to evade Indian EW. The adoption of Alternate navigation / GNSS techniques and hardening of drones against EW jamming including adoption of OFC FPV drones has further limited the effectiveness of EW based C-UAS. Ukraine's more than 140 EW companies are not able to match up Russia's surging production capacities of Geran (modified Shahed) drones. Despite Ukraine's best EW system Bukovel-AD's detection ranges of up to 100 km and jamming radius of 20 km, the major limitations are that EW alone can't cover omni-directional simultaneous launch of drone swarms particularly at Russia's current scales of launch of Geran drones. [89]

Interceptor Drone Groups. The interceptor drone groups, invented by Ukraine, basically comprise the trained interceptor drone crews and radar detachments. As the Ukrainian military has advanced this interception technique and tactics from slower reconnaissance drones to Geran / Shahed series of drones, five varieties of interceptor drones have been approved for Ukraine's operational use. They have nearly achieved 70% interception rate of Shahed drones which is more than double of the mobile fire groups. While Ukraine plans to produce thousands of interceptor drones to match Russian Geran production capacities, the major challenge remains is the shortage of radar systems. While hundreds of radars are essential for better effectiveness of the interceptor drones, Ukraine holds only few of them. [90]

Aviation. A very distinct tactical change by Russian military to fly drones at altitudes varying from 2 to 4 km made it extremely difficult for Ukrainian ground units to undertake EW and also engage them. The Ukrainians, with limited Air Force, then modified their interception tactics by engaging the Russian Geran / Shahed series of drones with helicopters and light sport aircrafts like Yak-40. It basically involves the

co-pilot to engage the incoming Shahed drone at an approximate speed of 180-200 km per hour with his machine gun or rifle.[91]

DEW. Russia has supposedly started using Chinese DEW as per various videos on Chinese net. Similarly, many Ukrainian projects are supposedly underway. One Ukrainian laser system Tryzub has a claimed range of more than 2 km altitude. However, no large-scale use has been confirmed till now. [92] The DEWs are potentially one of the most effective C-UAS systems particularly against swarm drones and would have to be appropriately integrated at the earliest in the C-UAS architecture.

The ideal **mobile fire groups** at various levels within the Indian Army are suggested below: -

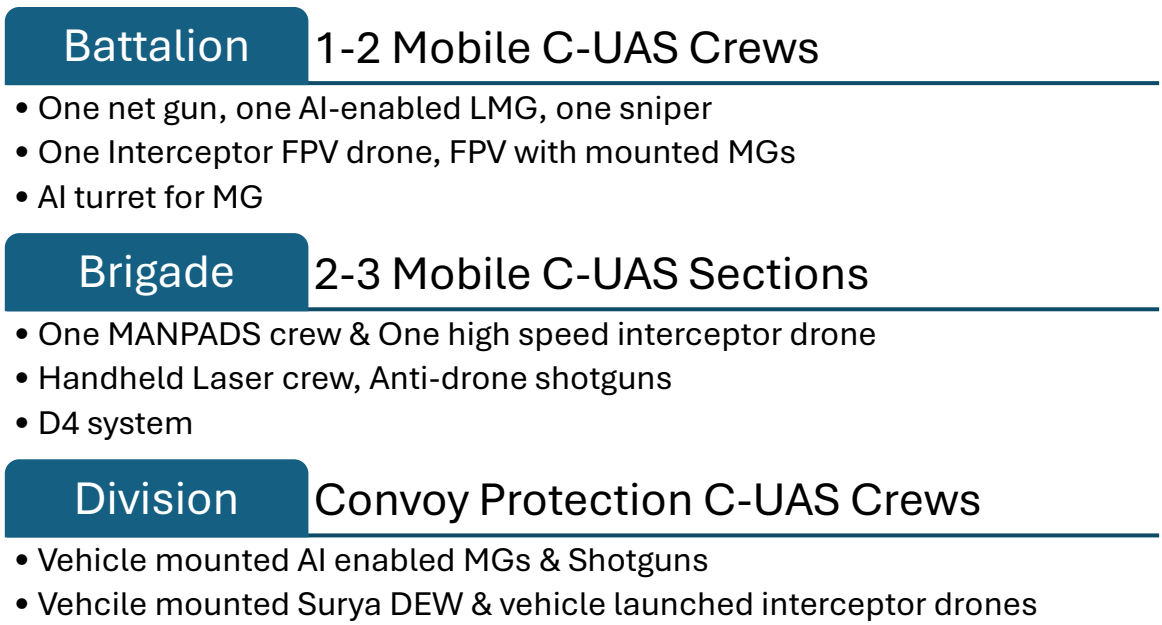

Figure 5: Recommended C-UAS Groups for Indian Army

(Source- Author's Research)

After understanding the C-UAS technologies, platforms and force structures, the next part of the primer shall focus at the most important issue – the proposed concept and C-UAS architecture for India.

Proposed C-UAS Concept

C-UAS architecture must be based on the basic concept of kill chain i.e. to detect, track, identify, classify, alert, deter / mitigate / engage and finally record, visualise and analyse the complete C-UAS performance cycle.

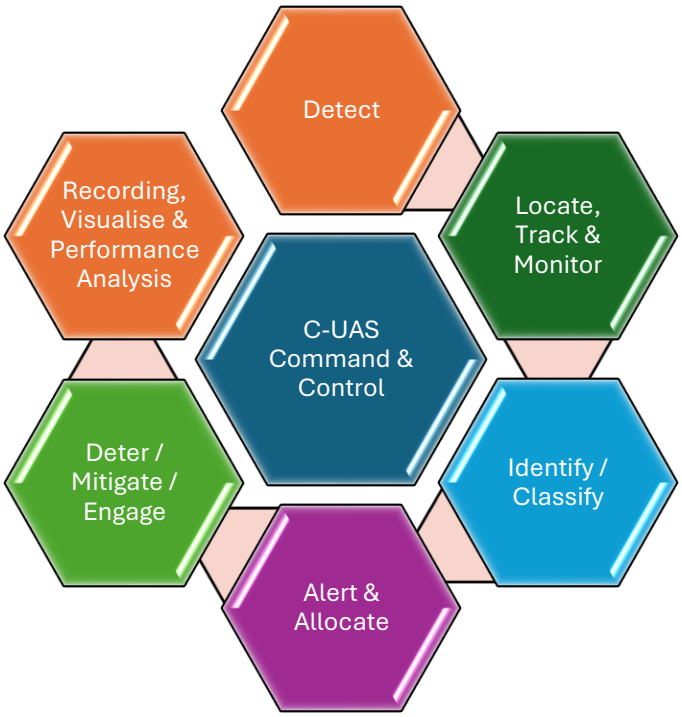

Figure 6: Essential Sub-Modules of Basic C-UAS Architecture

(Source-Author's Research)

