Taming the Skies: Managing the Unmanned Airspace and Countering Rogue Drones

Col. Vikrant S Shinde

Takshashila Discussion Document - 2025-12
Version 1.0, June 2025

Unmanned Aircraft Systems (UAS) and the manned aviation sector operate in a shared airspace. It is imperative to understand the evolving architecture for managing the UAS airspace, including the organisational structures for assessing risks and evaluating emerging threats, particularly from rogue drones. This document assesses the threats posed by rogue drones and the challenges in implementing regulatory frameworks in this sector and presents recommendations for a networked national Counter-Unmanned Aircraft System (C-UAS) grid.

Recommended Citation:
Vikrant S Shinde, "Taming the Skies: Managing the Unmanned Airspace and Countering Rogue Drones", Takshashila Discussion Document No. 2025-12, June 2025, The Takshashila Institution.

Executive Summary

- The rapidly evolving Unmanned Aircraft System (UAS) or drone ecosystem presents novel opportunities and threats.
- Frameworks regulating UAS operations in Very Low-Level (VLL) airspace can be found in the Drone Rules 2021 and the National Unmanned Aircraft System Traffic Management Policy Framework.
- A networked Counter-UAS (C-UAS) grid, concurrent with the Unmanned Traffic Management System (UTMS), is necessary to plug the gaps in the current air defence coverage, which is oriented towards aerial threats in the higher airspace.
- The key is to optimise regulatory provisions to distinguish compliant users from non-compliant ones, and then employ the C-UAS grid to neutralise the rogue drone threat.

This document has been formatted to be read conveniently on screens with landscape aspect ratios. Please print only if absolutely necessary.

Author
Col. Vikrant S Shinde is a Research Fellow in the Defence Fellowship Programme at The Takshashila Institution.

Acknowledgments
The author would like to thank Aditya Ramanathan and Ashwin Prasad for their valuable comments and feedback.

Table of Contents

I. Introduction

The Unmanned Aircraft Systems (UAS)[1] industry is evolving rapidly into a dynamic ecosystem. The industry began as a military enterprise, with drones being developed for intelligence, surveillance and reconnaissance (ISR) and targeting. It has since evolved to encompass multiple use cases spread over a broad technology spectrum, from low-cost consumer products to high-cost platforms for specialised applications. According to one estimate, the worldwide commercial drone market growth was valued at $8.77 billion in 2022, and is projected to grow from USD 10.98 billion in 2023 to USD 54.81 billion by 2030, at a CAGR of 25.82%.[2]

As per an analysis by the Institute of Economy and Peace, between 2018 and 2023, the number of states using drones rose from 16 to 40 (150% increase), while the number of non-state groups using drones rose from six to 91, an increase of over 1,400 % cent.[3]

UAS and the manned aviation sector operate in a shared airspace. Therefore, it is imperative to understand the evolving architecture for managing the UAS airspace, including the organisational structures for assessing risks, evaluating emerging threats, and countering rogue drones. The overall objective is to regulate the legitimate users of the UAS ecosystem while mitigating security threats from rogue drones.

This document assesses the threats posed by rogue drones and challenges in implementing regulatory frameworks for the UAS sector, and makes

Scope

The paper will be structured in three parts: -

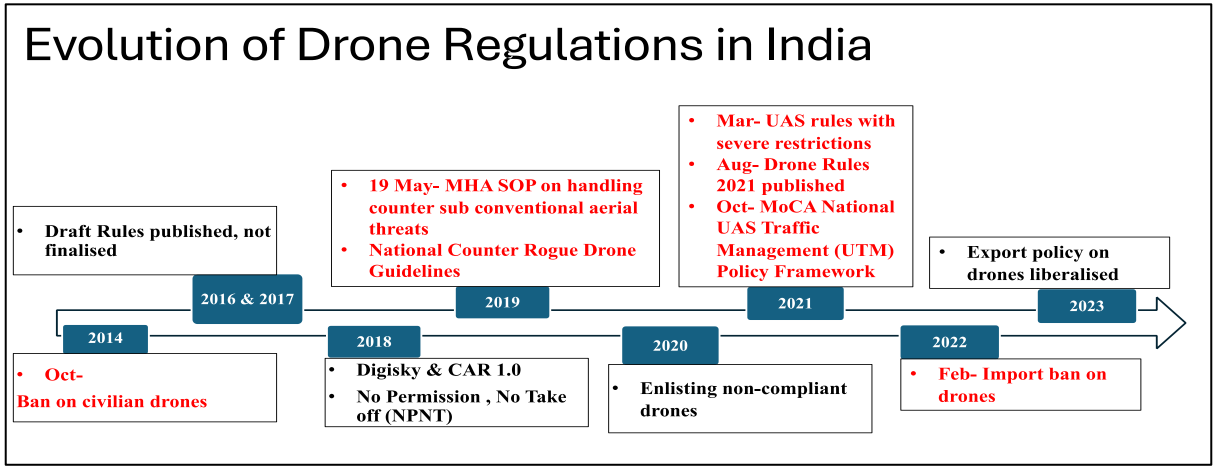
- Part one dwells into understanding the regulatory frameworks for UAS Operations & Unmanned Traffic Management (UTM).
- Part two examines the limitations of the current Air Defence cover, and an assessment of threats posed by UAS.
- Part three covers the capabilities and limitations of C-UAS Systems and proposes a C-UAS architecture.

recommendations for a networked national Counter-Unmanned Aircraft System (C-UAS) grid.

II. Understanding the regulatory frameworks for UAS Operations & Unmanned Traffic Management (UTM)

India's foray into regulating drone operations began with a blanket ban on the use of drones by non-government entities, organisations, and individuals, which was imposed by the Directorate General of Civil Aviation (DGCA) in October 2014.

Fortunately, the subsequent evolutionary progress around regulating the drone ecosystem shows evidence of constructive participation and interaction between 'Samaj-Sarkar-Bazar', and a promising commitment amongst all stakeholders to continue with the trend. Figure 1 below, adapted from a presentation by Shri Piyush Srivastava (Senior Economic Advisor to the Ministry of Civil Aviation) and updated with additional inputs, indicates the evolutionary trajectory of regulatory frameworks for Drone operations in India.[4]



Evolution of Drone Regulations in India

2014
- Oct-
Ban on civilian drones

2016 & 2017
- Draft Rules published, not finalised

2018
- Digisky & CAR 1.0
- No Permission , No Take off (NPNT)

2019
- 19 May- MHA SOP on handling counter sub conventional aerial threats
- National Counter Rogue Drone Guidelines

2020
- Enlisting non-compliant drones

2021
- Mar- UAS rules with severe restrictions
- Aug- Drone Rules 2021 published
- Oct- MoCA National UAS Traffic Management (UTM) Policy Framework

2022
- Feb- Import ban on drones

2023
- Export policy on drones liberalised

Figure 1. Evolution of Regulatory Frameworks for UAS & C- UAS Operations in India.

II.I. Drone Rules 2021

Fundamentals of the Regulatory Framework. The fundamentals of the regulatory framework are to ensure a smooth, safe, and secure commercial operations environment for drones in India. This includes categorising drones for shared understanding, and dynamic zoning of operational airspace into mutually segregated airspaces to manage operations and regulate operators and providers of allied support services.

The iterative process of formalising a regulatory framework began with successive draft rules released in April 2016 and November 2017, Civil Aviation Requirements (CAR 1.0) in 2018, followed by draft rules in Mar and July 2021.[5] The final framework was promulgated as the Drone Rules 2021 in August 2021.[6] The Drone Rules 2021 apply to the following: -

"*(a) all persons owning or possessing, or engaged in leasing, operating, transferring or maintaining an unmanned aircraft system in India;*

(b) all unmanned aircraft systems that are registered in India; and

(c) all unmanned aircraft systems that are being operated for the time being, in or over India.

The provisions of the Aircraft Rules, 1937 shall not apply to unmanned aircraft systems except in case of an unmanned aircraft system with a maximum all-up weight of more than 500 kilograms.

These rules shall not apply to an unmanned aircraft system belonging to, or used by, the naval, military or air forces of the Union of India."[7] [Emphasis added]

The drone rules converge with the broad principles enunciated by the International Civil Aviation Organisation (ICAO), which is a United Nations agency helping 193 countries to cooperate and share their skies for their mutual benefit.[8] The ICAO has proposed a UAS toolkit to assist states in realising effective UAS operational guidance and safe domestic operations, considering public and aviation safety first, concurrent with security and privacy protection, while promoting industry.[9]

There are three key pillars of the Indian Drone ecosystem, defined by the Ministry of Civil Aviation, around which policy formulation has evolved.

a) Ease of doing business, under which licensing and certification norms have been simplified. Digisky app is being leveraged to streamline the UAS operational processes through an Application Programming Interface (API).[10]

b) Financial incentives including Performance-Linked Incentives (PLI) for drone and drone components manufacturing, with a budget of INR 120 Cr from FY 2022-23 to FY 2024-25.[11]

c) Promotion of domestic industry, which hinges on an import ban on Completely Built Units (CBU), Semi Knock Down (SKD) and Completely Knock Down (CKD) drones. Drone components and drones for R&D and security and defence are exempted from the ban.[12] The policy also emphasises the role of the government as a marketplace for propelling demand and promoting exports.

II.II. Categorisation of Drones

According to the Drone Rules 2021, the UAS are categorised into three types, as explained and depicted below.[13]

a) An aeroplane is a power-driven (heavier-than-air) aircraft machine deriving support for its lift in flight chiefly from aerodynamic reactions on surfaces that remain fixed under given flight conditions.

b) Rotorcraft means an aircraft supported in flight by the reactions of the air on one or more power-driven rotors on substantially vertical axes.

c) Hybrid UAS means an unmanned aircraft capable of vertical take-off and landing. It depends principally on power-driven lift devices or engine thrust for lift during the flight take off/ landing and non-rotating airfoil for lift during horizontal flight.

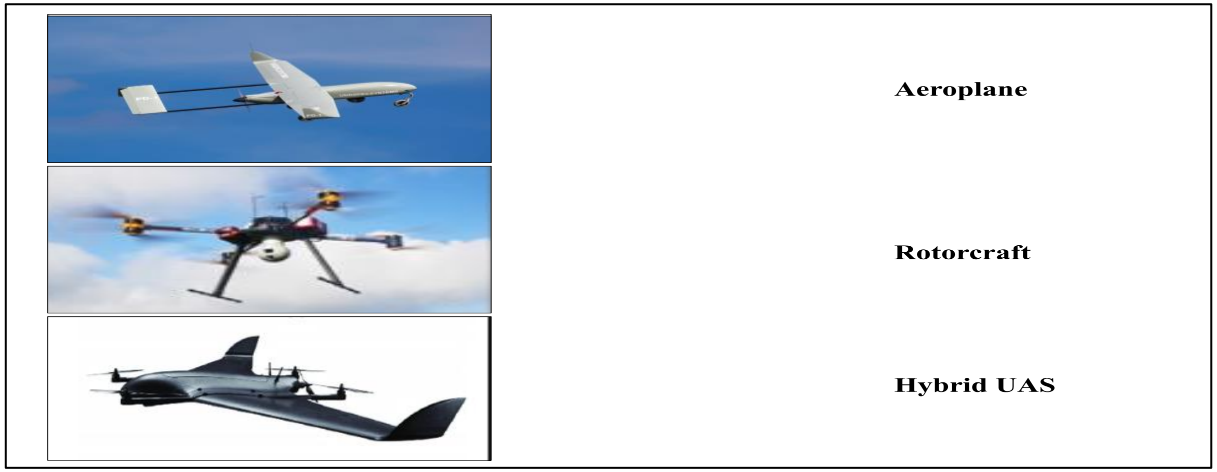


Figure 2. Categories of UAS. (Image credits Sun et al. (2023). UAV Platforms for Data Acquisition and Intervention Practices in Forestry: Towards More Intelligent Applications. Aerospace. 10. 317. 10.3390/aerospace10030317 and https://www.dronetrest.com/t/classification-of-drones-unmanned-aircraft-systems-unmanned-aerial-vehicles/9835)

