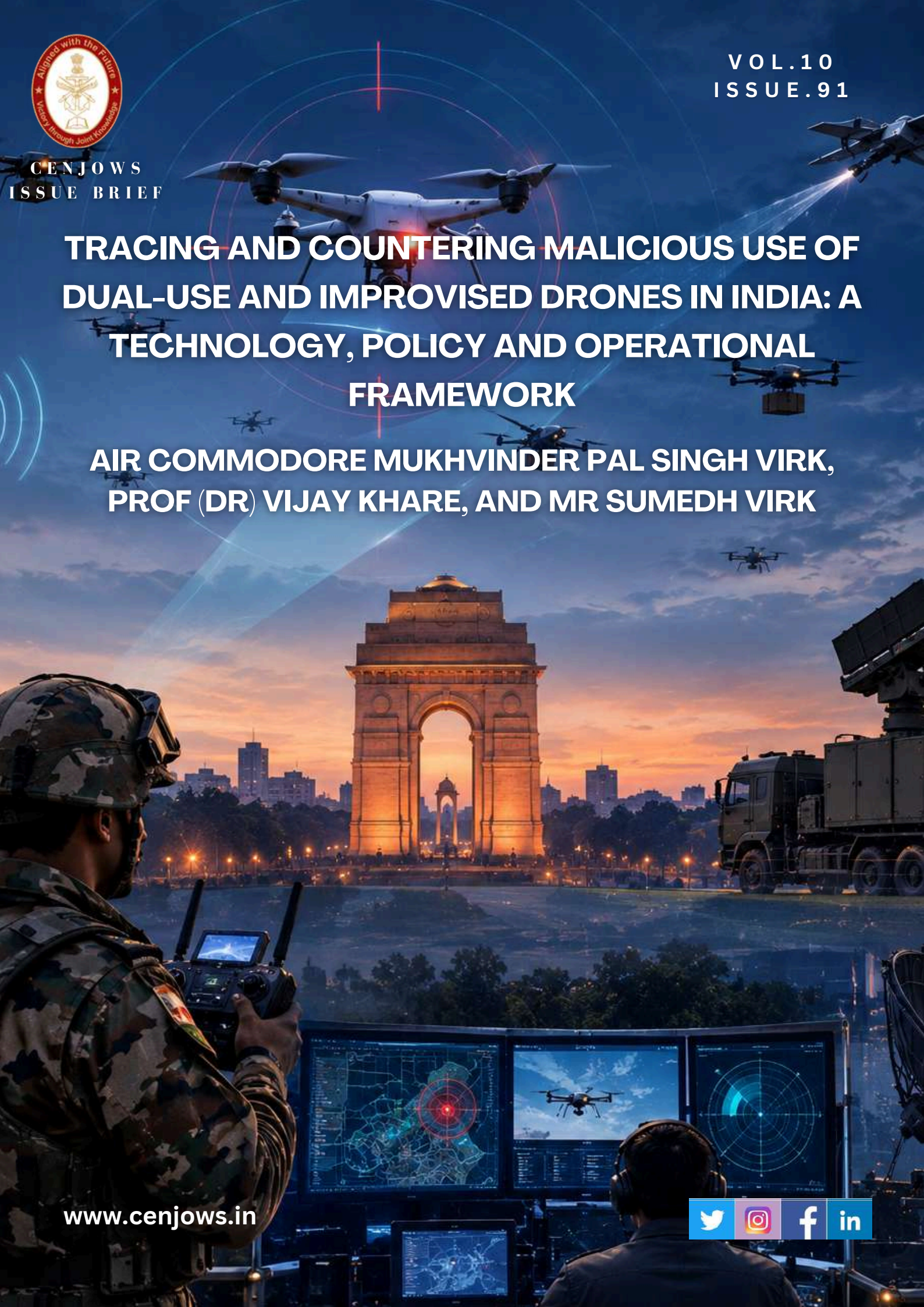
VOL.10
ISSUE.91

CENJOWS
ISSUE BRIEF

TRACING AND COUNTERING MALICIOUS USE OF DUAL-USE AND IMPROVISED DRONES IN INDIA: A TECHNOLOGY, POLICY AND OPERATIONAL FRAMEWORK

AIR COMMODORE MUKHVINDER PAL SINGH VIRK,
PROF (DR) VIJAY KHARE, AND MR SUMEDH VIRK



www.cenjows.in

CENJOWS ISSUE BRIEF

Volume 10 Issue 91 NOV 2026

CENJOWS

(Established: 2007)

Room No 301, B-2 Wing, 3rd Floor

Pt Deendayal Antyodaya Bhawan,
CGO Complex, Lodhi Road
New Delhi –110003 (INDIA)
Telephone Nos: 011-24364881, 24366485
Fax: 011-24366484
Website: www.cenjows.in
E-mail: cenjows@cenjows.in

ABOUT US

CENJOWS was raised in 2007 as an independent think tank, registered under the Societies Registration Act, 1860. This aims to promote Jointness as a synergistic enabler for the growth of Comprehensive National Power and provide alternatives in all dimensions of its applications through focused research and debate.

Starting Year : 2017

Year of Publication : 2026

Frequency : Weekly

Language : English

Publisher : Maj Gen (Dr) Ashok Kumar, VSM (Retd) Director General, CENJOWS

301, B-2 Wing, 3rd Floor
Pt. Deendayal Antyodaya Bhawan CGO Complex, Lodhi Road
New Delhi-110003

Editor : Maj Gen (Dr) Ashok Kumar, VSM (Retd) (dg@cenjows.in)

Deputy Editor : Dr Ulupi Borah, Distinguished Fellow (distinguishedfellow1@cenjows.in)

Editorial Board :

Brig K Ranjeev Singh, YSM (ddg@cenjows.in)
Col Ajay Kumar Rajak, SM (secy@cenjows.in)
Gp Capt Ashish Kumar Gupta (Retd) (seniorfellow2@cenjows.in)
Dr Ulupi Borah, Distinguished Fellow (distinguishedfellow1@cenjows.in)
Dr Monojit Das, Senior Fellow, PRO (monojit.das@cenjows.in)

301, B-2 Wing, 3rd Floor
Pt. Deendayal Antyodaya Bhawan
CGO Complex, Lodhi Road
New Delhi-110003

Publication Head : Ms Vaibhavi Katal

All correspondence may be addressed to:
Editor
Centre for Joint Warfare Studies (CENJOWS) 301, B-2 Wing, 3rd Floor
Pt Deendayal Antyodaya Bhawan CGO Complex, Lodhi Road
New Delhi-110003
Telephone: (91-11) 24366485/Telefax: (91-11) 24366484 e-mails:
cenjows@cenjows.in / cenjows@yahoo.com Website: http://cenjows.in

© Centre for Joint Warfare Studies

Price: Rs 300/- INR

All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage and retrieval system without permission from the DG, CENJOWS, New Delhi.

TRACING AND COUNTERING MALICIOUS USE OF DUAL-USE AND IMPROVISED DRONES IN INDIA: A TECHNOLOGY, POLICY AND OPERATIONAL FRAMEWORK

CONTENTS

Title	Page No
Abstract	**5**
Introduction	**6**
Research Methodology	**7**
Threat Landscape	**8**
Technical Tracing Framework	**10**
Digital Forensics	**12**
Blockchain and Distributed-Ledger Component Traceability	**13**
Detection and Monitoring Technologies	**14**
Non-Compliant Drone Detection in the Drone Rules 2021 Context	**16**
Layered Deployment Concept	**20**
Chip-Based Identification and Digital Tagging	**20**
Policy and Legal Framework: Reforming the Drones Rules 2021	**22**
Criminal Provisions and Legal Admissibility	**23**
Global Case Studies	**26**
India-specific Recommendations	**29**
Limitations	**36**
Conclusion	**37**

CENTRE FOR JOINT WARFARE STUDIES

CENJOWS

Tracing and Countering Malicious Use of Dual-Use and Improvised Drones in India: A Technology, Policy and Operational Framework





Air Commodore Mukhvinder Pal Singh Virk is presently serving as Principal Director with the IAF at the Aeronautical Development Agency (ADA), **Prof (Dr) Vijay Khare** is Senior Professor at Savitribai Phule Pune University, and **Mr Sumedh Singh Virk** is pursuing B.Tech in CSE at BMSCE, Bangaluru.

"In the contest of cheap drones and expensive defences, the side that sees, names and traces first, wins." Authors

Abstract

The strategic question for India is no longer whether dual-use drones will be misused, but how the country will trace, attribute and prosecute that misuse without smothering a legitimate civil drone economy. A small quadcopter sliding across the Punjab fence at night, a first-person-view platform recovered after a refinery probe, and an unregistered hexacopter loitering over a metro stadium, each event is a fragment. Each fragment, however, leaves a digital and physical trail. Battery chemistry, Pixhawk unique IDs, GNSS module signatures, MAC addresses, telemetry packets, and firmware hashes - these are ballistics of the unmanned age. Paper studies the ability to decode these signatures, which is what turns an isolated sighting into attribution and attribution into deterrence.