Command and Control (C2). The C2 module and system in the C-UAS architecture must facilitate **real time decision support across multi-mission capabilities and converge multi-disciplinary multi-OEM platforms**: -

- **Clear delineation of C2 organisational structure**. It can't be divided anymore. While Operations branches of HQ at all levels are busy with major combat operations, AD and IAF are busy with kinetic mitigation of aerial threats, EW entities with RF based detection, jamming and spoofing, there is no single entity to stitch the complete C-UAS kill chain together.
- **Layered and multi-tiered** system integrating all stakeholders, sensors and shooters in the designated area of responsibility.
- **Converge drone / UV hunters and killers** in near real time thereby matching the speeds of incoming drones.

- **Indigenous multi-media communication** means between the sensors, C2 setup and engagement platforms of both hard and soft kill variety.
- **Comprehensive situational awareness** with effective **multi-domain battle space management** of drones and C-UAS platforms particularly in the RF and aerial domains.
- A **cost-effective sensor-target-weapon matching module** to match the threat level, speed, and quantum with own tracking and engagement methods.
- Ensure overlap of both sensors and shooters to **mitigate blind zones**.
- Capabilities to **handle both stack and swarms of drones** in temporally displaced formats.
- **Alert concerned agencies** involved in tracking, and mitigation of drones' threat as well as generate **warning alerts** for impacted population / military entities to undertake suitable survivability and mitigation measures.
- **Cyber resilient algorithms to overcome data poisoning attempts and excessive false positives.**
- **Ensure interoperability and systems convergence throughout between detection and mitigation sub-modules.**

Detection. The detection sub-module needs to adopt a layered approach to converge inputs from variety of dis-similar sensors. The proposed conceptual contours of Detection sub-system of C-UAS architecture are: -

- **Sensor agnostic** mixed array of complementary sensing platforms for **maximised detection probabilities** with minimal false targets.
- **Maximise passive sensors** which are invisible to enemy and least effected by weather. It's very important for our Northern borders where the weather is generally bad and enemy has strong EW capabilities.
- **Overcome multi-vendor heterogenous sensors fusion challenges by multi-sensor and multi-app** data cum image fusion and multi-streams convergence for enhanced situational awareness to present one **Common Threat Picture**.

- **Interoperability** amongst the complete detectors array to facilitate cross sensor "**tip and cue"** procedures and with the C2 and shooter networks through standardised Application Programming Interfaces (APIs).
- All detectors must be **deployable / mobile at acceptable costs**.
- **AI enablement** for Near real time updated drone threat library. **Indigenous LLM / VLM based collation**, corroboration and analysis software with automatic "tip and cue" procedure facilitating faster decision for engagement.
- **Identification of friend and foe** with increased accuracy.
- **Drone Detection from air** is a new phenomenon to overcome ground-based LOS restrictions and signal attenuation concerns. Thus, the form factor or profile (dimensions, weight, power requirements etc) etc need to be kept in mind while placing the detection platform in air.
- **Integrate villagers, locals and veterans** as a large array of visual and acoustic sensors.
- **No drone is small enough to be ignored**.
- **Maximising passive coverage** comprehensively and mitigating dead grounds.

Location, Tracking, Monitoring, Classification and Identification. Location means acquisition of coordinates of a static position of GCS or the UAV crew while tracking requires dynamic acquisition of drone coordinates over a period of time. Similarly, Classification is confirming the drone type basically the group, manufacturer and the probable communication protocol whereas identification is physically confirming exact modem / IP address and the exact model of drone.[93] This sub-module must thus fuse inputs from variety of sensors to generate the most accurate flight track and predicted flight path of multiple drones simultaneously. Tracking of incoming drone threat not only leads to engagement of the drone by the most suitable weapon at appropriate range but must also prevent any collateral damage. An EW based engagement of resistance group's explosive laden drone by Myanmar's military had caused many casualties in Myanmar's monastery. Thus, tracking sub-module must facilitate the following: -

- AI-enabled drones' flight and battle pattern predictive analysis.

- Monitor local cellular communication networks in conjunction with local cellular companies for enhanced data usage for flying of drones by non-state actors or enemy drone operators.
- Provide regular, comprehensive and real time location updates of adversarial drones and even some own interceptor drones to be able to accurately guide them if required.
- Fully automated, with minimised human involvement to simultaneously track multitude of drones.
- Identification of type of threat and classifying it as high / low threat to ensure allocation of appropriate platform for neuralisation / destruction.
- A regularly updated adversarial and rogue drones' library with every validated OSMINT input, drones' forensics report and every C-UAS engagement cycle.
- Discard false surveillance reports or clutter.
- Enhance the accuracy of predicted position for engagement by suitable shooter.

Engagement. Every drone threat needs to be deterred by timely neutralisation / interdiction, disruption, and mitigated through hard kill options if soft kill fails. Since neutralisation mainly aims at preventing an incoming rogue drone from entering a pre-defined friendly zone, it minimises the chances of collateral damage of engagement especially over a large friendly area. A multi-dimensional drones engagement architecture thus needs to be evolved to minimise drones' intrusion and maximise their disruption by a balanced combination of assured hard and soft kills while mitigating any chance of collateral damage. A **hybrid approach converging cyber, EW and kinetic options on a single platform, whether static or mobile, is the ideal C-UAS solution**.