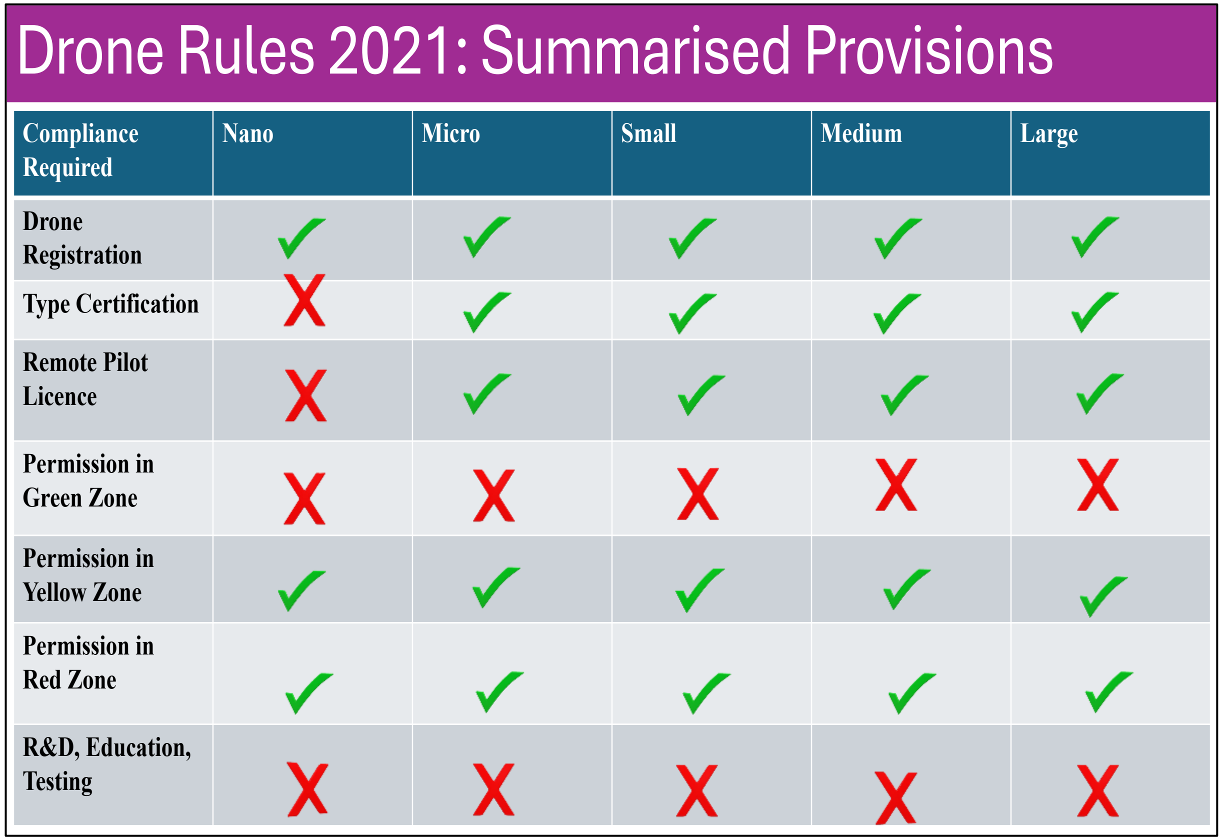
Each of the above categories is further sub-divided into three sub-categories based on the piloting arrangements, command and control (C2) links and purpose as follows: -

a) Remotely piloted aircraft system.
b) Model remotely piloted aircraft system.
c) Autonomous unmanned aircraft system.

UAS are classified based on maximum all-up weight, including payload. The regulatory requirements for each class of UAS are as per the graphic below.[14]

a) Nano	(<= 250 gms)
b) Micro	(>250gms, <= 2 Kg)
c) Small	(>2 Kg, <= 25 Kg)
d) Medium	(>25 Kg, <= 150 Kg)
e) Large	(> 150 kg)

All classes of UAS, except Nano UAS, are mandated to undergo all certifications and obtain permission for operations. A Nano UAS is exempted from type certification and remote pilot licensing due to its limited all-up weight and minimal disruptive potential. No permission is required for UAS operations in the Green zones.



Drone Rules 2021: Summarised Provisions

Compliance Required	Nano	Micro	Small	Medium	Large
Drone Registration	✓	✓	✓	✓	✓
Type Certification	X	✓	✓	✓	✓
Remote Pilot Licence	X	✓	✓	✓	✓
Permission in Green Zone	X	X	X	X	X
Permission in Yellow Zone	✓	✓	✓	✓	✓
Permission in Red Zone	✓	✓	✓	✓	✓
R&D, Education, Testing	X	X	X	X	X

Figure 3. Summarised Provisions for Applicability of Certifications and Permissions to Classes of UAS.[13]

Classification by Ministry of Home Affairs (MHA). While the above classification is used for commercial UAS, the MHA classifies Remotely Piloted Aircraft Systems (RPAS) used by Defence services, or whose use can be restricted by DGCA, based on range and endurance as tabulated below: -

S No	Type	Operating Range	Operating Altitude	Endurance
(a)	Long Endurance RPAS • High Altitude Long Endurance (HALE) • Medium Altitude Long Endurance (MALE)	>200 km	Beyond 35000 ft Below 35000 ft	>24 hours
(b)	Tactical RPAS • Medium Range • Short Range • Mini RPAS (AUW 1- 20 Kg) • Micro UAS (palm sized)	Upto 200 Km 100 - 200 Km Upto 100 Km		Upto 2 hours Upto 1 hour

Table 1. Classification of RPAS

II.III. Classification of Airspace and Dynamic Zoning

Airspace for aviation purposes is divided into two categories: controlled and uncontrolled airspace. Controlled airspace encompasses five different classifications (A, B, C, D and E), with specified altitude ranges under which Air Traffic Control (ATC) service is available.

Uncontrolled airspace is the Class G airspace, a part of general airspace, which the ATC has no responsibility or authority to control.[15] Commercial UAS are mandated to use the uncontrolled Class G airspace with no ATC services and, therefore, need to be regulated for safe, secure, and seamless UAS operations.

Concepts in Airspace Management. Four conceptual choices that can be made while defining this space are depicted in the graphic below.[16] The four concepts are based on progressive restrictions on degrees of freedom in movement through air. An object in the air can move in four degrees of freedom i.e. two in the horizontal plane, forward/backwards or sideways, third being varying speeds and fourth varying altitudes. These four concepts are explained below.

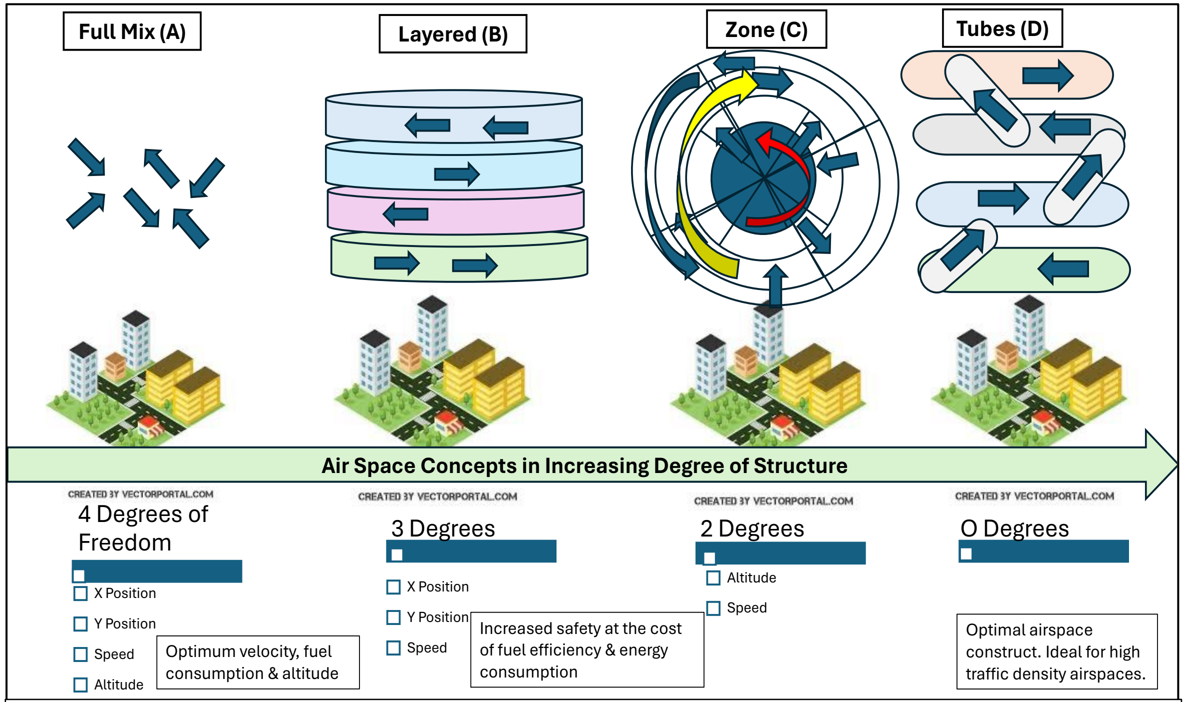

Full Mix (A)
Layered (B)
Zone (C)
Tubes (D)
Air Space Concepts in Increasing Degree of Structure
CREATED BY VECTORPORTAL.COM
4 Degrees of Freedom
□ X Position
□ Y Position
□ Speed
□ Altitude
Optimum velocity, fuel consumption & altitude
CREATED BY VECTORPORTAL.COM
3 Degrees
□ X Position
□ Y Position
□ Speed
Increased safety at the cost of fuel efficiency & energy consumption
CREATED BY VECTORPORTAL.COM
2 Degrees
□ Altitude
□ Speed
CREATED BY VECTORPORTAL.COM
O Degrees
Optimal airspace construct. Ideal for high traffic density airspaces.

Figure 4. Airspace Management Concepts.[16]

a) **Concept A (Full Mix).** This concept allows all four degrees of freedom and, therefore, is the most complex model for airspace management. This model, however, results in optimal velocity, fuel consumption, and altitude in operations. This may be useful for the management of low-traffic density airspace. This arrangement is suitable for airspace management over vast agricultural, rural areas with low population densities, less susceptible to collateral impact.

b) **Concept B (Layered).** This concept divides the airspace into layers by altitude, and within a layer (altitude being fixed), only three degrees of freedom are allowed i.e. freedom of movement in the horizontal plane and varying speeds. This leads to increased safety, albeit at the cost of fuel efficiency and energy consumption. This model can be adopted by the military for managing drones and rotary wing operations.

c) **Concept C (Zone).** This divides the airspace into radials like ring roads in an urban township. The UAS can travel clockwise or anticlockwise in a particular ring and radially travel inbound or outbound in fixed radials. Only two degrees of freedom, altitude and speed, are allowed. This model could be used by a vertiport in an urban setting.

d) **Concept D- Tubes**. This concept allows zero degrees of freedom. Tubular airspaces, like airspace tunnels, are earmarked at different altitudes and allotted to the flights. These are interconnected at the nodes for inter-tubular movement to ascend or descend between the tubular airspaces. The aircraft's speed increases with the increase in altitude of successive tubes. All flights within the same layer or tube are expected to travel at the same altitude, direction, and speed at recommended space-time routes. This is the most strictly regulated airspace management concept and is ideal for high-traffic density urban settings serviced by multiple UAS service providers.

While establishing airspace management protocols, the traffic management authority can select any one of the concepts, or even a hybrid model can be adopted. The hybrid airspace management model proposed by Drone Rules 2021 is diagrammatically depicted below.[17]

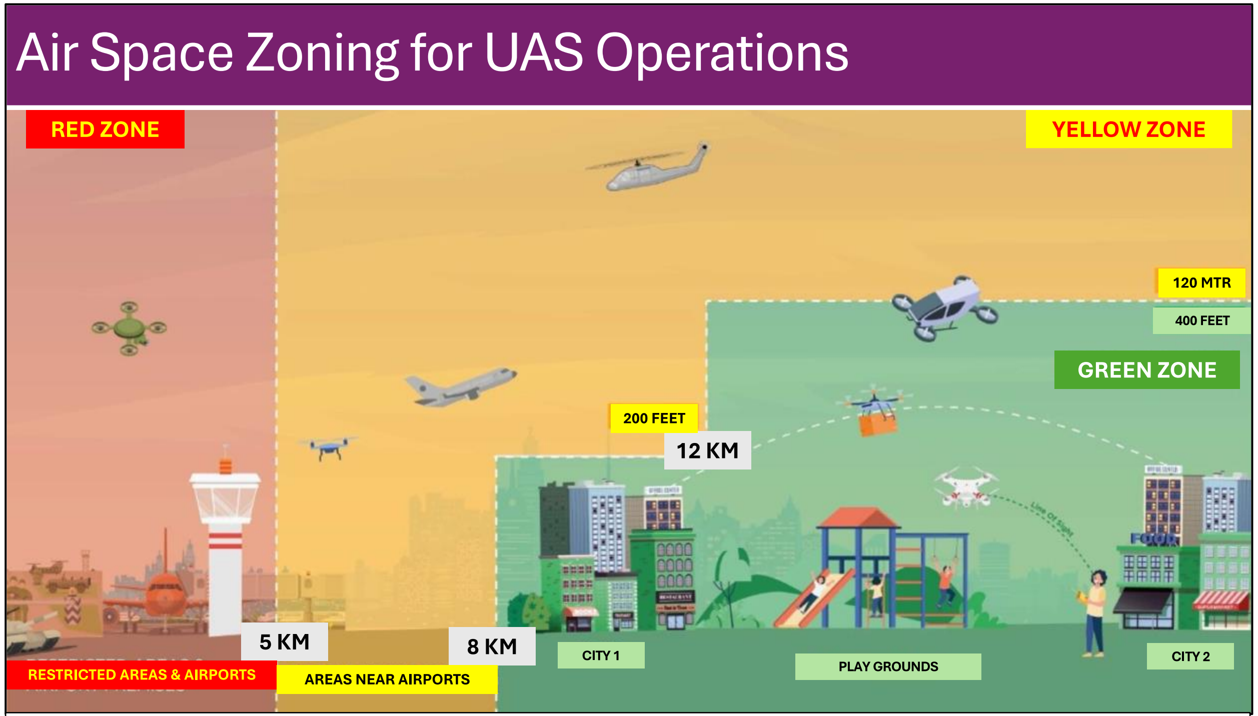


Figure 5. Airspace Zones for Drone Operations.[17] Graphic credits.[17]

In this model, the airspace is dynamically segregated into Green, Yellow and Red zones as defined in the drone regulations, with the defining features tabulated below. An appropriate airspace management concept can be adopted for UAS operations in each zone.