This paper builds an integrated framework across four layers. First, it studies technical architecture to trace and maps supply chain forensics, chip-level identity, embedded TPM modules, blockchain-anchored component ledgers and digital forensics for firmware and remote ID. Second, a layered detection and tracking grid combining radio-frequency triangulation, acoustic propeller-signature analysis, electro-optical / infra-red imagery with AI classification, radar micro-Doppler and multi-sensor fusion. Third, a conceptual ground-based integrated transmitter-receiver network — federating counter-UAS systems such as DRDO's anti-drone systems and international Sky Shield-type point defences with a national common operating picture under a proposed National UAS Threat Coordination Centre (N-UTCC). Fourth, a policy and policing reform agenda anchored on the Drone Rules 2021 and its visible enforcement gaps. Critically, the paper treats global lessons — Israel, the United States, China, Europe and Ukraine — not as imports but as data points calibrated against Indian terrain: cross-border drone corridors in Punjab and Jammu and Kashmir, coastal vulnerabilities from Mumbai to the Andamans, and the dense civil airspace of Indian metros. A forward look at AI-enabled drones, swarms and grey-zone employment frames the next three to seven years.

The paper concludes that the counter-drone problem in India is one-third technology, two-thirds governance — and that the costliest mistake would be to over-militarise civil airspace while leaving supply chains untraceable, evidence inadmissible and inter-agency seams unsewn. An indigenous capability roadmap, a risk matrix, technology readiness levels and a cost-effectiveness map are offered as decision aids. The objective is modest but firm: keep drone misuse a manageable risk, not a strategic surprise.

Keywords. Dual-Use Drones, Tracing, Attribution, Counter-UAS, Drone Rules 2021, SkyShield, Embedded Identity, Remote ID, Sensor Fusion, India National Security.

Introduction

There is a habit in Indian strategic conversations of treating the drone threat as a recent surprise. The first cross-border drops along the Punjab fence were reported in 2019; by 2024 the phenomenon was a steady tempo, not an exception. Recent conflicts and military operations demonstrated that even regular adversaries increasingly employ low-

cost unmanned aerial platforms as part of a wider concept of operations. In Jammu and Kashmir, terrorists have moved past curiosity into routine use of low-end UAS for surveillance and small payload delivery. The trend line is unforgiving.[1]

What makes the problem genuinely difficult is the dual-use character of the underlying technology. A DJI quadcopter that maps a power line on Monday can drop contraband on Wednesday. A Pixhawk autopilot built for a college research lab can equally guide a kamikaze run. The components do not change; the intent does. This is a classic governance challenge dressed up as a technology problem.[2]

The Drone Rules 2021 made a credible start. Registration on DigitalSky, airspace zoning, type certification, remote-pilot licensing and the introduction of remote identification all moved the needle. But the rules were written for the legitimate operator. The malicious operator does not register, does not certify and does not broadcast a remote ID. Closing that asymmetry is the work of this paper.[3]

This paper deliberately avoids tactical instruction. The purpose of this paper is to bridge the gap between technology, operations and governance by identifying what is technically possible, operationally viable and institutionally effective. It offers an integrated framework for policymakers, regulators and security practitioners, moving from threat assessment and attribution to detection, architecture design, policy reform and future challenges.[4]

The analysis is guided by a simple doctrinal principle: effective counter-UAS strategy rests on detection, attribution and accountability. You cannot interdict what you cannot see, you cannot prosecute what you cannot prove, and you cannot deter what you cannot attribute.[5]

This paper adopts a security-governance perspective, treating malicious drone use as a challenge that cannot be addressed through technology alone but requires integration of regulatory, institutional and operational mechanisms.

Research Methodology

This paper employs a qualitative analytical approach combining document analysis, comparative case-study assessment and technology-policy synthesis. The analysis is informed by official government publications, international regulatory frameworks,

academic literature, think-tank research, open-source intelligence (OSINT) and publicly reported drone incidents, with the aim of identifying key trends, capability gaps and governance challenges relevant to India's evolving counter-UAS environment. Incident trends presented in the paper are derived from open-source aggregation of reported events from government statements, media reporting, security analyses and international counter-UAS studies. The objective is not to produce a comprehensive incident database but to identify recurring patterns, capability trends and governance challenges relevant to India's evolving drone-security environment. Technical assessments of tracing, detection and attribution mechanisms are based on currently available commercial, governmental and research literature and are intended to inform policy development rather than provide operational instructions.

Threat Landscape

The Indian threat landscape is a layered one. The Indian threat landscape combines characteristics observed in contemporary conflicts, cross-border security environments and civil-aviation disruption scenarios, producing a uniquely complex counter-UAS challenge.[6]

Patterns of Misuse

- **Acquisition and Improvisation.** Commercial platforms, parts and software flow through open markets, e-commerce and grey imports. Local groups combine offline tradecraft with online tutorials. The cost of entry is a few months' rent.[7]
- **Roles and Missions.** Reconnaissance, smuggling, propaganda, IED delivery, kamikaze runs, sensor saturation. Indian operators of harm have, so far, concentrated on the first three; the assumption that they will not graduate to the rest is a planning indulgence.[8]
- **Innovation Hubs and Diffusion.** Contemporary conflicts demonstrate the rapid diffusion of military innovation. Tactics tested and refined in theatres such as Syria, Iraq and Ukraine frequently appear in Asia and Africa within months, making the transfer of operational lessons the rule rather than the exception.[9]

- **Hybridisation with Other Tech.** 3-D printing, encrypted comms, mesh radios and open-source autopilots together close the capability gap with state actors at a fraction of the cost.

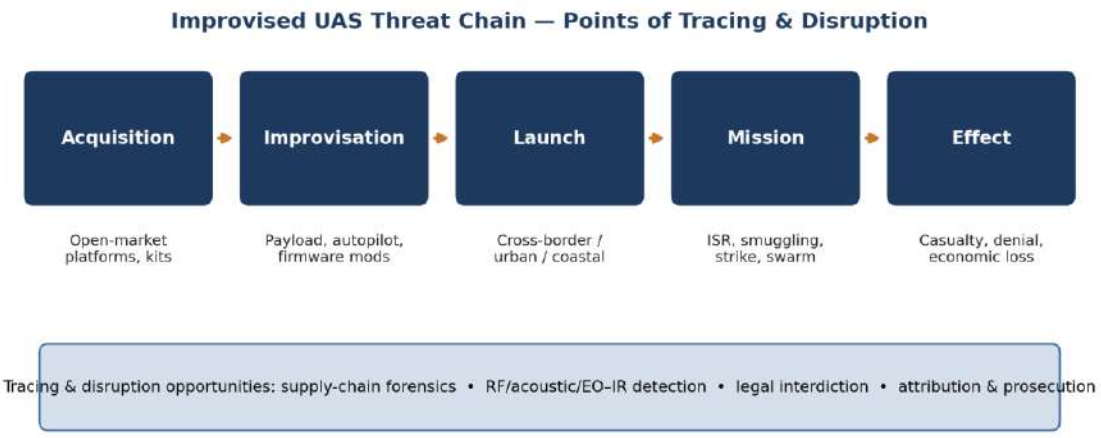


Figure 1. The improvised UAS threat chain — points of tracing and disruption **Source:** Author's own compilation.

Threat Vectors Specific to India

- **Western Border (Punjab, Rajasthan, J&K).** Repeated low altitude drops of narcotics, small arms and improvised payloads. The pattern is industrial in cadence, not opportunistic.[10]
- **Northern Frontier.** High-altitude reconnaissance and electronic environment interactions, where attribution and calibration of response are inseparable problems.[11]
- **North-East and Riverine Belts.** Jungle canopy and porous lines defeat radar; community reporting and acoustic sensing deserve far more weight here than in metros.[12]
- **Coastal and Maritime Zones.** Launches from small craft, fishing dhows or remote islands threaten ports, oil platforms and nuclear sites. The Andaman and Nicobar archipelago is a strategic exposure of the same type that the southern Philippines manages every day.[13]

- **Urban Critical Infrastructure.** Airports, refineries, metro corridors, crowded religious gatherings and sports venues. Even a benign quadcopter can shut down an airport for hours; even a packet of harmless powder, dropped into a procession, can produce a stampede. The economic and political costs of nuisance are not nuisance costs.[14]

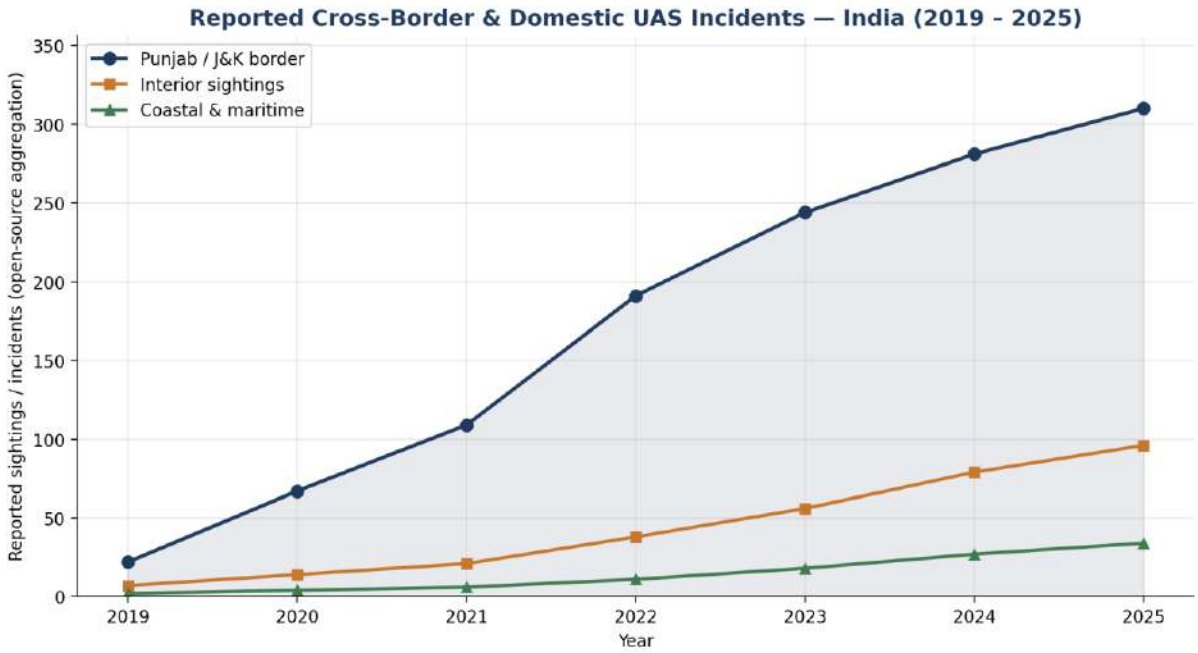


Figure 2. Illustrative trend derived from open-source reporting and incident aggregation

Source: Values represent author-generated trend estimates derived from publicly reported incidents and are intended only to illustrate directional patterns.