- **Soft Kill Options**. Net drones, Cyber take-over, Spoofing, Jamming (all varieties- fixed and mobile, SDR enabled).
- **Hard Kill Ground Based**. SAMs, AD guns, DEWs – Lasers and HPMs, Hand-held guns- AI enabled MGs, Shotguns with special C-UAS cartridges, Net guns.

- **Hard Kill Aerial Options**, Helicopter engagements, Interceptor Drones, FPV drones / Quadcopters with mounted shotguns.

Recording and Visualisation. Every data point is recorded and archived in the common data lake. The recorded data then facilitates predictive visualisation of future engagement cycles based on lessons from use cases.

Performance Analysis. It's a 24x7 real-time analysis of each sub-component to identify data poisoning and effectiveness reduction indications.

Overall Concept. Overall, the C-UAS architecture and its components must ensure the following: -

- Data lake with inbuilt DL / ML / RL to ensure the indigenous system learns with every success or failure in detection.
- Platform and sensor agnostic detection and timely engagement of every incoming drone without any collateral damage.
- Multi-domain resilience to withstand adversary's multi-domain precision strikes and have adequate redundancy.
- Scalability to integrate any additional sub-module as per progress of the operations.
- **Convergent battlespace solutions** to effortlessly integrate disparate and compartmentalised systems, platforms and data links across the complete array- military services, civil, PMF, etc; indigenous or any import; varying GIS and LLMs etc.
- **Tailor made for terrain** but yet capable of mobile deployment for any event or contingency.

Recommendations

Every conceptual primer must bring out relevant recommendations for effective implementation. Since drones in modern era maximise dual-use employment for farmers / civil world and soldiers / military, it's necessary to undertake few steps at all levels in India by the government, military, private industry and individuals. First and foremost, **India needs to enhance C-UAS training while undertaking R&D for post quantum era wherein QAI drones will dominate the battlespace**.

Immediate Implementation. **The repeated strategic threats by Pakistan's top politico-military hierarchy Army Chief Munir, Prime Minister Shahbaaz Sharif**, and Bilawal Bhutto **are surely failed attempts to scare anyone in India** but indicate clear intentions of Pakistan. With renewed **American staunch support guided by Trump 2.0, pacing Turkish drones and EW assistance, availability of Chinese military support, Pakistan Army's on ground infiltration attempts and raising of Conventional Rocket Force Command in August 2025 are clearly indicative that Operation SINDOOR 2.0 may just happen soon**. Having the possibility of mapped Indian AD and EW locations by flying 300-500 low-cost Chinese and Turkish drones every night from 7 to 10 May 2025 in Operation SINDOOR 1.0, Pakistan military will surely be better prepared for launching swarms of drones this time with more explosive content at both civilian and military places of importance unless the strategies over plans better. **Hence, the urgency of layered and resilient C-UAS architecture is real, urgent and absolute essential**. And more importantly, **the C-UAS grid needs to be part of a much larger "Sudarshan Chakra" RAAMD defence wall earliest but surely not later than 2035**.

C-UAS Solutions Against OFC FPV Drones. Many PLA propaganda videos depict them employing OFC FPV drones. With hardly any soft kill option available against them, India needs to strengthen its density of hard kill C-UAS platforms with greater focus on training of interceptor drone pilots and their selection for the task.

Legal Laws and Policies. As the usage of drones and UVs gets enhanced across the length and breadth of India, it's very necessary to streamline the legalities both for drones and C-UAS platforms like the drones' licensing / certification mechanisms, geo-

fencing software and policy framework for regulating C-UAS operations against identified rogue drones' threats. The major legal issue will come in the delineation of clear responsibilities for engagement and interception of non-cooperative / rogue UVs / drones. The C-UAS architecture legalities must be comprehensive and must address issues relating to cyber security, telecommunication, data exchange, jamming policies etc. **A strategic or operational surprise by Pakistan's sleeper cells may just be averted by immediately handling the policy restrictions imposed on C-UAS grid while not disturbing the normal functioning of civil flights**.

C-UAS Standards and Convergence. There is a need of organising an experts' committee to streamline the C-UAS standards for interoperability amongst various modules and platforms. With multitude of service based compartmentalised C2 systems, foreign imported disparate C-UAS combat platforms, development of indigenous systems, cost restrictions of more frequent use of SAMs and most importantly reliability on Chinese components, "**Systems and Platforms Convergence**" is an essential inescapable solution to stitch the C-UAS grid together.

Drones' Incident Management Cell. Without overloading the existing bureaucratic offices both within civil setup from the border villages to the national level, a Rogue Drones' Monitoring and Incident Management Cell needs to be established immediately with presence of government representatives (local / district / state / centre), police (State / CRPF / CAPF / CISF / Railways), Airport authorities/ DGCA, PMF (BSF / SSB / ITBP / Indian Coast Guard), critical infrastructure governing body (Golden Temple / Ayodhaya Temple, Nuclear Power Plants, Dams etc), Tourism spots management authorities, and most importantly military (IAF, IN, IA including RR and AR) from brigade to HQ IDS level. Even without composition of such cells, **Stakeholders' Collaboration** is extremely necessary for handing / taking over of drones' threat.