Zone	Defining Features[18]
Green Zone	• Operating altitude up to 400 feet /120 meters above land or territorial waters. • Area NOT designated as red or yellow zone in UAS airspace map. • Vertical space of 200 feet/60 meters above the lateral space between 8 km to 12km from perimeter of an operational airport.
Yellow Zone	• Vertical space above 400 feet/ 120 meters above the green zone or 200 feet/ 60 meters above land/ territorial waters defined by notification within which UAS operations are restricted and permission from the ATC authority is required.
Red Zone	• Airspace of a defined dimension over land or territorial waters notified by the Central government within which UAS operations are prohibited and require sanction of the Central government.

Agencies can dynamically change an area's status from one type to another by notifying it on the Digisky airspace map. The change in status takes effect seven days after notification. In emergencies, an officer not below the rank of a Superintendent of Police can notify a temporary Red Zone updated on the Digisky map. However, a temporary Red zone cannot be permitted for longer than 96 hours at a stretch.

A protocol of 'No Permission, No Take off (NPNT)' is in place for UAS operations in the Red and Yellow zones. Any violation of Drone Rules can incur a penalty not exceeding one lakh rupees and the cancellation of licences.

II.IV. Mandated Compliance Measures

The drone rules mandate four types of compliances to regulate the UAS ecosystem. These apply to UAS operators, remote pilots, training organisations and subsidiary service providers. They are passive measures for ensuring safe and secure participation in UAS operations, with accountability devolved to the participants in the ecosystem. Compliance itself acts as a filter for threat assessment.

a) **Type Certification of UAS**. As per Drone Rules 2021, a UAS without a type certificate cannot be operated in India. Model and Nano UAS are exempted from type certification. No type certification is required for manufacturing or importing a UAS. Type certification by DGCA is based on quality assessment carried out under the Quality Council of India. Directorate General of Foreign Trade or Central Government authorised entities regulate the import of UAS. An exhaustive type certification process evaluates ten aspects of a UAS, which include general requirements, performance, power plant, structure, material and construction, data link, secure flight module and tracking mechanism, instruments and equipment, qualification testing, and documentation.[19] This ensures quality specifications are maintained and any security concerns with a non-exempt UAS deployed in the Indian UAS ecosystem are addressed.

b) **Registration of UAS**. The Drone Rules 2021 make it mandatory for a UAS user to register the UAS on the Digisky app and get a Unique Identification Number (UIN). The UIN is linked to the unique serial number provided by the manufacturer and the unique serial numbers of its flight control module and remote pilot station, which must be updated whenever a change occurs. Transfer of UAS to another person or operator and deregistration are also compulsorily to be updated on Digisky. 30 November 2021 was laid down as the cutoff date for registration of UAS possessed before Drone Rules 2021. Currently, 91 type-certified, 646 non-type certified (enlisted), and 3973 non-type certified nano and model UAS are registered on the Digisky app.[20] The Digisky app maintains a library of all registered users, which law enforcement agencies can access. This is similar to the vehicle registration process. This regulation enables tracing back a UAS to its owner and pilot.

c) **Remote Pilot Licensing**. Drone Rules 2021 requires a UAS pilot to be registered on the Digisky platform. The eligibility criteria for a remote pilot licence include age between 18 and 65 years, minimum education qualification of matriculation from a recognised board, and training certification from a DGCA-approved organisation. The licence is valid for ten years, after which it can be renewed. No remote pilot licence is required to operate Nano and Micro drones for non-commercial purposes. 12,229 remote pilot licences have been recorded on the Digisky app as of 14 January 2025.[21] This streamlines the entry of remote pilots into the UAS ecosystem through a formal process.

d) **Registration of Remote Pilot Training Organisations**. DGCA has set mandatory, physically-verifiable requirements for registering organisations that train remote pilots. The training organisations have to abide by the training syllabus mandated by DGCA, including practical training requirements. The training organisations are integrated into Digisky, and are an integral part of the time-bound processing of remote pilot licences. One hundred and fifty-two training organisations are registered on the Digisky platform as of 14 January 2025.[22] This ensures that untrained, unlicenced remote pilots do not become a part of the UAS ecosystem.

II.V. UAS Traffic Management (UTM)

The uncontrolled airspace designated for UAS operations is not serviced by Air Traffic Control (ATC), except by providing flight information services about manned flights. UAS flight plans were not subjected to an ATC clearance until Drone Rules 2021, wherein dynamic zoning arrangements were notified. A rapidly expanding UAS ecosystem, therefore, makes it imperative that a UAS Traffic Management System (UTMS) is brought into service as soon as possible to manage this space. Mr Amber Dubey, the

Chairperson of the National UTM Committee, summarised India's aspirations from its UTMS,

"*The number of unmanned aircraft operating in the Indian Airspace is expected to increase manifold. The interplay between manned and unmanned aircraft has to be managed with utmost attention to global safety norms. India's UAS Traffic Management system shall play a vital role in doing so.*"[23]

The national UTM policy framework[24] defines the mechanism and architecture for managing the UAS operating space – called the Very Low Level (VLL) airspace, up to an altitude of 1000 feet above ground level. The policy's threefold objectives are seamless communication between identified stakeholders, the ability to separate a given UAS from other manned and unmanned aircraft, and the provision of real-time situational awareness of the VLL airspace to all stakeholders.

UTM Stakeholders. The key UTM stakeholders identified by the policy are given below[25] and their roles are at Appendix A.

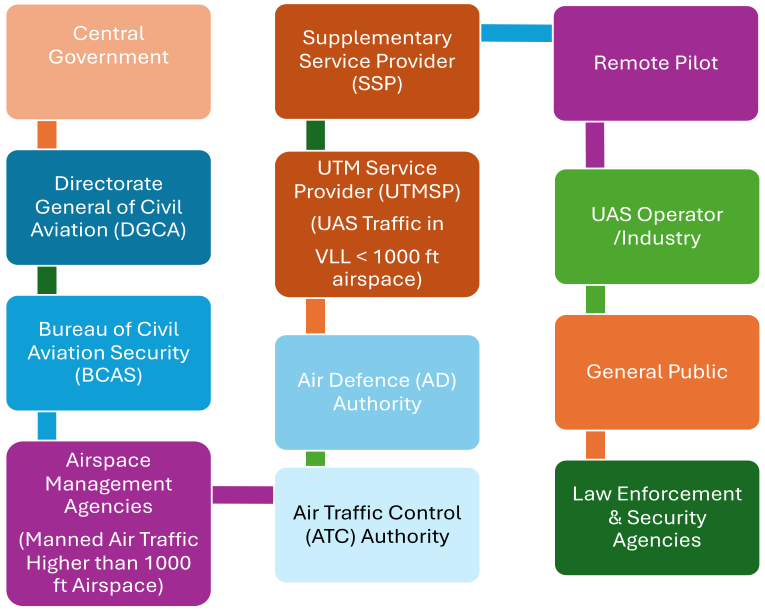

Central Government
Directorate General of Civil Aviation (DGCA)
Bureau of Civil Aviation Security (BCAS)
Airspace Management Agencies (Manned Air Traffic Higher than 1000 ft Airspace)
Supplementary Service Provider (SSP)
UTM Service Provider (UTMSP) (UAS Traffic in VLL < 1000 ft airspace)
Air Defence (AD) Authority
Air Traffic Control (ATC) Authority
Remote Pilot
UAS Operator /Industry
General Public
Law Enforcement & Security Agencies

Figure 6. Unmanned Traffic Management Stakeholders.[25] Graphic by author.

UTM Architecture. As highlighted in the National UTM Policy Framework 2021, the UTM ecosystem is envisioned as "*a collaborative extension of the current ATM [Air Traffic Management] services, but for unmanned aircraft in airspaces where such ATM services currently either do not exist or are not adequate to handle the expected volume of unmanned aircraft traffic.*"[26]

The architecture design is required to ride on a highly-automated, digitally-shared, software-based model, riding on secure datalinks, with a layered need-to-know approach to information sharing, and data exchange with minimal dependence on voice communications. The architecture envisioned in the national framework document is discussed below.[27]

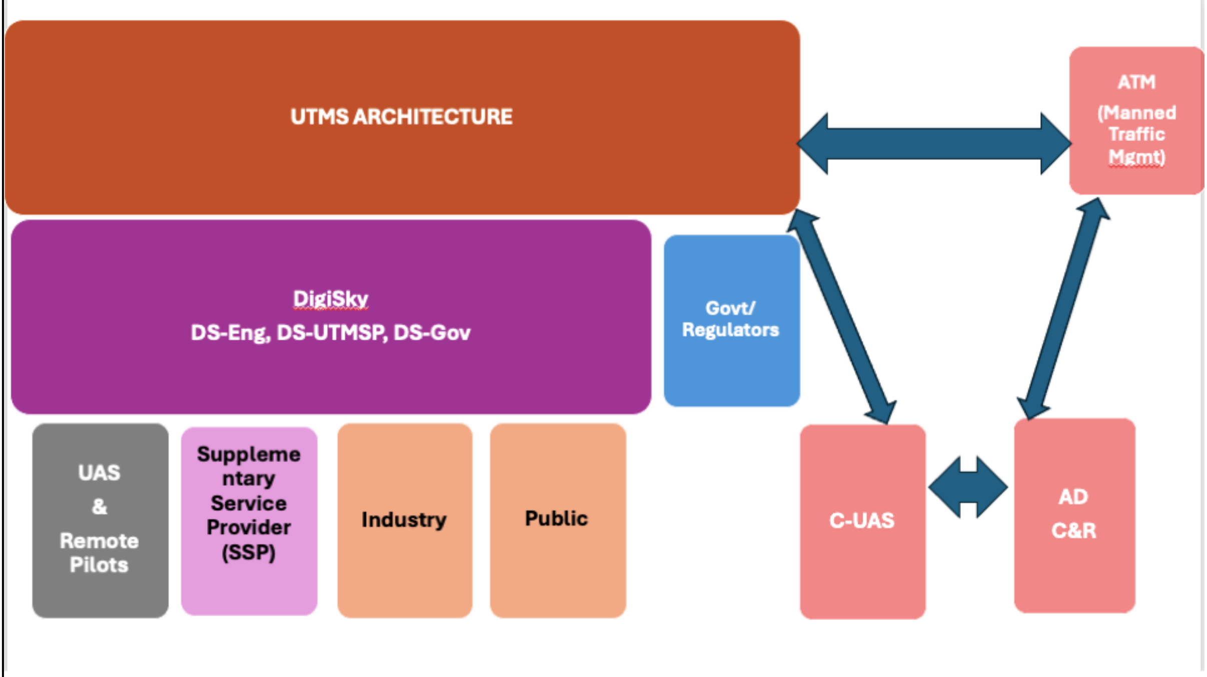


Figure 7. UTM Ecosystem Architecture.[27] Graphic by author.

The proposed UTM ecosystem is modular in character. The modules are interfaced based on functionality through API-based access protocols. Standardised protocols for intermodular communications are intended to facilitate seamless scaling up of the architecture. Nine key components of the architecture are: -

a) **DigiSky (DS) platform**. This is at the core of the ecosystem and consists of DS-Eng, DS-UTMSP and DS-GOV.

   - DS-Eng is the engine responsible for managing different databases, implementing business rules, and integrating various third-party services and platforms. It manages the digital airspace map. It contains the user registry of various UTM stakeholders like airspace management agencies, manufacturers, remote pilot training organisations, licensed remote pilots, and other government and administrative users. It stores data regarding all flight permissions and flight logs.
   - DS-UTMSP (Digisky UTM Service Provider) will provide a pan-India coverage through an interface between public and private UTMSP by acting as a common platform for interfacing between different UTMSP.
   - DS-Gov provides an interface for the State and UT governments and law enforcement agencies to interact with the UTM ecosystem to dynamically enforce yellow and red zones, including flight plan approvals in these zones.

b) **UTM Service Provider (UTMSP) Block**. Each UTMSP will provide technical and operational service augmentation to the DS-UTMSP through time synchronised, real-time/ near real-time situational awareness to subscribing operators, deconflicting flight plans, and sharing operationally essential information with stakeholders. As per the policy document, "*[s]uch synchronisation will happen over secure protocols and use a Discovery and Synchronisation Service hosted within the DigiSky Engine.*"[28]

c) **UAS Block**. This consists of type-certified UAS and licensed remote pilots executing UTMS-approved flight plans. The pilots may rely on information drawn from the UTMSP block and SSP blocks for overall in-flight situational awareness.

d) **Supplementary Service Provider (SSP) Block**. This shall provide supplementary services such as weather data, terrain and obstacle data, navigation and airspace surveillance data, payload data, etc, for optimising the operational efficiency of UAS with safety and security.

e) **Industry Block**. This provides an interface for the regulators with the industry stakeholders, such as manufacturers, importers, operators, etc.

f) **Government Block**. This comprises the central, state and UT governments, law enforcement agencies, IAF, DGCA and AD authority to enable seamless certifications, permissions, dynamic zoning of airspace etc.

g) **Public Block**. This allows the public to monitor UAS operations from a public safety and privacy point of view. The public may use UTMSPs to access such data and report issues in case they may suspect that a particular unmanned aircraft may not be flying as per the regulations or may be breaching their privacy.

h) **Air Traffic Management (ATM) system** as an external plugin to the UTM ecosystem.
j) **Counter UAS (C-UAS)** as an external plugin to the UTM ecosystem.