The trajectory is steep, but the more important point is shape: the curve in the Punjab/J&K belt has not flattened despite the deployment of point-defence systems and a regulatory regime. Cheap drones outpace expensive defences when the supply chain is unaccounted for. The implication is structural, not tactical.[15]

Technical Tracing Framework

Tracing the framework is important to carry out forensics on recovered drones. Drones/UAS are an assembly of components which can be identified and traced. They

are made up of physical components and electronic chips and have digital signatures that can survive crash, fire or tampering.[16]

Component-Level Forensics

Lithium-Polymer Batteries. Cell material and construction vary across manufacturers. These elements can be traced back to the producer. Further, battery-management-system (BMS) chips, metadata, batch and serial numbering can be a valuable source of forensic evidence. Along with supply-chain records and component-level analysis, these can assist in tracing the origin of the drones.[17]

Autopilot and Flight-Controller Boards. Pixhawk-class flight controllers and microcontrollers from the STM32, ESP32 and NXP families incorporate identifiers that can help in forensic and post-incident analysis in respect of drones.[18]

GNSS Modules. Drones such as, U-Blox, Quectel and DJI receivers have serial numbers, PVT (position-velocity-time) configurations, National Marine Electronics Association (NMEA) fingerprints, almanac data and proprietary message formats. These can serve as evidence. Further, GNSS chip-level extraction can also reveal the history of drone.[19]

RF and Telemetry Modules. TBS Crossfire, ExpressLRS, DJI O3, Wi-Fi and cellular modems each broadcast distinctive sequences. Software-defined-radio (SDR) data and recorded radio-frequency traffic can facilitate post-event reconstruction after incident.[20]

Motors, ESCs and Frames. Physical components often provide useful evidence for forensic. Electrical signatures for brushless motors, firmware-related evidence for electronic speed controllers and manufacturer-specific moulding or material characteristics for airframe of drones, can be good source of evidence. While no single indicator is necessarily determinative, the cumulative assessment of such

artefacts can contribute significantly to provenance determination and post-incident investigation.[21]

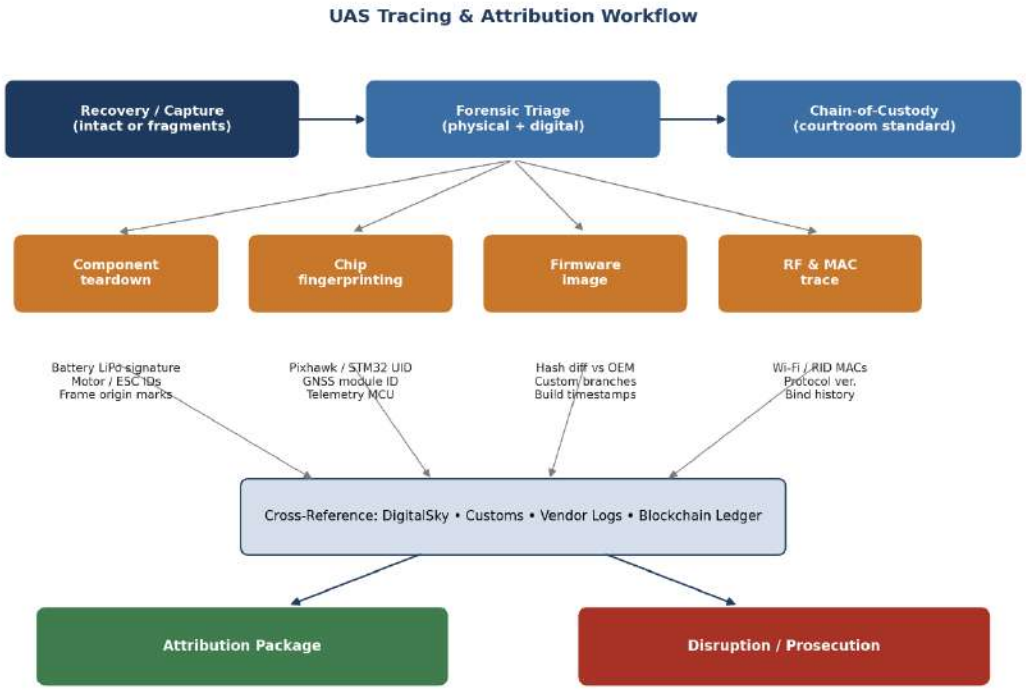


Figure 3. UAS tracing and attribution workflow, from recovery to prosecution. **Source:** Author's own compilation.

Digital Forensics

- **Firmware Fingerprinting.** ArduPilot, PX4, Betaflight and DJI firmware possess known cryptographic hashes that can be used for verification. A hash mismatch indicates a custom build. Departures from known firmware baselines can provide valuable forensic and intelligence leads. Customised or modified software may retain compiler signatures, build metadata, timestamps and developer-specific identifiers that can assist in attribution effort. Firmware-hash comparison has become a standard digital-forensic technique. Cryptographic hashes allow investigators to determine whether recovered software corresponds to a known manufacturer or a modified variant.[22],[23]
- **MAC Address Tracing.** Wi-Fi and Bluetooth modules carry IEEE-allocated organisationally unique identifiers (OUIs). Even when a module is tampered, the

OUI can trace the vendor and the integrator. Remote-ID frames that include the manufacturer code add a second corroborating line.[24]

- **Embedded Chip IDs.** Beyond the autopilot UID, the GNSS chip ID, the IMU sensor IDs, the radio transceiver IDs and the camera ISP IDs together form a multi-fingerprint that is far harder to forge than any one identifier on its own.[25]
- **Remote-ID Spoofing Detection.** Remote ID was always going to be spoofed. Several aviation regulators and counter-UAS researchers have observed that broadcast-based Remote ID systems were designed primarily for airspace awareness and safety rather than adversarial security environments. Consequently, authentication, cryptographic integrity and multi-sensor verification are increasingly viewed as necessary future enhancements.[26]

  The question is whether the spoof is detectable. Cross-correlation of broadcast position with radar return, with RF angle of arrival, and with EO/IR confirms or denies the broadcast. Drift between broadcast and observed track is a near-perfect spoof indicator.
- **Manufacturing-Origin Intelligence.** Customs declarations, courier waybills, e-commerce purchase records and vendor support logs together reconstruct procurement. Indian Customs already maintains the data; the gap is the legal and technical pipeline that turns it into admissible evidence in a drone case.[27]

Blockchain and Distributed-Ledger Component Traceability

A widely discussed but rarely operationalised proposal is to anchor critical drone components on a permissioned distributed ledger. The proposition is straightforward: at the point of manufacture, each batch of batteries, each autopilot board, and each GNSS module is registered with a hash of its serial number, factory, batch and date. Distributors, integrators and end-buyers add transactions as the part moves. When a damaged board is recovered after an incident, its UID is queried; the ledger returns a verifiable history. The system does not prevent diversion, but it makes post-incident attribution dramatically faster and removes plausible deniability from middlemen.[28]

The Indian use case is unusually strong, given the existing DigitalSky platform, the maturity of Aadhaar-grade public infrastructure and the country's comfort with permissioned ledgers in supply chains. A National Component Ledger (NCL) for UAS, federated with customs, GST and DigitalSky, is proposed in the policy section.[29]

Although distributed-ledger solutions are not a substitute for regulation or enforcement, they have demonstrated utility in pharmaceutical traceability, logistics management and critical supply-chain assurance. Their value lies less in prevention and more in accelerating post-incident attribution and evidentiary reconstruction.[30]

While no major jurisdiction has yet implemented a comprehensive blockchain-based drone-component traceability regime, comparable approaches have been employed in pharmaceutical and high-value logistics supply chains.

Detection and Monitoring Technologies

Single-sensor counter-UAS is a marketing fiction. Every modality has a blind spot. RF detection fails the moment a drone goes autonomous and silent. Radar struggles with tiny radar cross-sections and ground clutter. Acoustic sensors lose ground in wind or urban noise. EO/IR is wonderful at twenty metres and helpless at five kilometres; sensor fusion is the optimal solution.[31]

- **RF Signal Detection and Triangulation**

  RF detection works on two assumptions. First is that the drone communicates and secondly that the communication is recognisable. Both hold for the commercial and dual-use platforms. A distributed network of RF sensors, each with an SDR at the front end and a known time stamp, can triangulate an emitter to within tens of metres. Spectrum analysis identifies the protocols, models and fingerprinting used in generic 2.4 GHz or 5.8 GHz frequency systems. The output is generated in bearing, range and model used.[32]

- **Acoustic Detection**

  Multirotor and fixed-wing unmanned systems generate acoustic signatures in terms of frequencies and harmonics in the low-frequency to mid-frequency bands.