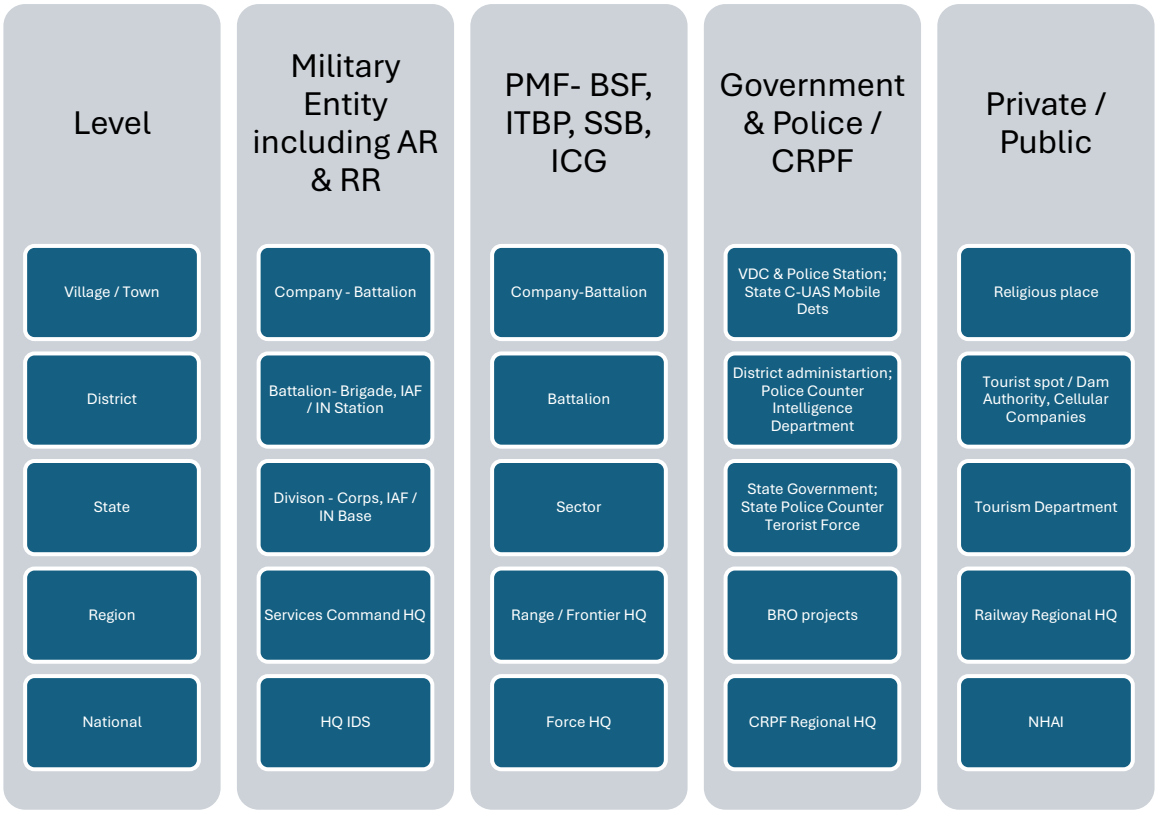

Figure 7: Drone Incidents' Monitoring Cells
(Source-Author's Research)

Public Awareness and Veterans Participation - Sparsh / Digilocker – Drones Monitoring Contact App. Ukrainians exploited its Diia digital app for connecting its authenticated civilians with the military on the e-Enemy app to pick up information about the Russian military platforms and movements. Similarly, Digilocker can be exploited like the COVID app to spread awareness of drones' threats and sounding air alerts whenever and wherever required. A similar app as e-Enemy can be developed for India for the border populace to become the largest grid of sensors sending visual and acoustic tracks of adversarial / rogue drones. A much easier approach is to provide **an additional module within the existing Sparsh app for veterans to connect 30 lakhs plus veterans in India to its alma mater – the military to convey inputs of any threat from drones-missiles-rockets etc**.

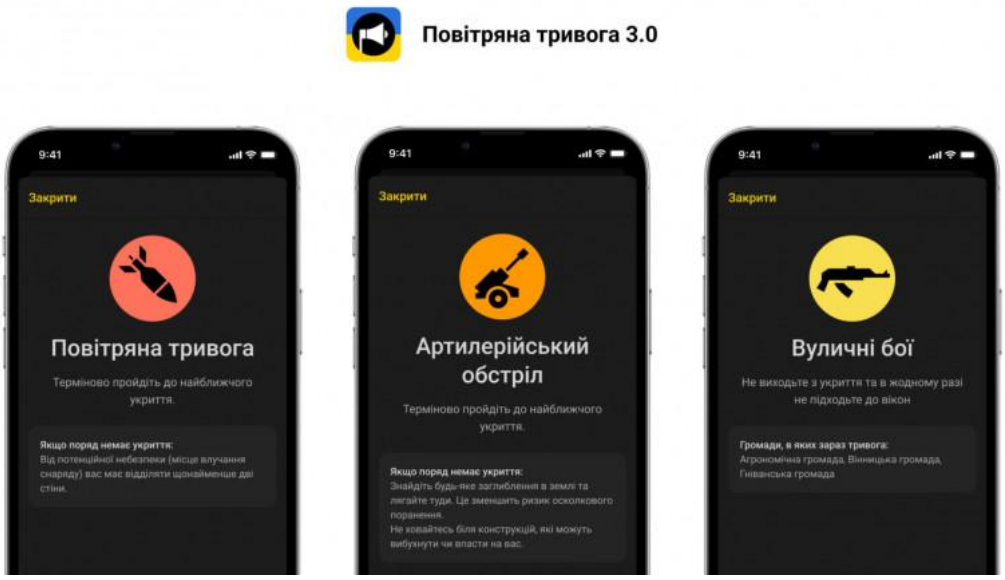

Figure 8: Ukraine's e-Enemy Software

Telangana Police, under MHA Drones Study Report has recommended that every state must have detection teams comprising citizens who[94]

> "*Must be encouraged to report drone sightings via Dial 100/Hawk- eye/ Facebook/Twitter/WhatsApp, etc. A Drone Sighting Report may include details like: Place of sighting; Time of sighting; Duration of flight; Approximate height; Physical features of drone-like colour, shape, size; Sighting of drone operator and his/her face or body features; Vehicle details if any of drone operators like make and model and colour and vehicle number of vehicle and direction of vehicle movement; make and model the drone if known; If the drone has dropped any object, then the location and size and shape, and colour of the object so dropped; Image/Video of drone flight as an attachment; map location as an attachment; sound details and description of the drone; details of citizen like name address phone number etc*".