Status of UTMS Implementation. According to a report of 2024 by Fact.MR, the global valuation of the UTMS market is estimated at USD 1.44bn, and is expected to grow annually at 16.5% CAGR to USD 6.62 bn by 2034.[29]

As per the Federal Aviation Administration (FAA) of the US, the UTM Operational Evaluation (OE) is a consortium of industry operators collaborating with FAA and NASA to implement UTM by effectively managing overlapping Beyond Visual Line of Sight (BVLOS) operations.

In early 2023, the FAA evaluated new UTM capabilities and standards in support of small drone operations proposed by the industry. The FAA has started to issue Letters of Acceptance (LOA) to companies in this consortium to safely conduct commercial drone flights without visual observers in the notified airspace.[30]

In Europe, UTMS is commonly referred to as U-Space. The European Commission adopted the U-space package in April 2021.[31] The European Commission thereafter published rules for establishing U-Space in January 2023. It is based on three regulations that manage both drone and manned aircraft operations in European airspace. U-space aims at enabling complex drone operations with a high degree of automation. U-space provides an enabling framework to support routine drone operations, as well as a clear and effective interface to manned aviation, air traffic management (ATM) and air navigation service (ANS) service providers and authorities. U-space is expected to be capable of ensuring the smooth operation of drones in all operating environments and in all types of airspace (in particular, but not limited to, very low-level airspace).[32]

In India, the Union Minister for Road Transport and Highways Nitin Gadkari, on 07 February 2023, unveiled Skye UTM, a cloud-based system for managing air traffic. As per media reports, it is the most cutting-edge UTMS in the world, capable of handling 4,000 flights per hour (96,000 flights per day).[33] It can capture more than 255 parameters of UAS movements and store them in its 'Blackbox', which is a damage-proof data recorder, enabling a published systematic description of the entire flight. As the market matures in the coming years, additional players are likely to empower and enrich the UTMS ecosystem.

II.VI. Challenges in Implementing Regulatory Frameworks

Capacity Building. Drone ecosystem-related regulatory frameworks rely on voluntary disclosures and compliance. The state's capacity to ensure compliance must be enhanced at pace with trends in the drone ecosystem. As of 29 Jan 2025, based on data accessed from the Digisky platform, 29,526 UINs have been registered, 12,371 Remote Pilot certificates have been issued, and 152 DGCA-approved Drone Training organisations and 11 Train-the-Trainer (TTT) organisations are listed. For an industry anticipated to reach INR 2.3 trillion, proactive measures will be required to enhance capacities to implement compliance requirements mandated for smooth operations. Any shortfall in capacity will have to be assessed, forecasted and addressed through adaptive regulatory frameworks for ease of compliance and capacity building to monitor and address non-compliance. The key to safe operations will be the foolproof ability to segregate non-compliant aerial activity from the compliant operators.

Technological Constraints. Since the ecosystem is on an evolutionary curve, drones, as well as UTMS solutions, are presently constrained by technological limitations such as miniaturising Automatic Dependent Surveillance-Broadcast (ADS-B)[34] transmitters as well as deployment of ADS -B ground stations for defined airspaces to cover vast VLL airspace for real-time air situational awareness. Hardware and software integration is needed to implement No Permission, No Take-off (NPNT) in all UAS registered in Digisky. The impact of navigation system performance, accuracy and availability as well as data services quality and availability on implementation of Geofencing and support infrastructure to operationalise Beyond Visual

Line of Sight (BVLOS) operations, are technological constraints that will be addressed as the ecosystem evolves.

Interagency Coordination Across Jurisdictions. According to Article 246/ paragraph 29 of Schedule VII, List 1 of the Constitution, the Union Government is entrusted with "*Airways; aircraft and air navigation; provision of aerodromes; regulation and organisation of air traffic and of aerodromes; provision for aeronautical education and training and regulation of such education and training provided by States and other agencies.*"[35] The IAF is responsible for the defence of the Indian airspace. However, MHA's counter-drone guidelines have delegated terminal defence against a rogue drone in the hinterland to the state police or the threatened entity which may belong to different ministries. This grey area must be ironed out to manage the C-UAS dynamics and avoid fratricide.

Even after countering a rogue drone or a drone incident, access to the drone for forensic analysis and seamless access to reports of such forensic analysis by stakeholders will be required to optimise for multiple objectives, such as securing the conviction of the rogue drone operators, evolving Techniques, Tactics and Procedures (TTPs) for C-UAS operations, and supporting R&D in C-UAS, drones, and UTMS.

III. Limitations of the Current Air Defence Cover and Assessment of Threats Posed by UAS

III.I. Current Modalities of Air Defence (AD) in a Non- Bifurcated Airspace

Airspace Management. Although the defence of the Indian airspace was mandated to the IAF for the first time in the Union War Book in 1993, the IAF has ensured the defence of the Indian airspace since independence.[36] Airspace management from an AD perspective can broadly be divided into three major activities: Air Space Coordination, Air Traffic Control and Air Defence. Air Space Coordination and Air Traffic Control help segregate the compliant from the non-compliant users of the airspace, whereas Air Defence (AD) involves neutralising hostile air threats.

a) **Air Space Coordination (ASC)**. This entails time and space division of the airspace into horizontal bands by altitude and vertical zones above the geographies underneath.

- Indian airspace is divided into six Air Defence Identification Zones (ADIZ). Aircrafts entering or operating in the Indian airspace are given an Air Defence Clearance (ADC), which is like the aircraft's identity while within the Indian airspace.

- Similarly, within this is the subset of the Digisky UAS map with Green, Yellow and Red zones notified for UAS operations in the VLL airspace.
- Base Air Defence Zones (BADZ) are promulgated around airfields to define the limits around the base, which, if breached by a hostile aircraft, are the responsibility of the AD resources allotted for the defence of the base.
- Positive controls are implemented using radars, Identification Friend or Foe (IFF) interrogators and receivers, beacons, computers, digital data links, and communications equipment.
- Procedural controls are procedures in vogue and implemented in airspace in volume and time to cater for disruptions in the positive control measures. For instance, two aircraft flying the same route at the same altitude must be separated by at least 10 minutes of flying time. If two aircraft are estimated to reach a waypoint less than 10 minutes apart, the controller will instruct one to change altitude, speed, or route to maintain safe separation.

b) **Air Traffic Control**. Once the airspace has been defined to the users by the ASC, the ATC ensures that legitimate users of the airspace are regulated, deconflicted, and tracked using technologies such as ADS-B, and Radio Frequency Identification (RFID). Since ATC services are not available to the users of VLL airspace, UTMS will be filling this void to regulate the traffic in VLL airspace. DGCA will have to ensure a handshake between the ATC and the UTMS for a comprehensive sir situational awareness.

c) **Air Defence**. To coordinate AD battles, Indian airspace has been divided into areas controlled by the Air Defence Control Centre (ADCC). Each area is subdivided into smaller sectors controlled by Air Defence Direction Centre (ADDC).

- The ADDC is the executing agency for all AD in the country. Each ADDC has a few Integrated Air Command and Control System (IACCS) nodes of IAF under its command, which act as the hubs of Air Defence Control & Reporting (AD C&R).
- A networked grid of aerial and ground-based sensors of all three services with varying effective ranges along with Mobile Observation Posts (MOPs) for the detection and tracking of aircraft feeds the AD C&R. Emission Control (EMCON) ensures electronic signatures of the sensors are managed to prevent enemy action against these sensors.
- AD weapons provide a layered AD cover (Area and Point AD). Air and Ground Based AD Weapons (GBADW), which are deployed for AD cover to resources integral to IAF, Army and Navy, are controlled by their respective services, except the strategic tasks for which resources are distributed centrally.[37]

- The AD resources are optimised to avoid duplication of effort. A real-time comprehensive air picture is available at the IACCS and shared with the ADDCs.
- Once an aircraft is detected, tracked, and declared hostile, the AD C&R seamlessly allocates the AD weapons based on a prioritised, deconflicted weapons control order to neutralise the target, while ensuring fratricide is avoided.

The integration of AD C&R between the Indian Army and IAF is currently devolved down to the Headquarters Corps at the Joint Air Defence Centre (JADC).[38] Given the proliferation of end users of the Air littoral decentralised down to Company /Inf battalion or Combat Team/ Combat Group levels, a case can be made to devolve the arrangement down to the level of Headquarters Division for better decision making, deconflicting time critical-mission requirements in the Tactical Battle Area (TBA), and better coordination of C-UAS effort without fratricide.

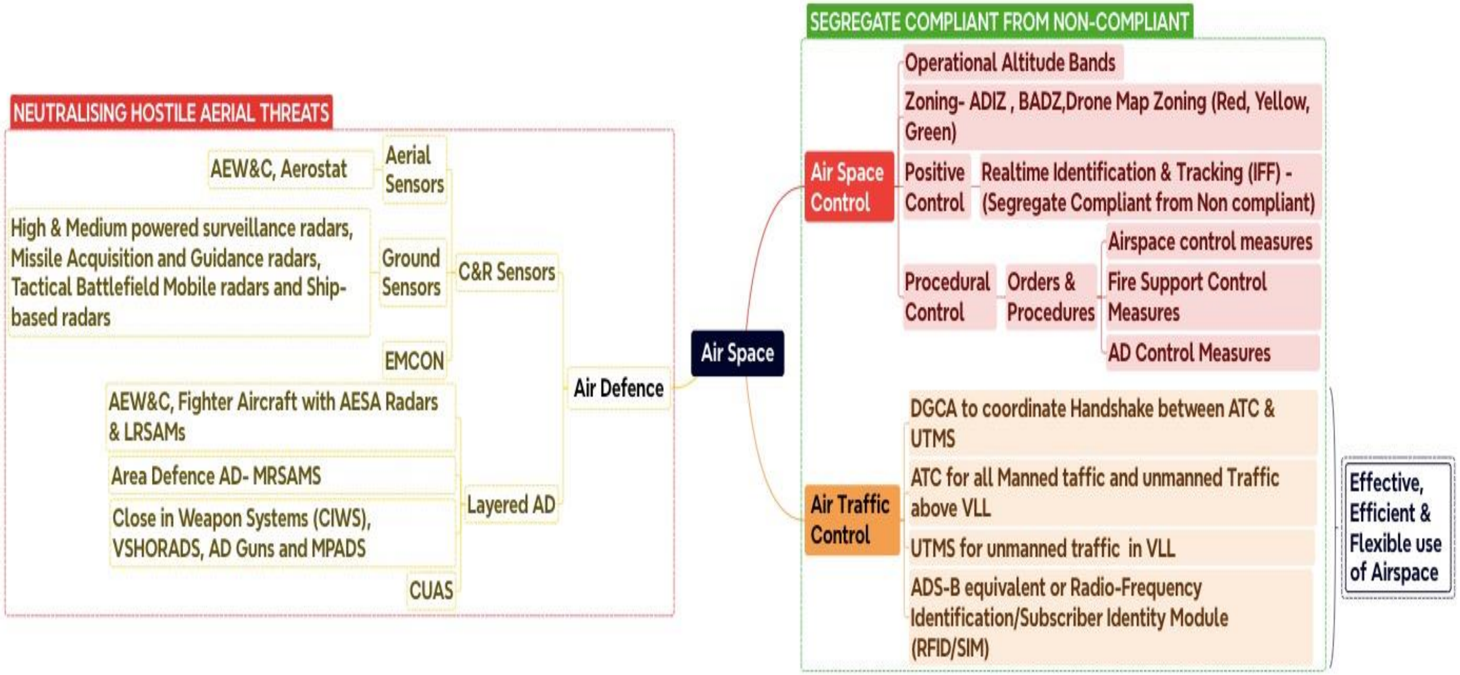

NEUTRALISING HOSTILE AERIAL THREATS
AEW&C, Aerostat
Aerial Sensors
High & Medium powered surveillance radars, Missile Acquisition and Guidance radars, Tactical Battlefield Mobile radars and Ship-based radars
Ground Sensors
C&R Sensors
EMCON
AEW&C, Fighter Aircraft with AESA Radars & LRSAMs
Area Defence AD- MRSAMS
Close in Weapon Systems (CIWS), VSHORADS, AD Guns and MPADS
Layered AD
CUAS
Air Defence
Air Space
SEGREGATE COMPLIANT FROM NON-COMPLIANT
Air Space Control
Operational Altitude Bands
Zoning- ADIZ , BADZ,Drone Map Zoning (Red, Yellow, Green)
Positive Control
Realtime Identification & Tracking (IFF) - (Segregate Compliant from Non compliant)
Procedural Control
Orders & Procedures
Airspace control measures
Fire Support Control Measures
AD Control Measures
Air Traffic Control
DGCA to coordinate Handshake between ATC & UTMS
ATC for all Manned taffic and unmanned Traffic above VLL
UTMS for unmanned traffic in VLL
ADS-B equivalent or Radio-Frequency Identification/Subscriber Identity Module (RFID/SIM)
Effective, Efficient & Flexible use of Airspace

Figure 8. Components of Air Space Management. (Mind map compiled by the author based on Chopra, Anil. 'Air Space Control: Challenges and Way Ahead'. *Air Power Journal* Vol. 13, no. No. 4 (December 2018). https://capsindia.org/wp-content/uploads/2022/08/Anil-Chopra.pdf.). Graphic by author

What has Changed? The arrival of drones has transformed the airspace security paradigm due to two factors.

a) **Horizontal Splitting of the Airspace**. From an airspace user's perspective, as posited by Anil Chopra, Air Space Control entails coordination, integration and regulation of activities in the defined air space by identifying and monitoring all air space users. It exercises a degree of authority necessary to achieve effective, efficient, and flexible use of air space.[39]

In an earlier paradigm (before drones), airspace control entailed control over a defined area for a specified period for uninhibited air, ground or maritime operations by employing high-end fighter aircraft through swift, transient presence to establish varying degrees of control.