This depends on propeller design and operating conditions. Microphone arrays of four to eight elements give reliable detection in calm conditions to several hundred metres. Further, doppler-shift analysis adds a coarse range rate. The main limitation is wind noise; however, the advantage is that acoustic sensing remains effective when the drone has gone silent on the RF side.[33]

- **EO/IR with AI Classification**

  Electro-optical (EO) and thermal cameras, paired with a modern object-detection system, classify drone from birds or balloons at predictable engagement ranges. The recent generation of edge accelerators makes such classifiers tractable on a pole-mounted camera with modest power. The classifier matters more than the sensor: a YOLO-class network fine-tuned on Indian skies, with a library of common civil airframes alongside known threat platforms, is the operational asset.[34]

- **Radar Micro-Doppler**

  X-band and Ku-band radars can detect drone-sized targets at several kilometres, depending on cross-section and clutter environment. The most useful classification feature is the doppler signatures generated by rotating propellers and other moving components. The resulting time-frequency patterns provide distinctive target characteristics that can be analysed using machine-learning techniques to distinguish drones from birds and other airborne objects and to classify broad categories of unmanned systems, including multirotor and fixed-wing platforms, with a high degree of reliability.[35]

- **Multi-Sensor Data Fusion**

  The fusion engine is the central technical claim of any serious counter-UAS architecture. Modern counter-UAS systems typically employ track-level fusion algorithms, including probabilistic data-association filters and machine-learning-based approaches, to integrate detections from RF, radar, EO/IR, acoustic and Remote ID sources. The resulting fused tracks provide a consolidated operational picture with quantified confidence measures relating to target identity, classification and trajectory. Multi-sensor data fusion (MSDF) offers significant

benefits in terms of performance, as it can offset limitations of one sensor by the strengths of another. Integrated architectures achieve lower false-alarm rates, improved classification accuracy and greater robustness under diverse environmental conditions.[36]

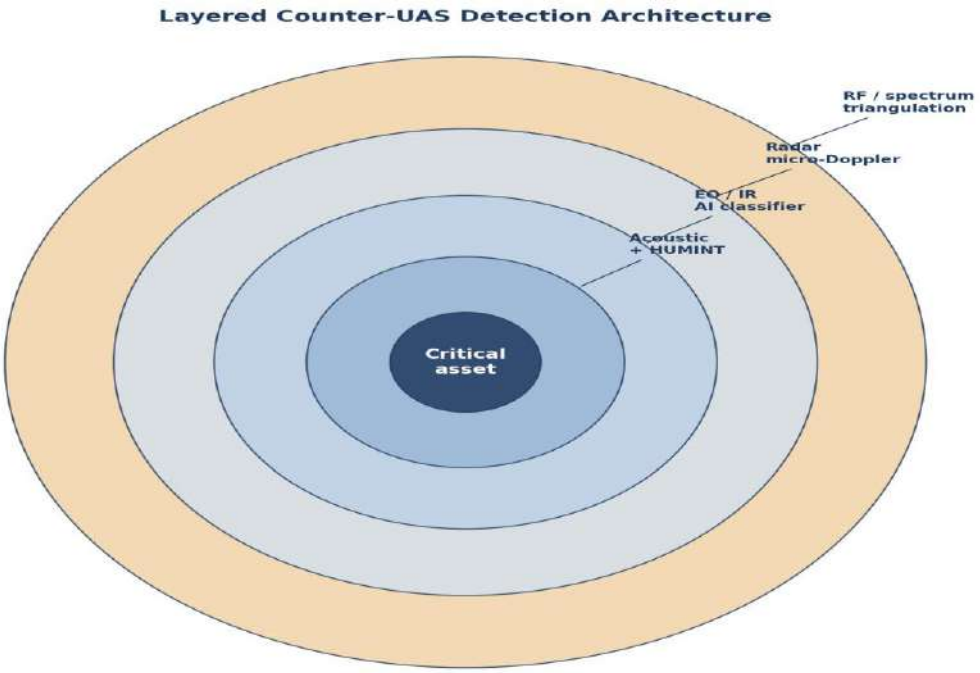


Figure 4. Layered counter-UAS detection architecture around a critical asset. **Source:** Author's own compilation.

Non-Compliant Drone Detection in the Drone Rules 2021 Context

The Drone Rules 2021 establish registration, classification and remote identification for civilian operators in India. The framework is sound on paper. The operational difficulty is that the threat actor is, by definition, non-compliant. Detection of the non-compliant drone is therefore the harder half of the problem.[37]

Signatures of Non-Compliance

- **Absent or invalid Remote ID broadcast.** An aircraft seen on radar or EO/IR with no corresponding Remote-ID frame is, ipso facto, non-compliant. The DigitalSky backend should be queried in real time.

- **Mismatched Remote ID and observed track.** Spoofed Remote-ID is detectable by cross-correlation with radar and EO/IR tracks.
- **Operation in the red or yellow zone without clearance.** Geofencing on compliant manufacturer firmware blocks such flights; their occurrence indicates either firmware tampering, a non-compliant manufacturer, or both.
- **RF protocol or telemetry inconsistent with any registered model.** Custom autopilot stacks are perfectly legal in the maker community, but their appearance in a sensitive geography deserves a second look.

Limitations of Remote ID and Spoofing Vulnerabilities

Remote ID was designed as an aviation-safety tool, not a security tool. A significant limitation of many existing Remote-ID architectures is the lack of cryptographic authentication of broadcast identity information. Consequently, Remote-ID data may be vulnerable to spoofing, impersonation or manipulation in adversarial environments. Strengthening the integrity and trustworthiness of such systems will require the adoption of cryptographically signed identity frameworks, in which each airframe possesses a unique cryptographic credential protected by a hardware root of trust, such as a Trusted Platform Module (TPM) or an equivalent secure element. Until that is mandatory, every Remote-ID frame must be treated as a claim, not a fact, and corroborated by independent sensors.[38]

Detection of Dark and GPS-Denied Drones

“Dark drone” in this paper means a UAS that broadcasts no Remote-ID, emits no command-and-control RF (because it is operating on a pre-loaded mission) and uses inertial or visual-odometric navigation rather than GNSS. Such a drone is a deliberate engineering choice by an adversary and represents the upper end of the threat. RF detection is useless against it; the remaining tools are micro-doppler radar, EO/IR with AI, acoustic sensing and the eyes of the public.[39]

The doctrinal phrase here is unavoidable: against the dark drone, sensor diversity is not a luxury; it is the only defence.

Ground-Based Integrated System Architecture

The conceptual architecture below treats counter-UAS as a national common operating picture problem rather than a perimeter-defence problem. SkyShield-type point defences continue to matter at the asset level; what they do not do, and were never meant to do, is integrate across thousands of nodes and dozens of jurisdictions. That is the work of the proposed N-UTCC.[40]

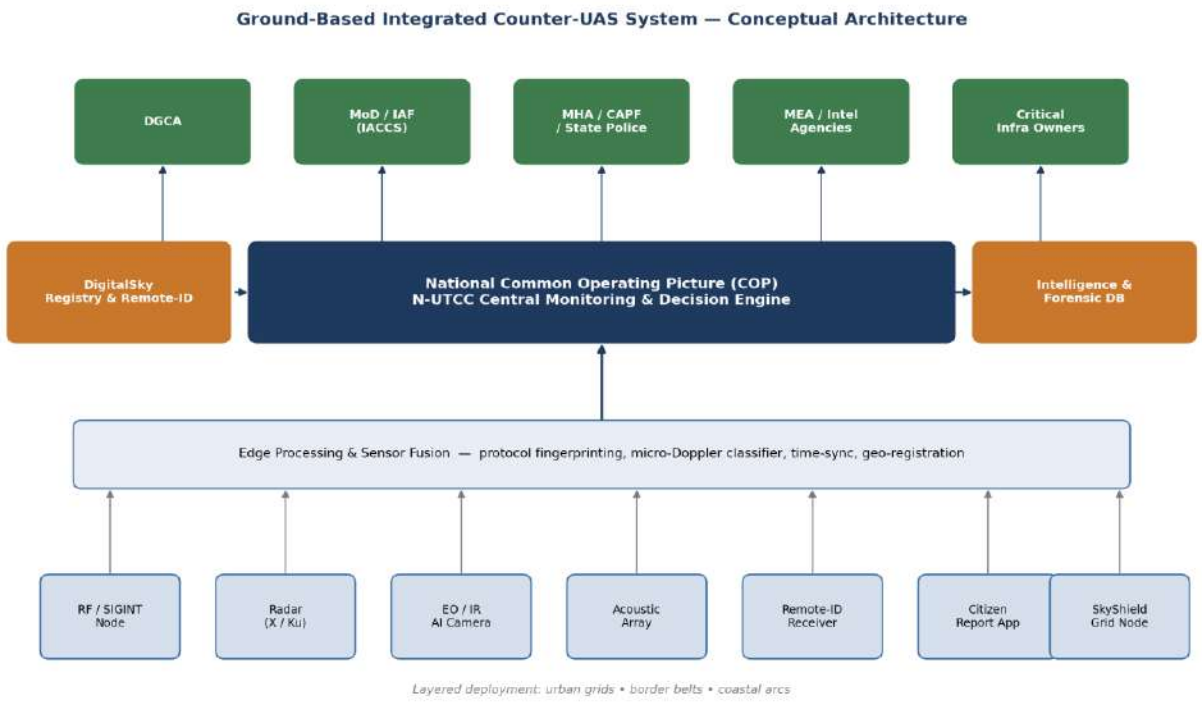


Figure 5. Ground-based integrated counter-UAS system — conceptual architecture (sensors, edge fusion, central monitoring, federated databases, consumer agencies). **Source:** Author's own compilation.