QAI Enablement. The indigenous QAI enablement of both drones and C-UAS platforms will require incorporation of indigenous quantum technology advancements and a large number of algorithms to be written and Large Language Models (LLMs) and Visual Language Models (VLMs) to be generated. As of now, most AI firms are picking up foreign seeds to create LLMs for use in Indian drones and C-UAS ecosystem. **While the generation of completely indigenous model from scratch**

is a tedious process and requires extensive database, it needs to be undertaken. **These indigenous QAI platforms and systems will thus form the building blocks of the offensive and defensive components of Sudarshan Chakra shield.**

HR Reforms - Super Specialisation. There is a need of series of HR reforms both within defence services and academia as recommended below: -

- Drones and C-UAS must be separate Engineering specialisation with passionate youngsters getting an opportunity to learn drones in school itself or at least option for B Tech (Drones and C-UAS) with thereafter super-specialisation in M Tech in C-UAS, Drones AI Models or Drones EW or Drones Forensics etc. In addition to the IITs, the ITIs must also introduce Drone and C-UAS engineering diplomas.
- Training on drones and C-UAS must be adequately recorded and accredited for certified recognition.
- While neither Indian Army nor any service needs to create a separate force but individuals should be encouraged and incentivised for such operations and achievements. Adequate avenues exist and must be utilised for encouraging specialisation at Captain / Major and equivalent and Super-Specialisation at next level.
- Every successful C-UAS mission or training hours must earn enough recognition on lines of flight hours for aircraft pilots.
- Explosive management on board drones is slightly different from standard ordnance issues and hence suitable training must be organised.

Collaborative Drones Forensics. Due to the omnipresent nature of drones' threat, all government, semi-government, public, private, military and non-military agencies get adversely affected by enemy or rogue drones. Hence, while the conduct of drone forensics maybe related to experts, the outcome and the recommendations must be shared with all stakeholders and the indigenous C-UAS experts to develop the solutions.

After having proposed the C-UAS architecture and focussed recommendations for all stakeholders involved, the primer shall now summarise the temporally linked key steps required to be undertaken on priority.

Summary of Recommendations

The Chinese display of multitude of latest Collaborative Combat Aircrafts (CCA) UAVs in its rehearsals, for grand military parade on 03 September 2025, along with many new missiles and aircrafts and other combat platforms is a stark reminder that India needs to urgently step up its C-UAS architecture whether or not there is thaw in India-China relations. To summarise in short, a phase wise C-UAS plan needs to be unrolled at all levels immediately as a whole-of-nation approach. **Sometimes, a wrong decision is better than a delayed decision**. Hence, **with Operation SINDOOR 2.0 anytime round the corner, an effective C-UAS grid is mandatory to defeat Turkish and Chinese drones' fleets launched by Pakistan military in conjunction with its missiles and rockets.**

Phase 1 – October 2025.

- **C2**. The inter-service, inter-ministry C-UAS organisational structures or so-called "Drones Incident Management Cells" must be in place.
- **Detection and Mitigation**. The immediately scaled up production of **upgraded D4 systems after incorporating all latest advancements and deployment at all strategic locations**. **It may be more potent to share the D4 technology amongst indigenous vendors to scale up production at mass manufacturing levels**. Locally, the lowest cost but high-speed drones, even Chinese drones, should be used as interceptor drones to tackle any combat surprises. The production must happen 24x7 day and night so that more and more vulnerable entities have some C-UAS backup.
- **Sparsh App**. The Sparsh app can be immediately upgraded to incorporate inputs of our veterans spread as eyes and ears across the length and breadth of the country.

- **Academia-Industry-Military Mathan**. Like Indian literature's famous "Saagar Manthan", it's urgent that the government ensures detailed collaboration amongst the military, paramilitary, industry and academia for a common indigenous executable C-UAS solution with minimum delays overcoming all turf wars. **Adapative Collaboration and Indigenous Innovation are essential for National Survivability and Strategic Autonomy**.

Phase 2 – End 2025.

- **R&D Testing**. A high-speed interceptor drone crossing minimum 200 kmph speed be tested by multitude of indigenous firms.
- **D4 System**. With day and night surge in manufacturing capacities, D4 system should be available at all operational level civilian and military entities as far as possible.
- **Foreign Testing**. Provision of D4 C-UAS platform, Surya DEW or new C-UAS platforms to Armenia or similar countries will ensure battle-testing against adversarial drones if any drones' conflict reoccurs.
- **DAP**. Revamp DAP to prioritise indigenisation especially non-Chinese components, quality and technology scalability and then only moving to cost parameters by suitably allocating percentages.
- **Scalability**. A group of Indian companies and start-ups must be identified which can scale up and meet surge production capacities.

Phase 3 – 2026.

- **Defence Exports**. With urgent need of C-UAS platforms world over, India should identify counter-drone solutions as a pocket of excellence for enhancing defence exports. The advantages gained are significant – indigenisation, jobs creation, technological innovation, larger manufacturing base and resultant lower costs etc.
- **Comprehensive C-UAS Architecture**. With 2025 as the year of Defence Reforms nearly over, a comprehensive national C-UAS architecture must be in place by June 2026 integrating all essential elements.

- **Aerial Detection and Mitigation**. The detection array needs to be placed in air either on tethered balloons, VLEO satellites or low-cost solar-powered drones. The more assured mitigation option in the immediate period seems to be aerial mitigation by low-cost interceptor or MG mounted drones.
- **Communication Satellites Constellation**. India needs to have its own indigenous communication satellites constellation up in space to ensure 24x7 communication amongst all components of its RAAMD / C-UAS architecture. 2026 must see the launch of at least the first set of one or two such indigenous constellations.
- **TEAM BHARAT "Sudarshan Chakra" AI**. With a purely indigenously seeded LLM and VLM, an Indian AI model needs to be created by amalgamating best coders and algorithm designers to create platform agnostic AI enablement models to traverse trans-frontier zones of our adversaries effortlessly, map every equipment profile of our adversaries and obtainable terrain.

Conclusion

The famous Indian scholar's "Chanakya Niti" encouraged innovation to foster creativity by thinking out of the box and organizational adaptability for enhancing survivability. In modern non-contact kinetic battles, commercialisation and miniaturisation of small drones has imposed an urgent need on all nations to protect their population and critical assets against UAS threat by saturating and exhausting traditional AD systems. Thus, India needs to develop a comprehensive C-UAS architecture which will integrate heterogenous and disparate systems and fuse the inputs from multitude of agencies and sensors to develop a Common UAS Threat Picture. C-UAS today has become a multi-disciplinary field amalgamating EW, electro-optics, acoustics, cellular monitoring, Quantum technology, AI, ML and Robotics.