With the arrival of drones into the equation, the VLL airspace and the adjacent airspace up to 10,000 feet and the airspace beyond 10,000 feet have assumed starkly different connotations from operational space and security of airspace perspective. The airspace adjacent to the ground, up to 10,000 feet, including the VLL airspace earmarked for commercial drones, is coming to be defined as the 'Air Littoral': "*[T]his airspace generally located below 10,000 feet is defined as the area from the Coordinating Altitude to the Earth's surface, which must be controlled to support land and maritime operations and can be supported and defended from the air and/or the surface.*"[40]

This band of airspace is different from the balance of the airspace, as this has a higher aggregate of users, which include artillery projectiles, cruise missiles, multi-purpose UAS, and manned rotary and fixed-wing aircraft. This band is narrower, densely used, more chaotic, and significantly impactful for actors in the Tactical Battle Area (TBA). Therefore, securing this space or controlling operations in this band is more complex in wartime than in peacetime.

In peer or near-peer contestations like in the Indian context, control of the air will be for short durations. The enhanced complexity of the Air Littoral due to drones entails that this control will never be absolute in future contestations. Earlier control was denied to the adversary through offensive counter-air operations to degrade the enemy air force's manned aircraft (the prime contributor of aerial threats above the Air Littoral) and air defence for friendly forces and vital assets on the ground. The Air littoral, instead, demands control through a persistent presence in this space, including passive and active air defence against threats.

b) **Area Defence vs Point Defence**. Aerial threats earlier were typically from across borders due to prohibitive establishment costs restricting access to enabling technologies to only state actors. The Air Littoral has become vulnerable to cross-border as well as internal security threats from within the hinterland due to easy access to drone technology, as argued by Bermer and Grieco, "*Clusters of technological breakthroughs in nanotechnology, additive manufacturing (3D printing), materials science, robotics, and quantum computing will allow the employment of numerous small, cheap, smart, and highly lethal weapons.*"[41] Therefore, securing the airspace during peacetime requires measures to counter the threats in this band not from a predominantly area defence perspective but an exponentially dense point defence perspective (due to drones rendering more assets vulnerable in a cost-effective way).

Threat Assessment. The use of drones by state and non-state actors has risen exponentially over the past decade. As per the Global Peace Index 2024: "*[t]he growth in the use of drones over the past decade indicates an increasing reliance on unmanned systems for reconnaissance, surveillance, and combat purposes, showcasing a shift towards more sophisticated and autonomous military capabilities. The trend may also imply a potential shift in traditional military strategies towards remote warfare and asymmetric warfare, with UAVs set to play a pivotal role in future military operations and security strategies worldwide.*"[42]

In 2018, before the policy notification (CAR 1.0), approximately 50,000 drones were operating in India despite a ban on drones dating back to 2014. Amit Shah, the Home Minister of India, unequivocally flagged drones as an emerging security threat during the 60th BSF Raising Day on 08 December 2024. C-UAS operations figures of the Punjab frontier of BSF aggregated since 2022, given in Figure 9 below, indicate the severity of this emerging threat.

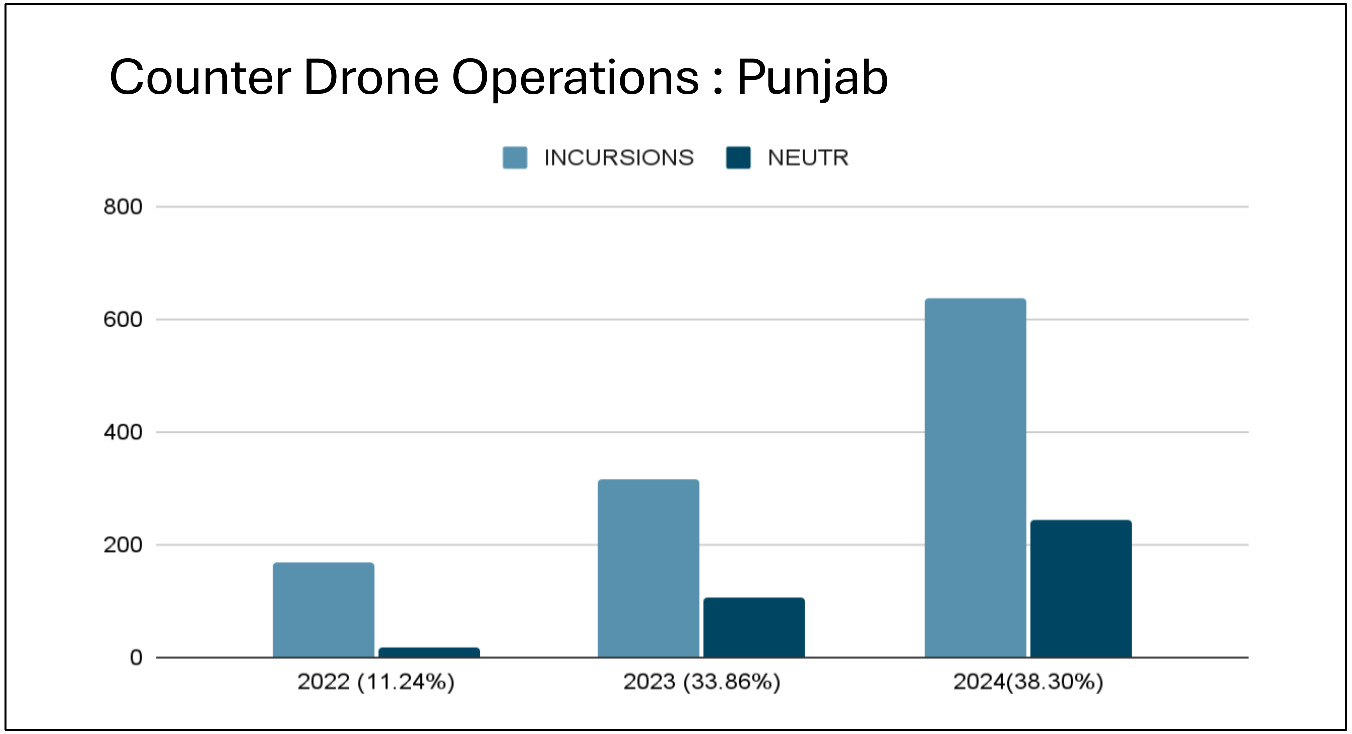


Figure 9. Counter Drone Operations Punjab. (Compiled by the author from multiple sources.)

A nascent, low-density C-UAS grid, with a success rate of approximately 38% in countering the detected cross-border drones, must evolve into a foolproof nationwide C-UAS grid to effectively counter the emergent threat from a cross-border and internal security perspective.

III.II. Potential Threat Scenarios

Aerial threats include weapons launched from aerial and space-based platforms and surface-launched weapons. Drones are emerging as a potent aerial threat, added to the paradigm of conventional aerial threats.

Countries in India's neighbourhood, especially China, Pakistan, and Bangladesh, have added drones to their conventional UAS arsenal for ISR as well as targeting operations. UAS capability has been built through imports in the case of Pakistan and Bangladesh (with assistance from China and Turkey) and through extensive indigenous capacities in the case of China. While UAS capability development by militaries in the neighbourhood has focused on long-range RPAS, a substantial number of tactical RPAS are being operated by the respective militaries.

In addition, criminals, as well as non-state actors, have increased their usage of tactical drones of the Chinese DJI variety for trans-border operations, such as delivery of weapons and contraband across the borders. Drones have emerged as an obvious choice due to their dispensability, cost-effectiveness, ease of fabrication for unconventional payloads, inherent operator safety and plausible deniability. Therefore, like most technologies, apart from large-scale potential social benefits, many use cases for security threats by inimical elements emerge which need to be addressed.

Capability Based Threats. The inherent capabilities of a drone which can be exploited by inimical elements to cause disruptions are discussed below.

c) **ISR & EW**. Most drones are equipped with integrated electro-optical sensors, which can assist in gathering intelligence on target areas which can be further exploited over a broad spectrum, ranging from breaching individual privacy, to 3D profiling of targets for weapons, to target matching to be exploited in subsequent kinetic attacks. Drones have been used to reconnoitre defence works to plan prospective operations. Electronic Support Measure (ESM) and Electronic Countermeasure (ECM) payloads can also be used for electronic warfare (EW).

d) **Suicide or 'Kamikaze' Drone**. A drone, flying at high speeds by its momentum combined with an explosive payload, can be used as a guided, remotely-piloted, or autonomous projectile to execute an offensive mission such as an aerospace collision or attack on personnel/infrastructure. The attack on Saudi Aramco's petroleum storage facility in Jeddah by Houthi rebels on 25 Mar 2022 or 07 October 2023 drone attacks by Hamas against Israel are prominent examples.

e) **Dangerous Payload Delivery**. A drone's inherent ability to ferry and deliver a payload can be exploited to deliver munitions, Improvised Explosive Devices (IEDs), adapted armament/ explosives, contraband, etc. Payloads delivered across the International Border (IB) in Punjab by Pakistani state-backed criminal gangs are an example.

f) **Overwhelming Air Defence (AD) Systems.** Drone swarms can be low-cost, low-tech options to overwhelm multi-million dollar high-tech AD systems. As highlighted in the issue brief by Zachary Kallenborn, "*[i]f defenders employ expensive surface-to-air missiles to shoot down cheap*

> *drones, missile stocks will not be available for use against more valuable targets like manned aircraft.*"[43]

Vulnerability of Targets. While AD architecture caters for conventional aerial threats manifesting in the national airspace, the Ministry of Home Affairs has appreciated the following target groups that are vulnerable to sub-conventional aerial threats, including rogue drones:-

- Government institutions such as State/ UT secretariats, assemblies, Courts etc.
- Public transport hubs (airports, railway stations, metro stations, Interstate bus terminals, ports etc).
- Targets of economic importance (Stock exchange, power grids, vital installations under Central/State and UT administration).
- Embassies/ consulates.
- Targets with dynamic threat perceptions based on intelligence inputs may include VVIP residences, venues of public gatherings / religious congregations etc.

Threat and Vulnerability Matching. Aerial threats can be assessed and countered based on the technical capability of the aerial weapon used for targeting and the target's relative importance and risk profile. Apratim Sharma elucidates the interlinkage between threat and risk in the context of UAS as: "*[A] threat is an actor possessing both capability and intent to attack. A risk is a function of a threat, a vulnerability, the likelihood of the threat* *attacking the vulnerability, and the potential impact of the attack."*[44] *The relation is explained as,*

"Threat = Capability × Intent

Risk = Likelihood (Threat + Vulnerability) × Impact"

The capability component of the threat is a function of a drone's category and the nature of its payload, which C-UAS technology needs to counter. In contrast, regulations and operational procedures must focus on ensuring a safe operational environment and avoiding collateral damage to the peaceful users of the UAS ecosystem. C-UAS deployment must be determined by matching intelligence-based threats and risk factors with the existing capability of the C-UAS system.