Sensor Layer

RF SIGINT nodes, radar, EO/IR cameras, acoustic arrays, Remote-ID receivers, the citizen reporting application and SkyShield-type class grid nodes all live at the sensor layer. Density is the design variable. Urban grids deserve thick coverage with EO/IR and Remote-ID; border belts deserve long-range radar and RF; coastal arcs deserve a mix weighted toward radar and surface-search fusion.[41]

Edge Processing and Fusion Layer

Each sensor cluster feeds an edge-processing node responsible for protocol fingerprinting, micro-Doppler classification, time synchronisation and geo-registration. Performing these functions at the edge enables preliminary data processing close to the point of collection, reducing bandwidth demands, lowering latency and improving the scalability of the overall system architecture. The edge processor emits compact track files to the centre.

Central Monitoring and Decision Engine

The proposed N-UTCC core ingests track files from every edge processor across the country. It maintains the national common operating picture, fuses tracks across overlapping jurisdictions, runs threat-classification heuristics, and dispatches alerts. Critically, it is not a kill chain. Designation of a target as hostile, and any decision to interdict, remains with the empowered human commander — military for cantonments and active borders, police for civil airspace, with pre-agreed transfer rules.[42]

Federated Database Layer

Two federated stores anchor the architecture: DigitalSky (registry and Remote-ID) and an Intelligence and Forensic Database. The proposed National Component Ledger sits alongside DigitalSky. Customs, GST, courier and e-commerce data feed the forensic store under appropriate legal authority. Federation, not centralisation, is the design principle — the data stays where the law leaves it, only the queries cross.

Consumer Agency Layer

DGCA receives compliance and traffic information; the IAF's Integrated Air Command and Control System (IACCS) receives military-grade tracks; MHA, the CAPFs and state police receive police-action alerts; MEA and intelligence agencies receive cross-border attribution packages; private critical-infrastructure owners receive site-level advisories. Each consumer sees only what it needs.

Layered Deployment Concept[43]

- **Urban deployment.** Dense Remote-ID receivers, EO/IR poles every few hundred metres around critical sites, RF triangulation in three-sensor clusters, citizen reporting front and centre. The operational challenge is discrimination, not detection.
- **Border deployment.** Long-range radar and RF, with EO/IR fill-in, acoustic stretches in canopy terrain and a tight integration with the Border Security Force's existing electro-optical fences. The challenge is sustained vigilance over hundreds of kilometres.
- **Coastal deployment.** An integrated maritime counter-UAS architecture should combine surface-search and drone-detection radars, EO/IR sensors deployed on coastal surveillance infrastructure, Coast Guard assets operating as mobile RF-sensing nodes, and dedicated sensor coverage across strategically significant areas such as the Andaman and Nicobar archipelago. The principal operational challenge stems from the geometry of the maritime environment: drones launched from small vessels can emerge within the surveillance or engagement horizon with little warning, leaving limited time for detection, classification and response.

Chip-Based Identification and Digital Tagging

Every layer of the framework above runs into the same hard wall: the device identity it relies on must itself be trustworthy. A Pixhawk UID is an excellent fingerprint; it is a poor authenticator. The next mandatory step in the Indian regime is hardware-rooted identity for civil drones above a defined mass and capability threshold.[44]

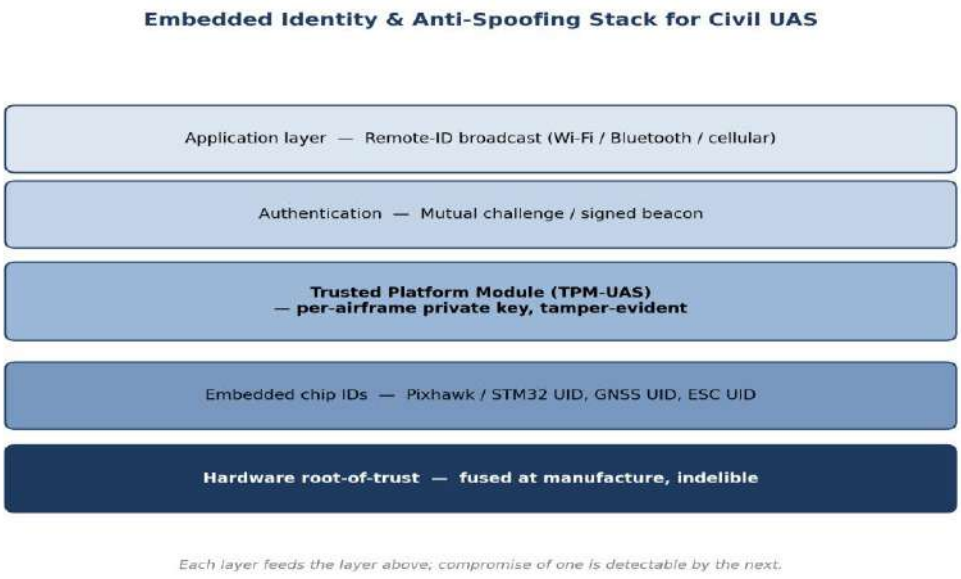


Figure 6. Embedded identity and anti-spoofing stack for civil UAS. **Source:** Author's own compilation.

Hardware Root of Trust

A small trusted-platform module (hereafter TPM-UAS), no larger than a postage stamp, anchored at manufacture into the airframe and bound cryptographically to the autopilot, is the minimum viable hardware root of trust. TPM-UAS is presented as a conceptual architecture for future policy consideration. The private key never leaves the chip; the public key is registered with DigitalSky at the point of registration. Every Remote-ID frame, every flight log and every firmware update is signed by the TPM. This TPM-UAS is a proposed architecture derived from established trusted-computing principles rather than a currently fielded Indian capability.[45]

The concept draws upon hardware-root-of-trust architectures already employed in trusted-computing environments, secure mobile platforms and industrial control systems. Although implementation challenges remain, hardware-based identity mechanisms offer a robust means of enhancing authentication, reducing the risk of spoofing and strengthening digital attribution.

Mandatory Tagging of Critical Components

Beyond the airframe, key components — battery packs above a defined energy threshold, autopilots, GNSS modules and RF transceivers — should each carry tamper-evident identity tags. Where the silicon already exposes a UID (STM32, u-blox, ESP32), the regulation can demand exposure rather than fabrication. Where the component does not, a low-cost authenticated micro-tag (Microchip ATECC-class, NXP A1006 or domestic equivalent) suffices.

Anti-Spoofing Authentication

Mutual challenge-response between the TPM-UAS and the ground monitoring infrastructure converts Remote ID from a broadcast claim into a verified attestation. The cryptographic overhead is trivial; the legal and forensic value is large, because a signed Remote-ID frame, tied to a registered public key, is courtroom-grade evidence rather than circumstantial telemetry.

The structural shift is simple to state and difficult to engineer, moving from “the drone says it is X” to “the drone proves it is X”.

Policy and Legal Framework: Reforming the Drone Rules 2021

The Drone Rules 2021 were drafted to liberalise the over-regulated sector. That goal remains valid. The reforms proposed below strengthen the original rules.

Mandatory Component Traceability

Type certification today addresses the airframe in respect of commercial drones. It should be extended to the principal subsystems such as autopilot, GNSS, RF transceiver and energy storage devices. Each certified subsystem should have identity (TPM, micro-tag or exposed UID). Further, each act of import, sale, transfer and integration must be logged in the proposed National Component Ledger. This legal model already exists for pharmaceuticals and explosives.

Supply-Chain and Import Regulation

Customs HS codes for drone components are coarse. A finer set of codes for autopilots, components above defined power ratings, FPV transmitters above defined output and specific GNSS modules are needed. This would let Customs apply differential scrutiny without affecting legitimate users. Coordination with customs authorities from neighbouring countries strengthens interdiction at borders itself.

Licensing of Critical Components

Three categories warrant targeted regulatory oversight: long-range RF systems operating beyond prescribed power and frequency limits, GNSS modules equipped with anti-jam features, and advanced lithium battery chemistries with significant dual-use potential. Such measures should be implemented through a proportionate, risk-based licensing framework that strengthens security while preserving the innovation ecosystem essential for the growth of India's indigenous drone industry. But the present blanket exemption is too generous.

Criminal Provisions and Legal Admissibility[46]

- **Specific offences.** Operating in a restricted zone, tampering with Remote-ID, and using a UAS to deliver a controlled substance or weapon should each be standalone offences with calibrated penalties. Today, prosecutors stitch these together from older statutes, weakening cases at trial.
- **Forensic admissibility.** The Bharatiya Sakshya Adhiniyam (BSA), 2023, provides a legal framework for the admissibility of electronic and digital evidence**.** However, specialised guidance, standard operating procedures and evidentiary standards may be required to ensure the consistent collection, preservation, authentication and presentation of drone-related digital artefacts, including firmware hashes, chip identifiers, RF capture logs and Remote-ID records.
- **Cross-border evidence sharing.** Mutual legal assistance treaties (MLATs) need a UAS annexure: standardised forensic packages, defined timelines, agreed forensic standards.

Roles of DGCA, MHA and MoD

The cleanest division of labour is functional, not territorial. DGCA owns registration, compliance and the integrity of DigitalSky and the National Component Ledger. MHA, through the CAPFs and state police, owns civil airspace enforcement, investigations and prosecutions. MoD, through the Service Headquarters, owns the response in active border airspace and around defence installations. The proposed N-UTCC sits structurally under MHA but with permanent representation from MoD, DGCA, MEA, intelligence agencies and the Coast Guard, mirroring the model the reference paper proposed and that the European experience validates.