While Americans have battle-tested their RAAMD defence components of proposed 'Golden Dome' against Iran repeatedly as part of Isreal's 'Iron Dome', the Russians are testing numerous Chinese C-UAS platforms particularly the DEW varieties against

the Ukrainian drones. Russians, under Putin's clear directions to dominate the global drones' industry, have also mastered the art of rapidly prototyping Ukrainian innovative drone technological solutions at mass scales. **In fact, Trump's possible deal to incorporate Ukrainian drones for a 50 billion USD deal is a transactional deal to take advantage of Ukrainian technological and tactical advancements in drones and C-UAS domains**. While the PRC has played a key role in Russian drones and C-UAS developments particularly technological assistance and various components, it's also simultaneously assisting Iranian military and Houthi rebels, Myanmar military and the opposing resistance groups in their own drone wars. Indian defence diplomacy must also pull out few leaves to realistically test their indigenous systems and not wait for own conflicts to draw out lessons.

Interestingly as **China has been testing both drones and C-UAS technological and tactical advancements in others conflicts, the Turkish drones' companies have been closely collaborating with the opposing sides- Ukraine, American and NATO countries. Amidst this current geopolitical quagmire, Turkish and Chinese drones' advancements converge in Pakistan and even Bangladesh to great extent**. **Thus, Pakistan is in a unique opportune win-win situation** and will gain access to key technological advancements whether directly through its key allies China and Türkiye or through America directly or indirectly and even Iran. **Amidst this multi-front threat profile and unchallenged dominance of China in sUAS industry, Indian C-UAS architecture must not imitate others but must innovate with its own talent by undertaking technological leaps while strictly enforcing indigenisation. This requires persistent execution of time-bound goals, attracting internal talent and its harnessing, urgent whole-of-nation organisational convergence and restructuring by relentless crushing of turf wars, genuine doctrinal transformation with a combined-arms and joint-service and multi-force approach, and pathbreaking QAI and technological advancements based on original Indian innovative thought process. With 'Strategic Autonomy' as the corner stone of our foreign policy, 'Technological Autonomy' will be essential in the next decade for realising the 'Sudarshan Chakra' shield by 2035 and more urgently its C-UAS component at the earliest possible to decisively win SINDOOR 2.0**.

About the Author

Brigadier Anshuman Narang (Retd.) is an alumnus of the RIMC and holds the *Adani Defence Chair of Excellence on UAS Warfare & Counter-UAS* at CENJOWS. He is Founder-Director of the think tank *Atma Nirbhar Soch* and Advisor at Suhora Technologies. A China watcher, OSINT expert, and author of three books (with two more underway, including *PLA's ORBAT Compendium*), his PhD focuses on *Chinese RMA and Centennial Goals – Implications for India*.

A gunner officer, he commanded a prestigious Composite Artillery Brigade on India's Northern borders before voluntary retirement in 2024. He raised a Surveillance & Target Acquisition Regiment, and has served across India's Western front from Siachen to the South. He has attended professional military courses in the US, Australia, and Japan. Post-retirement, he continues pioneering work in OSINT, ISR, drones, space, missiles, artillery, and mechanised warfare research, and is a sought-after speaker and analyst on military technology and China.

DISCLAIMER

References

[1] Drone Shield, "C-UAS Factbook" 8th Edition, available at https://asiapacificdefencereporter.com/wp-content/uploads/2025/08/CUAS-Factbook_8th-Edition.pdf, accessed on 19 August 2025.

[2] Olena Kryzhanivska, "Stopping Shaheds: Ukraine's Solutions - Seven solutions to Shahed problem in Ukraine", 19 July 2025, available at https://ukrainesarmsmonitor.substack.com/p/stopping-shaheds-ukraines-solutions?r=1xrkiw&triedRedirect=true, accessed on 20 July 2025.

[3] MJ Augustine Vinod, Eurasian Times, "India Unveils 'Powerful' D4 Anti-Drone System; IAF Expert Explains How It Will Be A Game Changer For Military", 23 March 2025, available at https://www.eurasiantimes.com/india-unveils-powerful-d4-anti-drone-system-iaf-expert-explains-how-it-will-be-a-game-changer-for-military/, accessed on 24 March 2025.

[4] Ventasde, Seguridad, "Look to the sky: commercial drones and new security threats", 13 May 2025, available at Look to the sky: commercial drones and new security threats - Ventas de Seguridad, accessed on 15 May 2025.

[5] Harpreet Bajwa, New Indian Express, "BSF trains dogs to detect drones coming from Pakistan", 12 August 2025, available at https://www-newindianexpress-com.cdn.ampproject.org/c/s/www.newindianexpress.com/amp/story/nation/2025/Aug/12/bsf-trains-dogs-to-detect-drones-coming-from-pakistan, accessed on 12 August 2025.

[6] Dharmendra Chauhan et al, "Nation's Defense: A Comprehensive Review of Anti-Drone Systems and Strategies".

[7] Ibid.

[8] Ibid.

[9] Ibid.

[10] Ministry of Home Affairs, "Project Report on Drone: A New Age Policing Tool", Project No.13/MM:03, 2024-25, 24 October 2024, accessed on 01 May 2025.

[11] Ibid.

[12] Mark Lupton, Operational Solutions Limited, Presentation "C-UAS System– Concept and Architecture", 03 June 2025.

[13] Thomas Meuter, Stefan Nitschke and Alexander Weidmann, Narda Safety Test Solutions, "Passive drone detection by means of radio monitoring and direction finding under consideration of operational and economic conditions", Book "Drones| Systems - Operations - Prospects| The future of unmanned military aviation in Europe", available at https://www.narda-sts.com/index.php?eID=dumpFile&t=f&f=5745&dl=1&token=64dfe5a0fd3bec41de58ed14646909c53478a7e1, accessed on 01 July 2025.