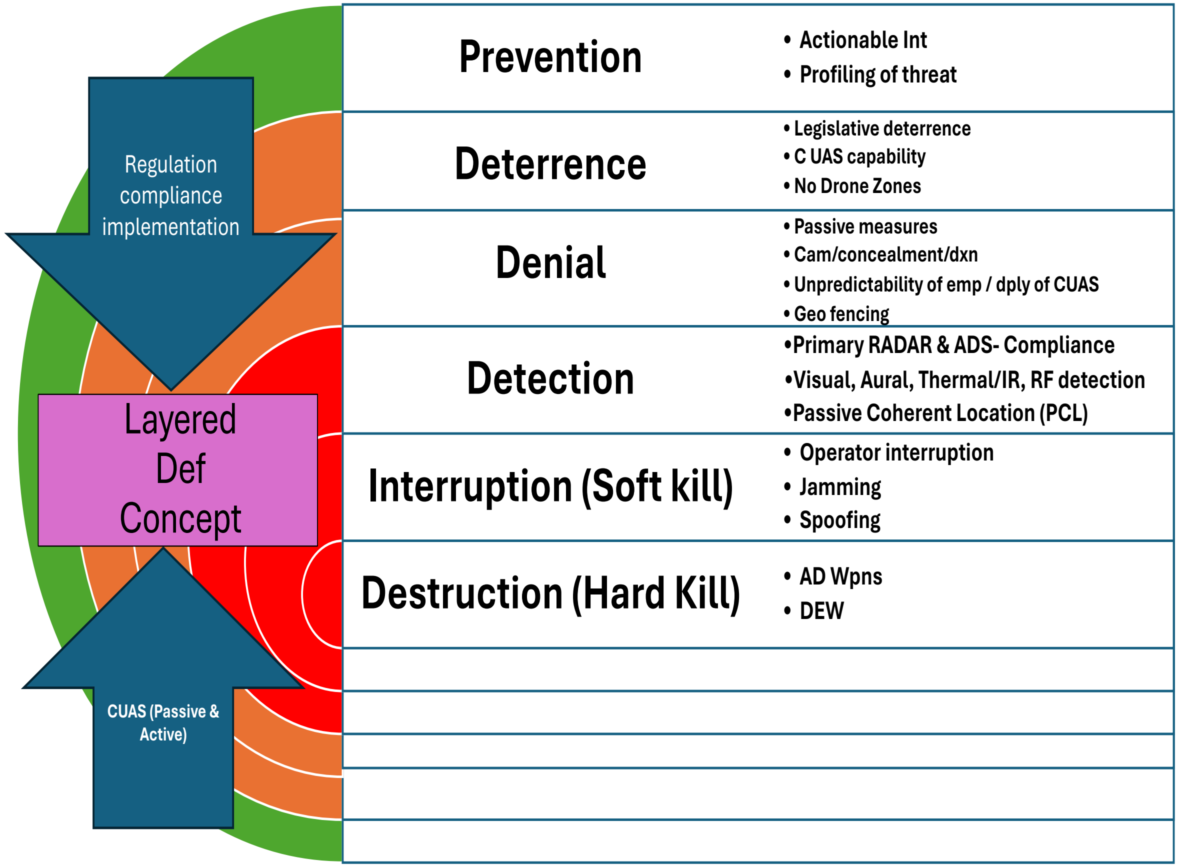
IV. Capabilities and Limitations of C-UAS Systems & Proposed C-UAS Architecture

IV.I. C-UAS Philosophy

Execution of C-UAS operations in the VLL airspace will be based on six mutually reinforcing functions: prevention, deterrence, denial, detection, interruption, and destruction (depicted in Figure 10, below). These functions are founded on a layered defence concept with a two-fold focus.

a) Firstly, ensuring regulation compliance to segregate the compliant from the non-compliant to ensure a safe operations environment for the compliant.

b) Secondly, detect and counter the non-compliant. These functions are explained in subsequent paragraphs.



Prevention	• Actionable Int • Profiling of threat
Deterrence	• Legislative deterrence • C UAS capability • No Drone Zones
Denial	• Passive measures • Cam/concealment/dxn • Unpredictability of emp / dply of CUAS • Geo fencing
Detection	•Primary RADAR & ADS- Compliance •Visual, Aural, Thermal/IR, RF detection •Passive Coherent Location (PCL)
Interruption (Soft kill)	• Operator interruption • Jamming • Spoofing
Destruction (Hard Kill)	• AD Wpns • DEW

Figure 10. Functions of C-UAS operations

- **Prevention**. This function aims to prevent the presence of non-compliant entities in the ecosystem. A significant part of this function hinges on a comprehensive intelligence picture. Intelligence on UAS and C-UAS technology as it evolves globally, what gets fielded in our immediate neighbourhood, and what is finding its way into our national ecosystem needs to be dynamically assessed, war-gamed, and countered.

- Insights into manufacturers, importers, retail vendors, buyers, operators and pilots are available through mandated type certifications and UID protocols for UAS and licensing norms for UTMS, which comprehensively cover security requirements. Intelligence will be the key to profiling the non-compliant actors and enforcing compliance or weeding the non-compliant out of the ecosystem.
- For example, at the district level, a suitably trained special cell of the police, similar to cyber cells, should be able to non-intrusively compile and verify details of legitimate users from Digisky or UTMSP, and thereby focus on non-compliant drone users in that jurisdiction.

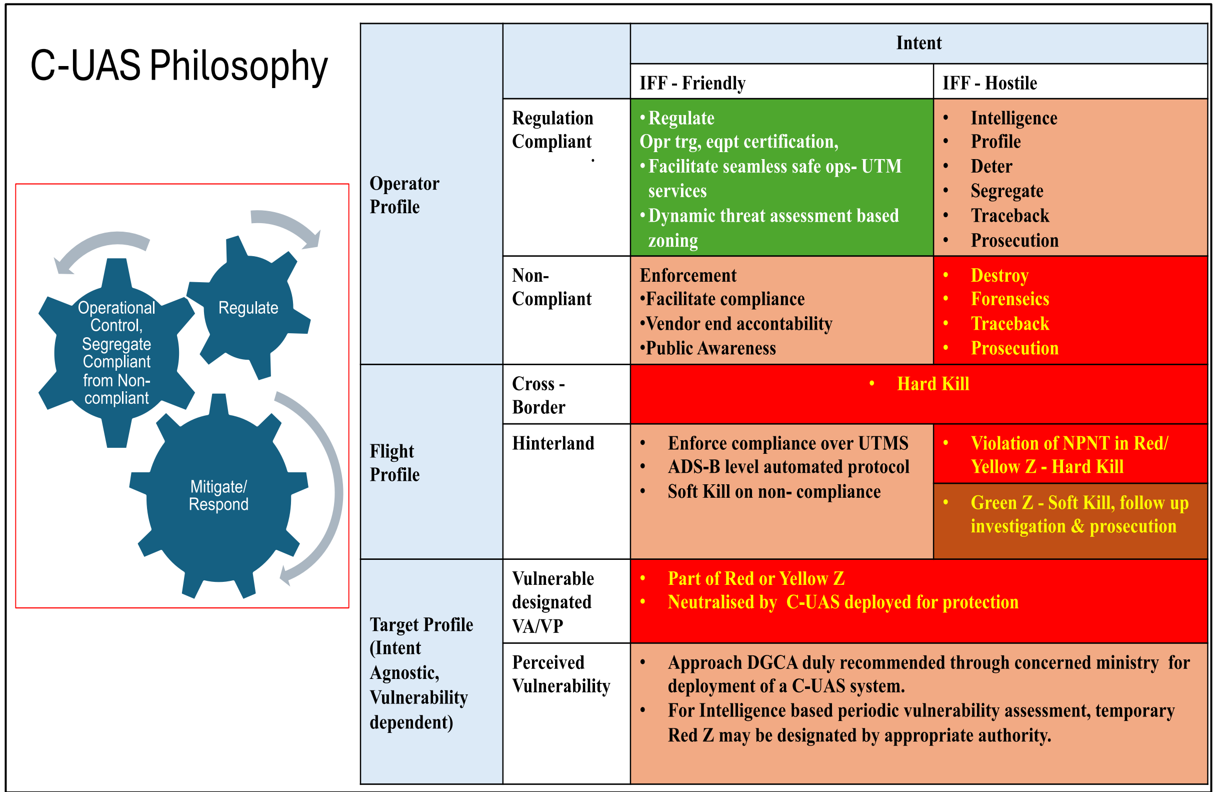
○ **Deterrence**. This is a function of stringent legislative provisions against the non-compliant, coupled with foolproof enforcement of Red and Yellow zones and regulated use of Green zones through a reliable UTMS. A networked C-UAS grid will further reinforce deterrence by rendering the viability of non-compliance cost-prohibitive.

○ **Denial**. This is hinged on denying a vulnerable target profile of a Vital Area (VA)/ Vital Point (VP) to a threat actor. This will be achieved through passive measures such as camouflage and concealment, maintaining unpredictability of the defensive posture by a target through threat-based C-UAS deployment and adopting commensurate zoning criteria to ensure that the VA/VP comes under the appropriate zone in the Digisky map.

- **Detection.** Once the above functions have significantly eroded a threat probability, a networked (C-UAS, UTMS, AD) C&R grid, reinforced by ADS compliance or geo fencing protocols, will detect a non-compliant UAS and take one of the subsequent actions to neutralise the threat.
- **Interruption**. This option will be exercised against a threat deviating from a flight plan declared on the UTMS in the Green zone to disrupt the UAS's capability to operate coherently by a soft kill through jamming or spoofing.
- **Destruction.** This option will be exercised against a threat in the Red or Yellow zone to destroy the UAS by a hard kill through an appropriate AD weapon or Directed Energy Weapon (DEW).

A C-UAS philosophy moored in adaptive regulations, stringent compliance norms and foolproof mitigation / response mechanisms will ensure a UAS operations ecosystem which is implementable, functional, versatile and scalable. This will be achieved by matching the operator / pilot's intent, discerned through IFF, with the operator profile (compliant / non-compliant) and the flight profile (which could be originating from across the border, or from within the national airspace through the transgression of a valid flight plan into restricted airspace, triggering execution of a decisive C-UAS action).

An intent-agnostic, vulnerability-dependent target profile must be ensured for VAs and VPs based on a realistic threat assessment and commensurate resource allocation against plausible threat scenarios. This philosophy is depicted through the matrix below.



C-UAS Philosophy

Operational Control, Segregate Compliant from Non-compliant
Regulate
Mitigate/ Respond

		Intent	
		IFF - Friendly	IFF - Hostile
Operator Profile	Regulation Compliant	• Regulate Opr trg, eqpt certification, • Facilitate seamless safe ops- UTM services • Dynamic threat assessment based zoning	• Intelligence • Profile • Deter • Segregate • Traceback • Prosecution
	Non-Compliant	Enforcement •Facilitate compliance •Vendor end accontability •Public Awareness	• Destroy • Forenseics • Traceback • Prosecution
Flight Profile	Cross - Border	• Hard Kill	
	Hinterland	• Enforce compliance over UTMS • ADS-B level automated protocol • Soft Kill on non- compliance	• Violation of NPNT in Red/ Yellow Z - Hard Kill • Green Z - Soft Kill, follow up investigation & prosecution
Target Profile (Intent Agnostic, Vulnerability dependent)	Vulnerable designated VA/VP	• Part of Red or Yellow Z • Neutralised by C-UAS deployed for protection	
	Perceived Vulnerability	• Approach DGCA duly recommended through concerned ministry for deployment of a C-UAS system. • For Intelligence based periodic vulnerability assessment, temporary Red Z may be designated by appropriate authority.	

Figure 11. C-UAS Decision Support Matrix

IV.II. C-UAS Capabilities

The papers[45] - [46] aid in understanding C-UAS technology. A UAS system has three components: the aerial vehicle with its payload and its integral electronics and positioning link, the control station, and the communication link between the two. Therefore, a C-UAS has to Detect, Track, Identify and Neutralise (disrupt or destroy) a UAS operation based on targeting any of these components. The capabilities of contemporary C-UAS systems are based on these functions integrated as a system.

a) **Detection, Tracking & Identification**. This is based on radio frequency and visual or aural detection through integrated sensors to provide a 'pick up' and a computed real-time fix for a drone. Sensors used for detection can be:

- RADAR, which is an active sensor (relies on active emission by the sensor)
- Radio Frequency (RF) sensor is a passive sensor that detects the RF link of the drone itself
- An acoustic sensor, also a passive sensor, depends on the acoustics of the aural signature of a drone for detection

- Optical sensors detect based on visual detection through Electro-Optical (EO), Infrared (IR) or Thermal Imaging (TI) cameras.

A C-UAS, therefore, integrates multiple sensors supported by computing to give an output which supports the Command and Control (C2) of the C-UAS.

b) **Neutralisation**. It aims to prevent the UAS from executing its intended mission. This can be done by disrupting the drone's operations (Soft Kill) or by destroying the drone (Hard Kill). Based on the sensor inputs to the C2 of the C-UAS and the intended effect, the Hard Kill or Soft Kill option can be executed.