Provision area	Current state (2021 rules)	Identified gap	Proposed reform
Registration	Mandatory above 250 g via DigitalSky	Self-declared identity; non-compliant actors invisible	TPM-bound airframe ID; cryptographic Remote-ID
Remote ID	Broadcast-only; unauthenticated	Trivially spoofable	Signed Remote-ID with challenge-response
Component certification	Airframe-level only	No traceability of autopilot, GNSS, RF, battery	National Component Ledger; chip-level identity tags
Imports	Restricted but coarse HS codes	Grey-market routes for components	Finer HS codes; coordinated customs scrutiny
Offences	Stitched from older statutes	Weak prosecutions; uneven sentencing	Specific UAS offences;

Provision area	Current state (2021 rules)	Identified gap	Proposed reform
			admissibility for digital evidence
Enforcement	DGCA + state police, undefined seam	Inter-agency lag	Proposed N-UTCC with pre-agreed civil-military transfer rules
Privacy	Limited mention	Surveillance creep risk	Statutory oversight; data minimisation

Table 1. Drone Rules 2021 — current provisions, identified gaps and proposed reforms.

Institutional and Policing Reforms

Rules without institutions are slogans. The institutional architecture for counter-UAS in India needs an explicit centre of gravity, dedicated technical units, trained investigators and a credible inter-agency rhythm.

State UAS Cells and Drone Forensic Laboratories

Each state should host a UAS Cell within the police, with a defined complement of cyber-forensic examiners, RF specialists and physical-evidence handlers. At the national level, two or three Drone Forensic Laboratories — co-located with existing Central Forensic Science Laboratories — should hold the deeper teardown, chip-extraction and firmware reverse-engineering capability. The state cells handle ninety per cent of routine cases; the national labs handle the hard ten per cent and set standards for the rest. [47]

CAPF and Intelligence Upgrades

Border-management agencies, including the Border Security Force, Sashastra Seema Bal, Indo-Tibetan Border Police and the Indian Coast Guard, require counter-UAS capabilities tailored to the distinct operational and geographic characteristics of their

respective areas of responsibility. The pattern should favour mobility and depth over fixed installations. Intelligence agencies need a dedicated UAS tasking cell with linguists, open-source intelligence (OSINT) capacity and the ability to push tip-offs into the police chain in near real time.

Training Doctrines

- **Investigator training.** A six-week core curriculum at the Central Detective Training Institutes covering safe handling, evidence preservation, basic teardown, RF capture and digital forensics. Annual refresh.
- **Tabletop exercises.** Quarterly civil–military–police tabletops simulating airport intrusion, refinery probe, religious procession drop, coastal launch and swarm event. Lessons should be written, not whispered.
- **Joint live exercises.** Annual exercises across at least four geographies — western border, northeast, metro airport, and coastal arc. The audience: state police, CAPF, IAF, Navy, Coast Guard, DGCA, the infrastructure operator concerned, and the prosecutor's office.
- **Curriculum at staff colleges.** Defence Services Staff College, College of Air Warfare, College of Defence Management and the National Police Academy must each carry a counter-UAS module. Doctrine without institutional study atrophies.

Inter-Agency Coordination

The proposed N-UTCC is the spine. State UAS Cells are the limbs. The intelligence community is the nervous system. The most often misjudged seam is the police–military one, particularly in the immediate aftermath of an incident in or near a cantonment. Pre-agreed transfer rules — who has primacy, when does the file move, how is evidence preserved — must be written, exercised and endorsed at the level of the Cabinet Committee on Security.[48]

Global Case Studies

Lessons from abroad are useful only when they survive translation. India is not Israel. India is not Ukraine. India is, however, comparable in different parts of its threat landscape

to different countries simultaneously, which is why a case-study basket — not a single model — is the right tool.

Israel — Layered Defence at the Threshold of Civil and Military

Israel has lived with the rocket-and-drone problem at the borders of its civil airspace for over two decades. The Iron Dome family handles ballistic threats; the counter-UAS layer evolved around Drone Dome, Rafael's Drone Guard and an unusually tight civil–military interface. Two specific lessons translate. First, the civil–military seam is permanent and must be staffed permanently, not assembled in a crisis. Second, electronic-warfare-led soft kill is preferred over hard kill in populated airspace, even at the cost of leakage, because hard kill in dense civilian terrain is its own form of damage.[49]

United States — Federal Architecture and Interagency Friction

The American experience is instructive precisely because it is messy. Counter-UAS authorities are split between the Department of Defence, the Department of Homeland Security, the Department of Justice and the Federal Aviation Administration, with a complex pattern of who may detect, who may track and who may engage. Recurrent legislative tweaks — most notably the Preventing Emerging Threats Act and successive National Defence Authorisation Acts — extend authorities incrementally. The lesson for India is to write its authorities completely, once, rather than to absorb a decade of fragmentation. The Federal Aviation Administration's Remote-ID rule, though imperfect, is the most influential civil instrument; it is being studied, sensibly, by DGCA.[50]

China — Vertical Integration, Indigenous Standards and the DJI Question

China is simultaneously the world's largest exporter of civil drones and one of the most tightly regulated civil drone airspaces. Its model — vertical integration of manufacturer, registration, geofencing and law-enforcement access — yields strong control but at the cost of monoculture risk and trust deficit abroad. India can learn the regulatory craft (mandatory geofencing that survives firmware updates, manufacturer cooperation with law enforcement) without importing the political model. The DJI question — how a country with a sensitive border manages a technology stack dominated by a single foreign vendor — is one India must answer explicitly. The answer is unlikely to be a ban; it is more likely

a combination of indigenous alternatives, certified configurations and selective procurement restrictions for sensitive users.[51]

Europe — Governance-Led Counter-UAS

The European experience, captured well by EASA's civil-aviation-led framework and the Geneva Centre for Security Policy's critical-infrastructure work (EASA, 2022; GCSP, 2023), is the closest civil-airspace analogue to India's situation. Repeated airport disruptions in the United Kingdom, protests around French nuclear sites, and Eastern European border-anxiety incidents — Europe has handled them by treating the drone problem as governance first and technology second. India's metropolitan and aviation context maps onto this experience with surprisingly little friction. The N-UTCC concept is an Indian version of the European inter-agency model.[52]

Ukraine — The Innovation Cauldron and Its Diffusion Risk

The conflict in Ukraine has highlighted two important trends: the emergence of first-person-view (FPV) drones as a pervasive feature of modern warfare and a dramatic acceleration in the pace of battlefield innovation, with adaptation cycles increasingly measured in weeks rather than years. Cheap First-Person-View platforms, fibre-optic-tethered drones to defeat jamming, ground-to-air drone-on-drone interceptors, autonomous terminal homing — each of these techniques is now in open literature, open video and open commerce. The diffusion risk for India is severe and proximate: techniques developed on the Donbas front are visible in adversary literature within weeks. For India, the lessons emerging from Ukraine should be viewed not as distant observations but as indicators of trends that are likely to influence future operational environments and security challenges.[53]

Jurisdiction	Dominant approach	Key strength	Caution / limitation	Applicability to India
Israel	Civil–military fused; soft-kill preference	Permanent inter-agency staffing	Small geography; high cost	Civil–military seam doctrine

Jurisdiction	Dominant approach	Key strength	Caution / limitation	Applicability to India
United States	Statute-led, agency-distributed	Mature legal frameworks	Authority fragmentation	Write authorities completely once
China	Vertically integrated regulator + manufacturer	Strong geofencing & registration	Monoculture; trust deficit	Regulatory craft, not political model
Europe (EU/UK)	Governance-first, civil-aviation-led	Inter-agency rhythm; proportionality	Variation across states	Closest analogue for Indian metros
Ukraine	Battlefield innovation; mass FPV	Speed of doctrine refresh	Diffusion to non-state actors	Treat as forecast, not tutorial

Table 2. Comparative counter-UAS lessons across jurisdictions and their applicability to India.

India-Specific Recommendations

The recommendations below need to be implemented. They avoid tactical instructions that could enable misuse, and they are grouped to map onto existing institutional owners.

Detection Grid

- **Border belt.** Layered radar + RF along the western and northern fronts, federated through the existing Comprehensive Integrated Border Management System (CIBMS) backbone. Acoustic stretches in canopy terrain on the eastern frontier.
- **Coastal arc.** Marriage of surface-search and drone-detection radar at major ports, with EO/IR cover at high-value sites and a dedicated Andaman and Nicobar arc.

- **Urban grids.** Remote-ID receivers as standard infrastructure on traffic poles and metro stations in tier-1 cities; EO/IR clusters at airports and stadiums; citizen reporting through a national app.