[14] Vikram Mittal, Forbes, "The Challenges Of Counter-Drone Technology As Seen In Recent Conflicts", available at https://www.forbes.com/sites/vikrammittal/2023/10/18/the-challenges-of-counter-drone-technology-as-seen-in-recent-conflicts/, accessed on 01 May 2025.

[15] Ibid.

[16] EverythingRF, "MarketsandMarkets Report Explores How AI is Reshaping Radar Systems for Military & Defense", 11 August 2025, available at https://www.everythingrf.com/news/details/20602-marketsandmarkets-report-explores-how-ai-is-reshaping-radar-systems-for-military-defense, accessed on 12 August 2025.

[17] Olena Kryzhanivska, "FPV Drone Localization in Ukraine', 16 August 2025, available at https://ukrainesarmsmonitor.substack.com/p/fpv-drone-localization-in-ukraine, accessed on 16 August 2025.

[18] Ibid.

[19] Autonomous Warfare, LinkedIn post on 15 August 2025, available at https://www.linkedin.com/posts/autonomous-warfare_the-autonomous-warfare-ontology-awo-is-activity-7361603300527378432-DkaD/?rcm=ACoAAEIqhcQBymSIcWgC1pRGqWUaN5m6skwxII4, accessed on 15 August 2025.

[20] Ibid.

[21] Drone Shield, "C-UAS Factbook" 8th Edition, available at https://asiapacificdefencereporter.com/wp-content/uploads/2025/08/CUAS-Factbook_8th-Edition.pdf, accessed on 19 August 2025.

[22] Dharmendra Chauhan et al, "Nation's Defense: A Comprehensive Review of Anti-Drone Systems and Strategies", 01 April 2025, accessed on 01 May 2025.

[23] Drone Shield, "C-UAS Factbook" 8th Edition.

[24] Mark Lupton, Operational Solutions Limited, Presentation "C-UAS System– Concept and Architecture", 03 June 2025, available at https://www.eurocontrol.int/sites/default/files/2025-06/20250603-best-practices-cuas-lupton-eurocae.pdf, accessed on 04 June 2025.
[25] Jugapro, Whitepaper on "Counter-Drone Solutions", accessed on 01 August 2025.
[26] Ibid.
[27] Dharmendra Chauhan et al, "Nation's Defense: A Comprehensive Review of Anti-Drone Systems and Strategies".
[28] Mark Lupton, Operational Solutions Limited, Presentation "C-UAS System– Concept and Architecture", 03 June 2025.
[29] Ibid.
[30] Drone Shield, "C-UAS Factbook" 8th Edition.
[31] Ibid.
[32] Jugapro, Whitepaper on "Counter-Drone Solutions", accessed on 01 August 2025.
[33] Vikram Mittal, Forbes, "The Challenges Of Counter-Drone Technology As Seen In Recent Conflicts".
[34] EverythingRF, "MarketsandMarkets Report Explores How AI is Reshaping Radar Systems for Military & Defense".
[35] Jugapro, Whitepaper on "Counter-Drone Solutions".
[36] Ibid.
[37] Mark Lupton, Operational Solutions Limited, Presentation "C-UAS System– Concept and Architecture", 03 June 2025.
[38] Thomas Meuter, Stefan Nitschke and Alexander Weidmann, Narda Safety Test Solutions, "Passive drone detection by means of radio monitoring and direction finding under consideration of operational and economic conditions", Book "Drones| Systems - Operations - Prospects| The future of unmanned military aviation in Europe", available at https://www.narda-sts.com/index.php?eID=dumpFile&t=f&f=5745&dl=1&token=64dfe5a0fd3bec41de58ed14646909c53478a7e1, accessed on 01 July 2025.
[39] Jugapro, Whitepaper on "Counter-Drone Solutions".
[40] Ibid.
[41] Mark Lupton, Operational Solutions Limited, Presentation "C-UAS System– Concept and Architecture", 03 June 2025.
[42] Harpreet Bajwa, New Indian Express, "BSF trains dogs to detect drones coming from Pakistan", 12 August 2025, available at https://www-newindianexpress-com.cdn.ampproject.org/c/s/www.newindianexpress.com/amp/story/nation/2025/Aug/12/bsf-trains-dogs-to-detect-drones-coming-from-pakistan, accessed on 12 August 2025.
[43] Jugapro, Whitepaper on "Counter-Drone Solutions".
[44] Ibid.
[45] Dharmendra Chauhan et al, "Nation's Defense: A Comprehensive Review of Anti-Drone Systems and Strategies".
[46] Gerhard Berz, "Disrupting Threats (GNSS RFI) Mastering the Skies: Best Practices in C-UAS Strategies Session on Counter UAS Initiatives and Solutions", 03 June 2025, available at https://www.eurocontrol.int/sites/default/files/2025-06/20250603-best-practices-cuas-berz-eurocontrol.pdf, accessed on 04 June 2025.
[47] Ibid.
[48] Ibid.
[49] Gerhard Berz, "Disrupting Threats (GNSS RFI) Mastering the Skies: Best Practices in C-UAS Strategies Session on Counter UAS Initiatives and Solutions".
[50] Andreas Ernst, Presentation "Counter-UAS - Fortifying the Airspace for Civil and Military Airports", available at https://www.eurocontrol.int/sites/default/files/2025-06/20250603-best-practices-cuas-ernst-rheinmetall.pdf, accessed on 04 June 2025.
[51] Vikram Mittal, Forbes, "The Challenges Of Counter-Drone Technology as Seen in Recent Conflicts".
[52] Jugapro, Whitepaper on "Counter-Drone Solutions".
[53] Drone Shield, "C-UAS Factbook" 8th Edition, available at https://asiapacificdefencereporter.com/wp-content/uploads/2025/08/CUAS-Factbook_8th-Edition.pdf, accessed on 19 August 2025.
[54] Ibid.
[55] Justin Nerdrum, LinkedIn post on 15 August 2025, available at https://www.linkedin.com/posts/jenerdrum_v-corps-just-battle-tested-30-counter-drone-activity-

7361879304739180544-9-oX/?rcm=ACoAAEIqhcQBymSIcWgC1pRGqWUaN5m6skwxIl4, accessed on 15 August 2025.