- **Soft Kill**. This may exploit protocol-based vulnerabilities in the drone's communication system to 'hack' into and disrupt it. However, modern drones are equipped with countermeasures such as 256-bit encryption against hacking. Another option, commonly referred to as 'Spoofing', involves the C-UAS feeding erroneous sensor outputs to the done sensors, causing the drone to either land at an alternate location or crash. The other option is to use jamming to disrupt either the communication link between the operator and the drone, causing it to initiate 'Return to Home (RTH)' protocols to land, or to disrupt the navigation link of the drone, sending it into a hover until battery discharges and the drone lands or crashes.

- **Hard Kill**. This may involve using kinetic projectiles, such as anti-aircraft weapons, or non-kinetic means, such as Directed Energy Weapons (DEW) or High-Power Microwaves, to destroy the drone. Other methods may involve using anti-drone nets flown by other drones to trap the targeted drone or even methods as rudimentary as trained birds to disrupt the rotors.

IV.III. C-UAS Kill Cycle

The C-UAS kill cycle can be broken down into three critical phases.[47]

a) **Phase 1 - Detection and Tracking (DT)**. This phase integrates inputs from multiple sensors, including basic visual/aural detection by sentries and continuous tracking, ensuring real-time awareness of potential threats.

b) **Phase 2 - Identification and Decision (ID)**. This phase involves affirmative identification between friend or foe (IFF), achieved through a software-driven synthesis of the DT phase inputs with the C-UAS library. In the future, it may include corroboration with the UTMS inputs to support C2 for decision to interdict.

c) **Phase 3- Interdiction (I)**. In this final phase, when a decision to interdict has been made, a software-driven logical process (either fully autonomous or human-in-the-loop), selects the appropriate countermeasure to achieve a hard or a soft kill.

The entire 'DT - ID - I' Kill-Chain is a time-critical process. Therefore, it must be automated to minimise response time, autonomous to accommodate a dense traffic environment, robust against countermeasures, and user-friendly for the C-UAS operators to execute its mission in a networked grid.

Limitations of C-UAS. The limitations of a C-UAS system are inherently an amalgamation of the limitations associated with each of the individual sensors and weapon systems integrated into the C-UAS system.

- Radars, being an active sensor, have a limitation of giving away their presence and are dependent on an unobstructed line of sight;
- Jammers have a restriction of power and range and, due to their wide cone of engagement, can have adverse collateral impact on friendly users of Electromagnetic Spectrum (EMS).
- RF detection sensors need a clear line of sight for accuracy and are susceptible to electromagnetic interference.
- The performance of electro-optical sensors can be degraded due to weather
- LASER/ DEW have limited range and depend on very high power requirements.

Incorporation of Artificial Intelligence (AI) in C-UAS- UAS- UTMS integration can significantly impact the efficiency of time-sensitive decision-making protocols, tending towards greater autonomy in the process. A multi-sensor, multi-weapon, integrated C-UAS grid (consisting of sensors and weapons, mutually compensating for intrinsic technological limitations) is the ideal solution for C-UAS. Some of these limitations and compensating advantages are tabulated below. [48]

S No	Kill Type	Technique	Advantage	Limitations	Remarks
(a)	Soft Kill	RF Jamming	Medium cost, non-kinetic disruption.	• Short range • Requirement of direct LOS. • Likely interference to friendly systems. Or other radio communications. • The possibility of collateral impact due to unpredictable behaviour of UAS.	E.g. Used in C-UAS operations by BSF.
		RF Hijacking	Ability to securely seize the UAS.	• High-cost, high-tech. • Requires high skill and extensive library of the data-link protocols of UAS. • Needs advanced software to break into secure 256-bit encryption.	

		GPS Jamming	Low cost and relatively simple.	Collateral impact of friendly systems/ aircrafts.	E.g. Used in C-UAS operations by BSF.
		Spoofing	Ability to securely seize the UAS.	• High-tech, high-cost. • Difficult against robust UAS integrated with sophisticated countermeasures.	E.g., Iran successfully captured a completely intact highly sensitive American RQ-170 Sentinel stealth UAS in 2011.
(b)	Hard Kill	High energy LASER effectors	Cost effective, physical destruction of Kamikaze drones.	• Short range (up to 3000 meters) and collateral impact on friendly use of EMS. • UAS structural design can be adapted to deflect LASER.	
		High Powered Microwave (HPM) Effector	• Disrupts system electronics. • Effective against UAS in range and swarms.	• Expensive. • Collateral impact on friendly systems and due to falling drones.	
		Kinetic Projectiles	• Low cost.	• Collateral impact along the effective range of projectiles.	

IV.IV. Challenges to Air Defence in the Bifurcated Airspace

IAF has challenges in ensuring the defence of the Indian airspace in an airspace which now stands bifurcated. Significant lessons will emerge in this regard from the recently concluded OP SINDOOR. These cumulative challenges will have to be addressed through delegated controls over UTMS.

a) **Air Space Control**. Drone Rules 2021 has laid down the zoning of VLL airspace into Green, Yellow and Red zones. The sectors for management of the vast airspace will have to be revisited in congruence with the expanding UAS operational space both in terms of geographical spread and density of operation. The sectors must be modular and scalable so that a suitable UTMSP can service each sector. A viable model would be to align the sectors to the administrative boundaries of districts, which will be easier to scale up as the ecosystem expands by enhancing the capacities of relevant administrative entities such as Police, Urban development etc. This will also allow ease of scaling up for BVLOS operations in future.

   Adequate sensor cover in the VLL airspace is unavailable; therefore, exercising positive control is challenging. Greater reliance will have to be on procedural controls. The procedural controls must be based on flight plan authorisations and monitoring through tamperproof ADS-B, RFID, and SIM protocols coopted onboard the UAS with remote authentication through UTMS.

b) **Air Traffic Control**. The national UTMS policy framework lays the roadmap for filling the void of ATC services in the VLL airspace. DGCA will have to promulgate means for a handshake between the airspaces managed by the ATC and UTMS for sharing relevant flight safety-related data. As UAS and UTMS technology evolves and the ecosystem adapts and matures, a situation is feasible where UTMS and ATC control aerial platforms operationally transgressing between the two airspaces.

c) **Air Defence**. Presently, the technological ability of C-UAS sensors to detect, track, and identify UAS is limited in range. The sensor grid for existing AD C&R cannot cover the VLL airspace. A UTMS for the defence services UAS operating in VLL must be co-developed and deployed alongside the commercial UTMS to deconflict flight plans between the two users without compromising mission priorities.

IV.V. Proposed C-UAS Grid

A lateral plug-in between ATC – UTMS – C-UAS grid – AD C&R grid based on strictly need-to-know information sharing protocols over secure data links will be required for a real-time, comprehensive air situational awareness, synthesised at IACCS for seamless AD cover in the bifurcated airspace. In the interim, R&D should focus on integrating sensors on aerial or space-based platforms into the AD sensor grid for comprehensive air situational awareness. EMCON will have to be coordinated to ensure minimum collateral impact on friendly EMS. A threat-specific, networked C-UAS grid will have to be deployed for different areas as given below.

a) **Linear Tiered Grid**. Along International Border (IB) and Line of Control (LC) or maritime borders where the ownership of airspace is well defined, a linear grid, tiered in depth, will be required. The lead border guarding force should be equipped with C-UAS systems in densities commensurate to the threat trends. The deployment should be multitiered based on the depth of hostile UAS operations, and layered based on effective operating ranges of the C-UAS systems forming a part of the grid. The grid should be plugged in rearwards to the AD C&R, for smooth scaling up of C-UAS operations using conventional AD weapons.

b) **Honeycomb Grid**. In urban and rural landscapes, C-UAS deployment should be based on risk assessment by the lead ministry in charge of the security of the VA/VP duly vetted by intelligence agencies and MHA. C-UAS systems can be deployed in a honeycomb-like networked grid with dynamic zoning promulgated. Standardisation of TTPs of all agencies manning C-UAS systems should be ensured.

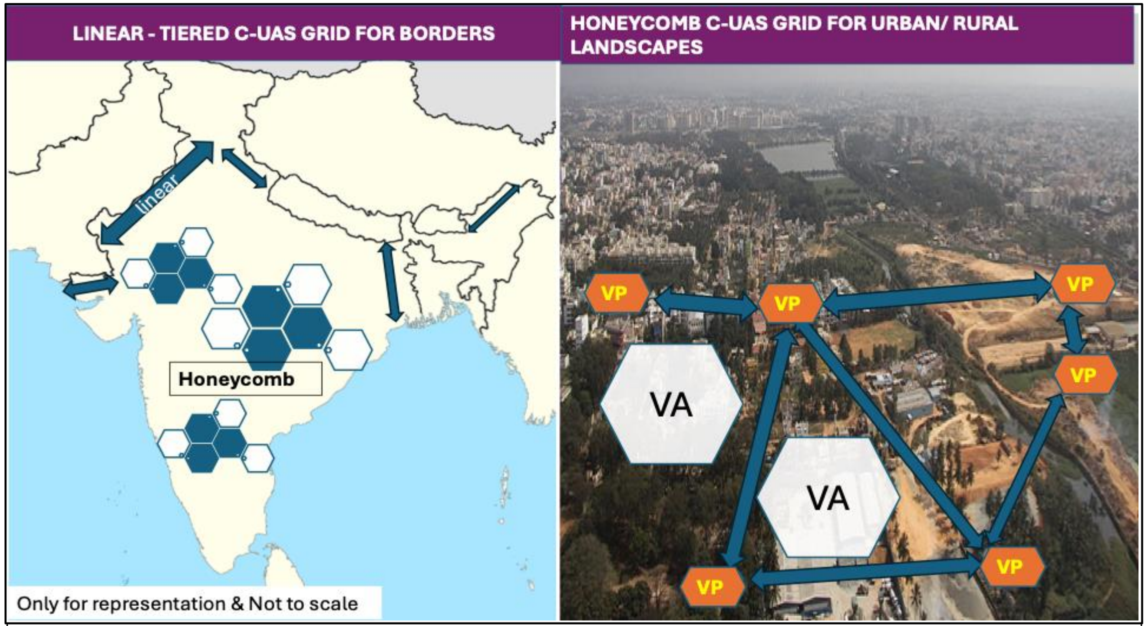

LINEAR - TIERED C-UAS GRID FOR BORDERS
linear
Honeycomb
Only for representation & Not to scale
HONEYCOMB C-UAS GRID FOR URBAN/ RURAL LANDSCAPES
VP
VP
VP
VP
VA
VA
VP
VP

Figure 12. Proposed C-UAS Grid Models. Graphic by author

V. Key Recommendations

V.I. C-UAS Grid Related

a) **Interagency Coordination**. IAF and DGCA should be the lead coordinating agencies for formulating regulatory frameworks in the UAS, UTMS, and C-UAS ecosystems.

b) **Capacity Building**. IAF, in collaboration with the AD arms of Indian Amy and Indian Navy, should take the lead in standardising the training and operations protocols of C-UAS, while manning of C-UAS is delegated to respective ministries responsible for the VAs/VPs. For example, the CISF unit managing the security of a refinery should go through a consultation process between MHA and the Ministry of Petroleum for threat assessment, and deploy a commensurate C-UAS system with a plug-in into the local UTMS, with operators trained on a standardised SOP. This should be networked backwards into AD C&R, synthesising real-time air situational awareness.

c) **Scalable Sectorisation**. The sectors in the VLL airspace should be aligned to the administrative boundaries of districts for ease of scalability, and for likely future BVLOS operations, by augmenting and leveraging existing security apparatus through focused training and capacity building.

V.II. UAS Related

a) **Realtime Situational Awareness**.

o Automated real-time position transmission and IFF through ADS-B equivalent protocols and RFID, SIM should be mandatory for all UAS operations.

o All UAS operations should be through a UTMSP to ensure real-time air situational awareness.

b) **Coordinated use of Airspace**. Defence services UAS operations should be coordinated through a tailormade UTMS, with an appropriate handshake with the commercial UTMS, to deconflict flight plans without compromising mission priorities, and for ease of transition between peace and war times.

V.III. C-UAS Related

a) **Controlled & Regulated Deployment**. All C-UAS manufacturing and deployment should be under licensing norms promulgated by the cabinet secretariat, similar to Jammer Guidelines 2023.[49]

b) **Modular Networked Grid**. All C-UAS should be networked into a sector-level grid and have a plug-in to the UTMS architecture.

c) **Post-Incident Analysis**. Drones successfully countered by a C-UAS should undergo thorough forensics, and technical reports from such investigations should be uploaded to a library accessible in a need-to-know manner on Digisky for all stakeholders, such as law enforcement, C-UAS developers and operators, to refine R&D, update electronic libraries, and fine-tune Techniques, Tactics, and Procedures (TTPs).

VI. Conclusion

Achieving India's Advanced Air Mobility (AAM) objectives will depend upon promoting flexible and safe management of the Indian airspace. This is a function of cooperation, regulation, and integration amongst all airspace users to optimise its use by leveraging advanced UAS, UTMS, and C-UAS technologies to tame our skies while unleashing their tremendous potential.

The proposed C-UAS grid based on the philosophy of six mutually reinforcing functions (prevention, deterrence, denial, detection, interruption, and destruction) will ensure that the compliant actors maximise the benefits of the UAS ecosystem while the non-compliant are held accountable.