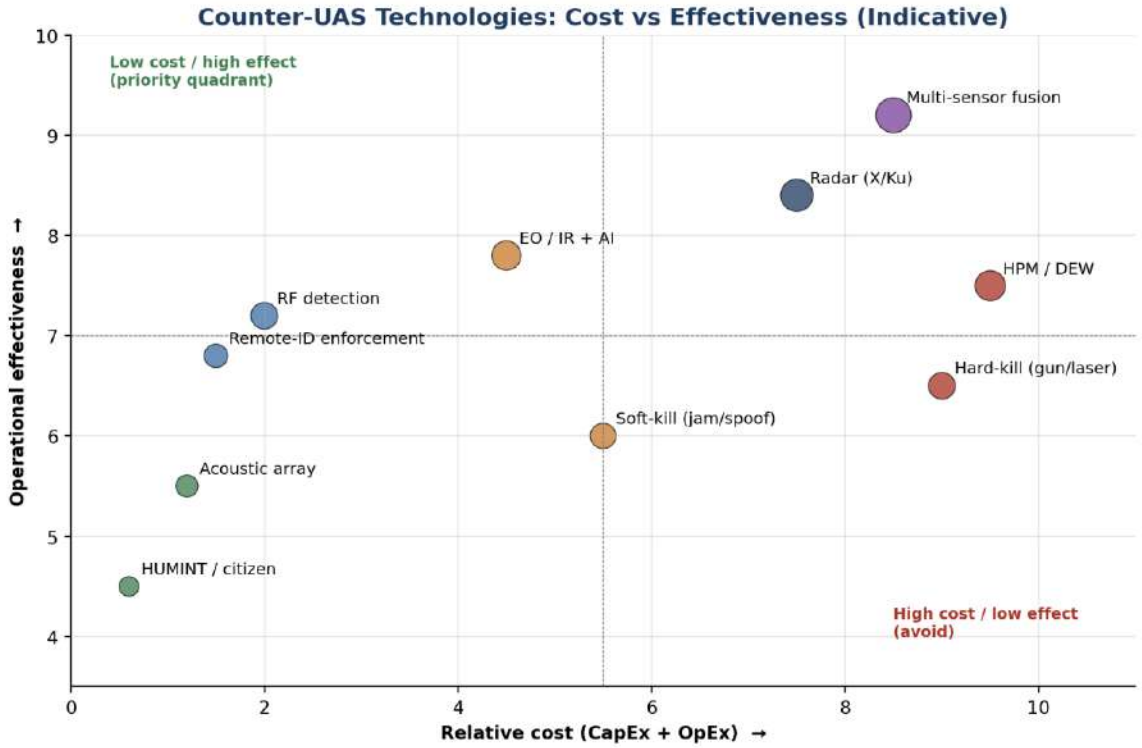


Figure 7. Counter-UAS technologies — indicative cost vs effectiveness map.

Source: Author's own compilation.

The cost-effectiveness map is indicative, not prescriptive. Two observations are robust. First, multi-sensor fusion sits in the upper-right quadrant — it is genuinely worth the spend. Second, Remote ID enforcement and citizen reporting are in the lower-left bargain quadrant — quietly the most important early investments.

Tracing Backbone

DigitalSky 2.0 with TPM-bound airframe identity, federated with a National Component Ledger, and connected to Customs, GST and the major e-commerce platforms under a defined access regime. Two or three drone forensic laboratories, state UAS Cells, and a forensic standard published by the Bureau of Indian Standards.

Governance Spine

The proposed N-UTCC will be under MHA with permanent representation from MoD, DGCA, MEA, intelligence agencies and the Coast Guard. State UAS cells be linked to N-UTCC. Civil–military operating protocol issued at the Cabinet Committee level. Annual public report on counter-UAS posture, in the spirit of the Defence Ministry's public review.

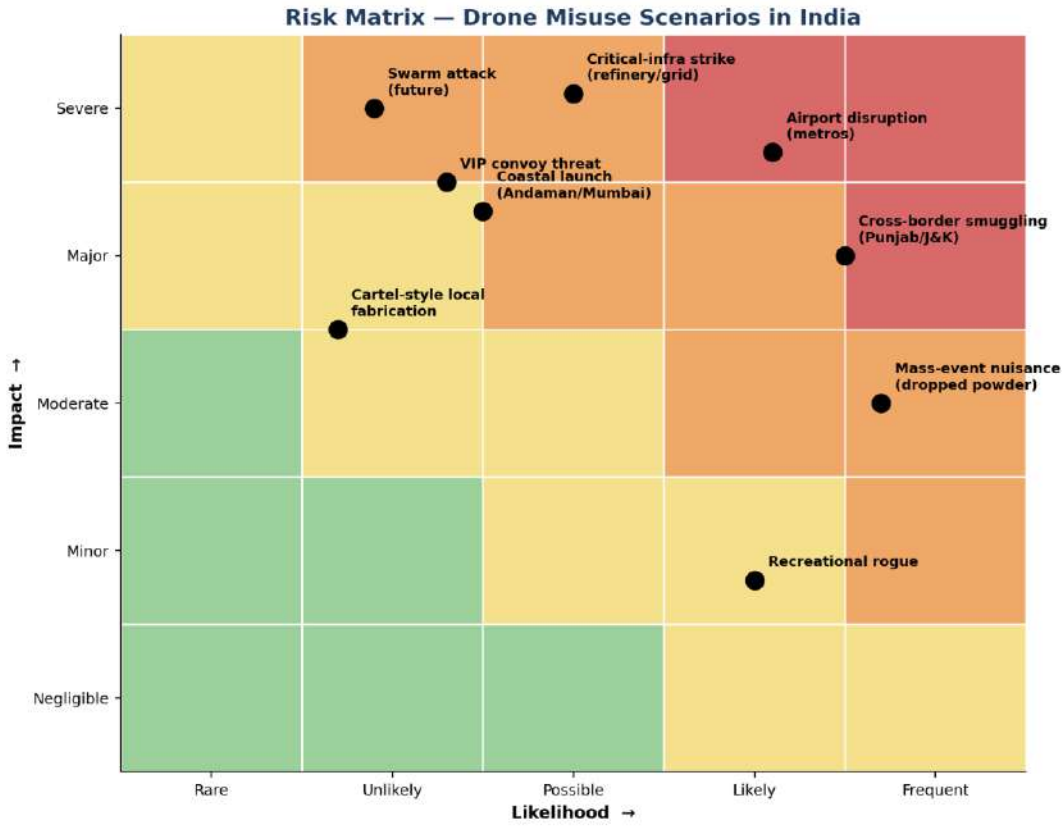


Figure 8. Risk matrix — drone misuse scenarios in India by likelihood and impact.

Source: Author's own compilation.

Action	Lead agency	Supporting agencies	Priority (1–3)	Indicative timeline
Stand up N-UTCC	MHA	MoD, DGCA, MEA, Intel, Coast Guard	1	2026–2027
DigitalSky 2.0 with TPM-bound IDs	DGCA	MeitY, BIS, industry	1	2027–2029
National Component Ledger	DGCA + MeitY	Customs, GST, industry	1	2027–2029
Two–3 Drone Forensic Labs	MHA / NFSU	DGCA, DRDO, academia	1	2026–2028
State UAS Cells (all states)	State Home Depts.	MHA, NFSU	1	2026–2028
Layered SkyShield type grid (urban)	MoD + State Police	Industry, infra owners	2	2026–2029
Western border sensor mesh	MHA (BSF) + IAF	DRDO, industry	1	2026–2030
Coastal C-UAS arc	Indian Navy + Coast Guard	MHA, port operators	2	2027–2031
AI fusion + dark-drone capability	DRDO + MoD	Academia, industry	2	2028–2031
HPM / DEW operational induction	MoD	DRDO, industry	3	2028–2032
BIS standards on UAS forensics	BIS	DGCA, NFSU	1	2026–2027

Action	Lead agency	Supporting agencies	Priority (1–3)	Indicative timeline
Mandatory cryptographic Remote-ID	DGCA	MeitY, industry	1	2027–2028

Table 3. Priority countermeasure roadmap for India — owners, timelines, dependencies.

Indigenous Capability Roadmap and Technology Readiness

India's industrial base is already strong in three of the four foundation areas: software, RF and AI. The gap, predictably, is in components — high-energy batteries, high-performance GNSS chips, and trusted-platform-module silicon at the price point a civil drone can carry. The roadmap below sequences indigenous capability against a realistic technology readiness baseline.

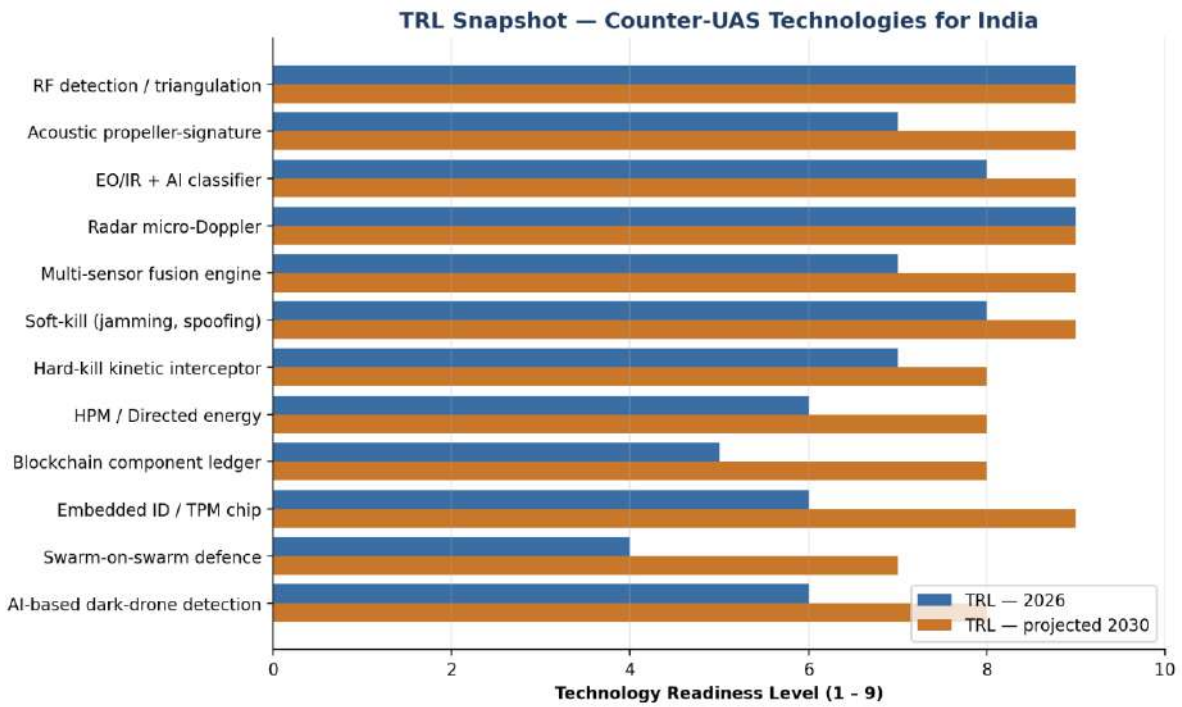


Figure 9. Technology Readiness Level (TRL) snapshot for counter-UAS technologies, current and projected to 2030. **Source:** Author's own compilation.