[56] Moshe Baum, LinkedIn post July 2025, available at https://www.linkedin.com/posts/moshebaum_counter-uas-space-is-red-hot-and-there-are-activity-7353151736125018112-bSeH/?rcm=ACoAAEIqhcQBymSIcWgC1pRGqWUaN5m6skwxIl4, accessed on 28 July 2025.

[57] Ibid.

[58] Jugapro, Whitepaper on "Counter-Drone Solutions".

[59] Vikram Mittal, Forbes, "The Challenges Of Counter-Drone Technology As Seen In Recent Conflicts".

[60] Drone Shield, "C-UAS Factbook" 8th Edition.

[61] Jugapro, Whitepaper on "Counter-Drone Solutions", accessed on 01 August 2025.

[62] Maheera Munir, "The Future Trajectory of Pakistan-China Multi-domain Cooperation", 15 August 2025, available at https://defensetalks.com/the-future-trajectory-of-pakistan-china-multi-domain-cooperation/, accessed on 15 August 2025.

[63] Olena Kryzhanivska, "Stopping Shaheds: Ukraine's Solutions - Seven solutions to Shahed problem in Ukraine".

[64] Autonomous Warfare, LinkedIn post on 15 August 2025, available at https://www.linkedin.com/posts/autonomous-warfare_the-autonomous-warfare-ontology-awo-is-activity-7361603300527378432-DkaD/?rcm=ACoAAEIqhcQBymSIcWgC1pRGqWUaN5m6skwxIl4, accessed on 15 August 2025.

[65] Dharmendra Chauhan et al, "Nation's Defense: A Comprehensive Review of Anti-Drone Systems and Strategies".

[66] Royca@GrandpaRoy2, X-post 18 August 2025 at 6:36 PM, available at https://x.com/GrandpaRoy2/status/1957428853640675627, accessed on 18 August 2025; Instagram account "drone_wars_", post on 20 August 2025, available at https://www.instagram.com/p/DNirqCAsZr2/?igsh=MXB4eDVoM3RvbmhqNQ%3D%3D, accessed on 20 August 2025.

[67] Royca@GrandpaRoy2, X-post 18 August 2025 at 6:36 PM, available at https://x.com/GrandpaRoy2/status/1957428853640675627, accessed on 18 August 2025; Instagram account "drone_wars_", post on 20 August 2025, available at https://www.instagram.com/p/DNirqCAsZr2/?igsh=MXB4eDVoM3RvbmhqNQ%3D%3D, accessed on 20 August 2025.

[68] Olena Kryzhanivska, "Stopping Shaheds: Ukraine's Solutions - Seven solutions to Shahed problem in Ukraine".

[69] Andreas Ernst, Presentation "Counter-UAS - Fortifying the Airspace for Civil and Military Airports", available at https://www.eurocontrol.int/sites/default/files/2025-06/20250603-best-practices-cuas-ernst-rheinmetall.pdf, accessed on 04 June 2025.

[70] Jugapro, Whitepaper on "Counter-Drone Solutions".

[71] Dharmendra Chauhan et al, "Nation's Defense: A Comprehensive Review of Anti-Drone Systems and Strategies".

[72] NextGenDefense, "US Navy Turns to AI to Plan Drone Swarm Missions", 28 June 2025, available at https://nextgendefense.com/us-navy-ai-drone-missions/, accessed on 01 July 2025.

[73] Dharmendra Chauhan et al, "Nation's Defense: A Comprehensive Review of Anti-Drone Systems and Strategies".

[74] Justin Nerdrum, LinkedIn post on 15 August 2025, available at https://www.linkedin.com/posts/jenerdrum_v-corps-just-battle-tested-30-counter-drone-activity-7361879304739180544-9-oX/?rcm=ACoAAEIqhcQBymSIcWgC1pRGqWUaN5m6skwxIl4, accessed on 15 August 2025.

[75] Drone Shield, "C-UAS Factbook" 8th Edition.

[76] Ibid.

[77] Ibid.

[78] Ibid.

[79] Ministry of Home Affairs, "Project Report on Drone: A New Age Policing Tool", Project No.13/MM:03.

[80] Bharat Electronics Limited (BEL), "Anti-Drone system", available at https://bel-india.in/product/anti-drone-system/, accessed on 15 August 2025.

[81] MJ Augustine Vinod, Eurasian Times, "India Unveils 'Powerful' D4 Anti-Drone System; IAF Expert Explains How It Will Be A Game Changer For Military", 23 March 2025.

[82] Ibid.
[83] Ibid.
[84] Ibid.
[85] Ibid.
[86] Times of India, "In a first, India uses laser-based weapon to shoot down aircraft, missiles and drones; joins select list of countries that have capability", 13 April 2025, available at https://timesofindia.indiatimes.com/india/watch-in-a-first-india-uses-laser-based-weapon-to-shoot-down-aircraft-missiles-and-drones-joins-select-list-of-countries-that-have-capability/articleshow/120253421.cms, accessed on 14 April 2025.
[87] Raghav Patel, "DRDO Plans to Develop 300kW 'Surya' Directed-Energy Laser Weapon with 20km Range by 2027, Designed to Neutralize Modern Aerial Threats", 13 April 2025, available at https://defence.in/threads/drdo-plans-to-develop-300kw-surya-directed-energy-laser-weapon-with-20km-range-by-2027-designed-to-neutralize-modern-aerial-threats.13697/, accessed on 14 April 2025.
[88] Olena Kryzhanivska, "Stopping Shaheds: Ukraine's Solutions - Seven solutions to Shahed problem in Ukraine".
[89] Ibid.
[90] Ibid.
[91] Ibid.
[92] Ibid.
[93] Drone Shield, "C-UAS Factbook" 8th Edition.
[94] Ministry of Home Affairs, "Project Report on Drone: A New Age Policing Tool", Project No.13/MM:03.