Appendix A

UTM Stakeholders and Their Roles

S No	Stakeholder	Regulatory/ Operational Function
(a)	Central Government	• Formulation of regulatory frameworks and permission for operations in Red Zones.
(b)	Directorate General of Civil Aviation (DGCA)	• Regulatory authority for civil aviation safety & air worthiness standards. • Coordination with ICAO. • Owns and manages Digisky platform on behalf of MOCA. • UAS type certification, remote pilot licensing, training organisations' certifications. • Likely to be regulatory authority for UTMS.
(c)	Bureau of Civil Aviation Security (BCAS)	• Regulates aviation security standards & implementation.
(d)	Airspace Management Agencies	• Agencies in National, State and UT administrations delegated with authority to notify zonings in the Airspace Map on Digisky.
(e)	Air Traffic Control (ATC) Authority	• ATCs responsible for granting permission for UAS operations within Yellow and Red zones within their designated limits & coordinate approved flight plans with remote pilots.
(f)	Air Defence (AD) Authority	• Indian Air Force (IAF) responsible for monitoring manned and unmanned operations within national airspace. • Will be providing AD clearance in Yellow zone to UAS operations. • AD clearance in Red zone consequent to permission by central government to the remote pilot.
(g)	UTM Service Provider (UTMSP)	• A DGCA approved public or private entity. • Responsible for facilitating flight permissions, managing UTM services and coordinating UAS

		operations (segregating, separating & managing flight plan operations) in UTMS airspace of responsibility.
(h)	Supplementary Service Provider (SSP)	• Navigation data, airspace surveillance data, weather data, terrain and obstacle data during the pre-flight and in-flight stages to ensure safe conduct of UAS operations. • Additional value added services like insurance providers, analytics providers, UAS manufacturers etc. may be provided access to DigitalSky Platform via Application Programming Interface (API).
(j)	Remote Pilot	• Individual in possession of a remote pilot licence, authorised by the operator with duties essential to the operation of an UAS and who controls the flight during flight time. • Responsible to register with concerned UTMSP as per planned flight route.
(k)	UAS Operator	• Licensee providing UAS services through Digisky.
(l)	General Public	• Need-to-know access to information through Digisky platform.
(m)	Law Enforcement & Security Agencies	• Access to real-time or historical information about UAS operations for security and surveillance; or for countering rogue UAS. • CUAS deployment and interface with UTMSP. • Physical verification/ audit of licensed entities as mandated by DGCA.

VII. References

[1] Broad nomenclature used for drones in 'Drone Rules, 2021'. The Gazette of India: Extraordinary, Controller of Publications,25 August 2021. https://www.dgca.gov.in/digigovportal/jsp/dgca/homePage/viewPDF.jsp?page=InventoryList/headerblock/drones/Drone%20Rules%202021.pdf.

[2] 'Commercial Drone Market Size, Industry Share & COVID-19 Impact Analysis'. Fortune Business Insights, 23 December 2024. https://www.fortunebusinessinsights.com/infographics/commercial-drone-market-102171.

[3] Rhordan Stephens. 'How Drones Have Shaped the Nature of Conflict'. *Institute of Economy and Peace* (blog), n.d. https://www.visionofhumanity.org/how-drones-have-shaped-the-nature-of-conflict/#:~:text=As%20general%20drone%20use%20in,168%20per%20cent%20since%202018.

[4] Piyush Srivastava. 'Regulatory Landscape of Indian Drone Ecosystem'. n.d. https://legalaffairs.gov.in/sites/default/files/Civil%20Aviation%20Regulatory%20Landscape%20of%20Indian%20Drone%20Ecosystem%20red.pdf.

[5] Ibid.

[6] *Drone Rules, 2021*. The Gazette of India: Extraordinary, Controller of Publications, 25 August 2021, https://www.dgca.gov.in/digigovportal/jsp/dgca/homePage/viewPDF.jsp?page=InventoryList/headerblock/drones/Drone%20Rules%202021.pdf.

[7] Ibid.

[8]'The ICAO UAS Toolkit'. ICAO, n.d. https://www.icao.int/safety/UA/UASToolkit/Pages/default.aspx.

[9] Ibid.

[10] API architecture is usually explained in terms of client and server. The application sending the request is called the client, and the application sending the response is called the server. In the Digisky example, the Digisky database is the server, and the app serving the users is the client. https://www.geeksforgeeks.org/what-is-an-api/

[11] 'Operational Guidelines of the PLI Scheme for Drones & Drone Components'. Ministry of Civil Aviation, GoI, 29 December 2022. https://civilaviation.gov.in/sites/default/files/migration/Guidelines%20for%20the%20Operation%20of%20Production%20Linked%20Incentive%20Scheme%20(PLI)%20fro%20Drones%20and%20Drone%20Components%20(1).pdf.

[12] 'Dirctorate General of Foreign Trade Notification No 54/2015-2020'. DGFT, Govt of India, 9 February 2022. https://www.referencer.in/Baggage_Rules/Files/DGFT_Notification_No.54_2022.pdf.

[13] 'Drone Rules, 2021'. The Gazette of India: Extraordinary, Controller of Publications, 25 August 2021. https://www.dgca.gov.in/digigovportal/jsp/dgca/homePage/viewPDF.jsp?page=InventoryList/headerblock/drones/Drone%20Rules%202021.pdf.

[14] Piyush Srivastava. 'Regulatory Landscape of Indian Drone Ecosystem'. n.d. https://legalaffairs.gov.in/sites/default/files/Civil%20Aviation%20Regulatory%20Landscape%20of%20Indian%20Drone%20Ecosystem%20red.pdf.

[15] Rakesh Shreshta, Inseon Oh, and Shiho Kim. 'A Survey on Operation Concept, Advancements, and Challenging Issues of Urban Air Traffic Management'. *Frontiers in Future Transporttion* Volume 2-2021 (26 April 2021). https://doi.org/10.3389/ffutr.2021.626935.

[16] Concept and Graphics adapted from, Rakesh Shreshta, Inseon Oh, and Shiho Kim. 'A Survey on Operation Concept, Advancements, and Challenging Issues of Urban Air Traffic Management'. *Frontiers in Future Transporttion* Volume 2-2021 (26 April 2021). https://doi.org/10.3389/ffutr.2021.626935. Credits Victorportal.com.

[17] Piyush Srivastava, 'Regulatory Landscape of Indian Drone Ecosystem', https://legalaffairs.gov.in/sites/default/files/Civil%20Aviation%20Regulatory%20Landscape%20of%20Indian%20Drone%20Ecosystem%20red.pdf.

[18] 'Drone Rules, 2021'. The Gazette of India: Extraordinary, Controller of Publications, 25 August 2021. https://www.dgca.gov.in/digigovportal/jsp/dgca/homePage/viewPDF.jsp?page=InventoryList/headerblock/drones/Drone%20Rules%202021.pdf.

[19] 'Certification Criteria Evaluation Checklist'. National Test House (NR), Ghaziabad Certification of UAS Model, 2 June 2023. https://nth.gov.in/storage/dronecertifications/725d9fc1627a28ec1778e377c94fd29a12413de4_4.pdf.

[20] Data accessed from Digisky platform on 14 January 2025. https://digitalsky.dgca.gov.in/home.

[21] Data accessed from Digisky platform on 14 January 2025.https://digitalsky.dgca.gov.in/home.

[22] Ibid.

[23] 'National Unmanned Aircraft System Traffic Management Policy Framework'. Ministry of Civil Aviation, GoI, 24 October 2021. https://digitalsky.dgca.gov.in/assets/files/National-UTM-Policy-Framework-2021-24-Oct-2021.pdf.

[24] Ibid.

[25] Ibid.

[26] 'National Unmanned Aircraft System Traffic Management Policy Framework'. Ministry of Civil Aviation, GoI, 24 October 2021. https://digitalsky.dgca.gov.in/assets/files/National-UTM-Policy-Framework-2021-24-Oct-2021.pdf.

[27] Ibid.

[28] 'National Unmanned Aircraft System Traffic Management Policy Framework'. Ministry of Civil Aviation, GoI, 24 October 2021. https://digitalsky.dgca.gov.in/assets/files/National-UTM-Policy-Framework-2021-24-Oct-2021.pdf.

[29] Fact. MR. 'UTM Market', July 2024. https://www.factmr.com/report/unmanned-traffic-management-utm-market.

[30] 'Unmanned Aircraft System Traffic Management (UTM)', Federal Aviation Administration, updated upto 22 January 2025. https://www.faa.gov/uas/advanced_operations/traffic_management#:~:text=Unmanned%20Aircraft%20System%20Traffic%20Management%20(UTM)%20is%20a%20%22traffic,Traffic%20Management%20(ATM)%20system.

[31] Directorate-General for Mobility and Transport. 'Drones: Commission Adopts New Rules and Conditions for Safe, Secure and Green Drone Operations', 22 April 2021. https://transport.ec.europa.eu/news-events/news/drones-commission-adopts-new-rules-and-conditions-safe-secure-and-green-drone-operations-2021-04-22_en.

[32] Lappas, Vaios et al. 'EuroDRONE, a European Unmanned Traffic Management Testbed for U-Space'. *MDPI* 6, no. 2 (18 February 2022). https://doi.org/10.3390/drones6020053.

[33] *Business Standard*. 'Gadkari Unveils Advanced Drone Air Traffic Management System "Skye UTM"'. 8 February 2023. https://www.business-standard.com/article/current-affairs/gadkari-unveils-advanced-drone-air-traffic-management-system-skye-utm-123020801048_1.html.

[34] ADS-B provides real-time precision and shared situational awareness to pilots and air traffic controllers.

[35] 'SEVENTH SCHEDULE (Article 246) List I—Union List'. Source:Ministry of External Affairs, n.d. https://www.mea.gov.in/images/pdf1/S7.pdf.

[36] Brig Rajat Upreti. 'Contours Of Integrated Air Defence Command (IADC): An Overview'. *CENJOWS*, n.d.

[37] Ibid.

[38] Ibid.

[39] Chopra, Anil. 'Air Space Control: Challenges and Way Ahead'. *Air Power Journal* Vol. 13, no. No. 4 (December 2018). https://capsindia.org/wp-content/uploads/2022/08/Anil-Chopra.pdf.

[40] Bremer, Maximilian K., and Kelly A. Grieco. 'The Air Littoral: Another Look'. *The US Army War College Quarterly: Parameters* 51, no. 4 (17 November 2021): 67–80. https://doi.org/10.55540/0031-1723.3092.

[41] Ibid.

[42] Chopra, Anil. 'Air Space Control: Challenges and Way Ahead'. *Air Power Journal* Vol. 13, no. No. 4 (December 2018). https://capsindia.org/wp-content/uploads/2022/08/Anil-Chopra.pdf.

[43] Zachary Kallenborn. 'A Plague on the Horizon: Concerns on the Proliferation of Drone Swarms'. Issue Brief. Issue Brief No. 743. Observer Research Foundation, October 2024. https://www.orfonline.org/research/a-plague-on-the-horizon-concerns-on-the-proliferation-of-drone-swarms.

[44] Apratim Sharma. 'Counter-Unmanned Aircraft Systems (C-UAS) Future of Warfare'. *Manohar Parrikar Institute for Defence Studies and Analyses* Journal of Defence Studies, Vol. 16, no. No. 4 (December 2022): 221–41. https://www.idsa.in/system/files/jds/jds-16-4_Apratim-Sharma_13.pdf.

[45] 'The Comprehensive Guide to Counter-UAS'. Dedrone by Axon, n.d. https://www.dedrone.com/white-papers/counter-uas#:~:text=Counter%2DUAS%20Capabilities,-Detecting%20Drones&text=Counter%2DUAS%20systems%20are%20used,including%20radar%2C%20optical%20and%20acoustics.

[46] 'Countering Rogue Drones'. FICCI, in collaboration with EY, 2 August 2019. https://defence.capital/wp-content/uploads/2019/08/countering-rouge-drones.pdf.

[47] Apratim Sharma. 'Counter-Unmanned Aircraft Systems (C-UAS) Future of Warfare'. *Manohar Parrikar Institute for Defence Studies and Analyses* Journal of Defence Studies, Vol. 16, no. No. 4 (December 2022): 221–41. https://www.idsa.in/system/files/jds/jds-16-4_Apratim-Sharma_13.pdf.

[48] Ibid.

[49] No.11/11/2022-SS,Cabinet Secretariat,O/o Secretary(Security). https://cabsec.gov.in/writereaddata/circular/policyonjammer/english/1_Upload_3730.pdf

TAKSHASHILA
INSTITUTION

The Takshashila Institution is an independent centre for research and education in public policy. It is a non-partisan, non-profit organisation that advocates the values of freedom, openness, tolerance, pluralism, and responsible citizenship. It seeks to transform India through better public policies, bridging the governance gap by developing better public servants, civil society leaders, professionals, and informed citizens.

Takshashila creates change by connecting good people, to good ideas and good networks. It produces independent policy research in a number of areas of governance, it grooms civic leaders through its online education programmes and engages in public discourse through its publications and digital media.