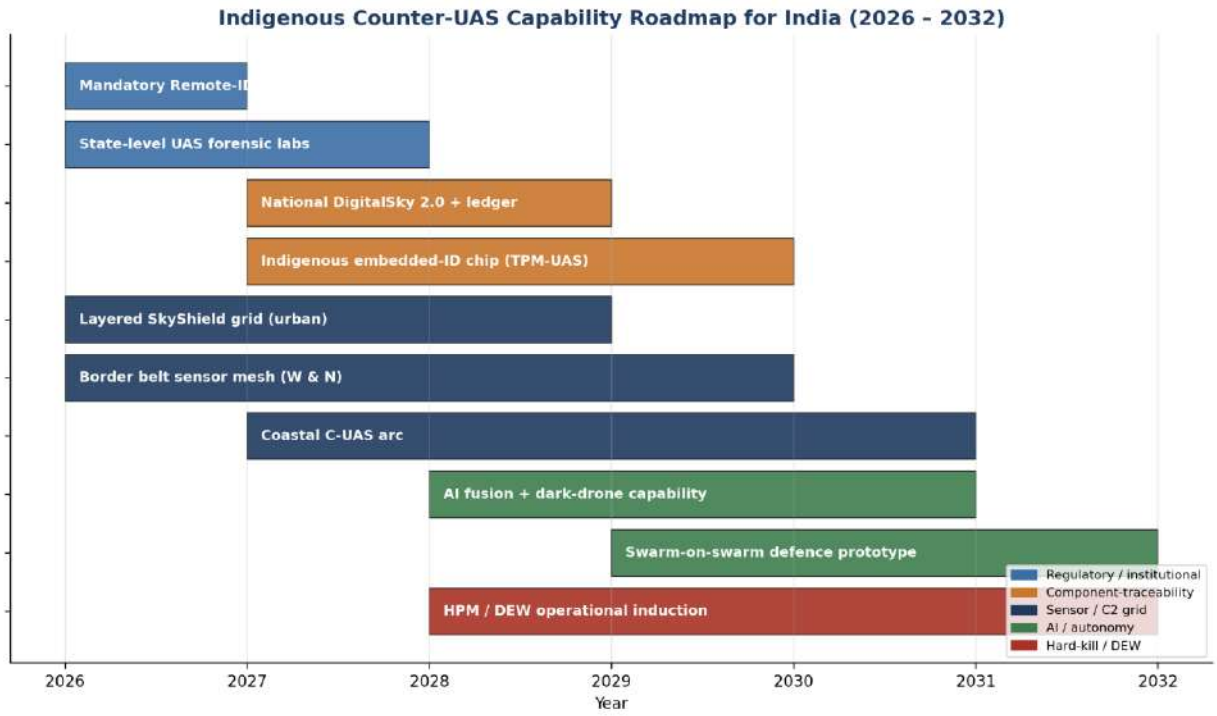


Figure 10. Indigenous counter-UAS capability roadmap for India, 2026–2032. **Source:** Author's own compilation.

Two judgements emerge from the roadmap. First, the regulatory and forensic stream (state UAS Cells, DigitalSky 2.0, National Component Ledger, indigenous TPM-UAS chip) must run ahead of the kinetic stream. The reason is honest: a hard-kill capability without an attribution capability deters nothing, because the deterrent effect rests on the certainty of being caught, not on the prospect of being shot down. Second, AI and fusion are the high-leverage investments — TRL is climbing, indigenous talent exists, and a national fusion engine is the single most consequential technology bet.

Future Threat Outlook (Three to Seven Years)

The threat surface in 2029–2033 will not be a linear extension of today's. Four trajectories deserve specific attention.

AI-Enabled Drones and Edge Autonomy

Drones with on-board recognition and decision-making — terminal homing on visual signatures, GPS-denied navigation by visual-inertial odometry, simple

swarming behaviours — are already at TRL 6 in open commerce. Within five years they will be commodity. The doctrinal implication is that RF-only counter-UAS, dominant today, becomes obsolete; the dark drone problem becomes the common case, not the exception.

Swarms

True swarming — coordinated multi-platform behaviour with shared perception — is harder than the demonstrations suggest, but disposable saturation attacks (a dozen cheap platforms with loosely synchronised launch) are well within reach of capable non-state groups. The defensive answer is twofold: high-rate-of-fire soft-kill across an arc (electronic warfare beating cost asymmetry) and swarm-on-swarm interception research that India should not outsource.

Counter-Countermeasures

Each defensive layer the state deploys will be probed. Frequency-hopping defeats narrow-band jammers; fibre-optic tethers defeat all jammers; spoofed Remote-ID defeats unauthenticated Remote-ID; AI-generated decoys defeat AI classifiers trained on yesterday's data. The honest response is treating counter-UAS as a continuous-investment problem, not a procurement event.

Grey-Zone Warfare Implications

Drones are the perfect grey-zone instrument: cheap, deniable, and scalable, which can be used below the threshold of conventional armed conflict. State actors will increasingly use proxies and improvised platforms to test red lines, harvest intelligence and impose cost without crossing the threshold of war. The Indian western frontier is already on this curve. Strategic doctrine must make explicit the threshold conditions for attribution, response and escalation control. Without that doctrine, the temptation will be to over-respond to a nuisance or to under-respond to a genuine probe.

> The doctrinal one-liner for the next decade is uncomfortable but useful: the cheap drone is not a tactical problem any longer; it is a strategic instrument used tactically.

Ethical, Privacy and Civil–Military Considerations

A capable counter-UAS architecture is, by construction, a surveillance architecture. Distributed RF sensors, EO/IR cameras, AI classifiers and a centralised common operational picture (COP) can be used for unethical surveillance. The Drone Rules 2021 acknowledge privacy briefly; however, further reforms are needed to ensure privacy.

- **Statutory oversight.** An independent oversight committee under Parliament, on the model of the Intelligence Services Commissioner regimes elsewhere, with scheduled reporting and powers of inquiry.
- **Data minimisation.** Sensor data must be retained only as long as operationally necessary, with automatic deletion timelines and purpose limitation.
- **Civil–military boundaries.** Military authorities must not, as a routine matter, hold raw civil-airspace sensor data. Federation, not centralisation, is again the design principle.
- **Recourse and redress.** A clear complaints mechanism for legitimately designated operators and judicial review of designation actions.

The European experience is instructive here as well: regimes that build privacy into the design from the outset enjoy more durable public consent and, therefore, more durable funding than regimes that bolt privacy on after the first scandal.

Limitations

This paper is built on open-source literature, publications, peer-reviewed research and official reports. The threat environment evolves rapidly; sensor capabilities and regulatory positions can change faster than a publication cycle. Three limitations should be borne in mind by the reader. First, the paper deliberately avoids tactical instruction; certain technical specifics that an adversary could operationalise are omitted, even where they are publicly known. Second, the indigenous capability roadmap is indicative; precise

timelines depend on industrial-policy and budgetary decisions. Third, the cost-effectiveness and TRL estimates are reasoned but not surveyed; they should be read as decision aids, not engineering specifications. Continuous monitoring, structured red-teaming and an annual review by the proposed N-UTCC would be the right correctives to all three. The framework should therefore be viewed as an adaptive model rather than a fixed blueprint.

Conclusion

The strategic problem this paper addresses are not unique to India, but the Indian instance is particularly demanding. A long contested western border, an active northern frontier, a porous northeast, an extended coastline, dense metropolitan airspace, a vibrant legitimate drone economy, and capable adversaries with cheap improvised platforms — these are not five problems; they are one problem expressed in five terrains.[54]

The framework proposed here is integrated by design. Tracing without detection is forensic archaeology; detection without tracing is data exhaust; without policy is a procurement exercise; policy without institutions is a press release. The four layers — technical tracing, layered detection, integrated system architecture, and policy-and-policing reform — succeed or fail together.

Three priorities deserve emphasis at the close. First, governance leads technology. The single highest-return investment is the National UAS Threat Coordination Centre and the legal instruments around it; without that spine, the most expensive radar is a curiosity. Second, tracing precedes interdiction. A country that can attribute will deter; a country that can only shoot down will be tested again. Third, the indigenous capability roadmap is a national industrial-policy choice as much as a security choice. The TPM-UAS chip, the AI fusion engine, and the cryptographic Remote-ID stack — these can be Indian, or they can be imported, but they will exist, and the cost of importing the foundation of one's sovereign airspace is paid in decades, not budgets.

The central argument of this paper is straightforward: the objective is not a drone-free sky but a transparent and accountable airspace in which drones can be identified, misuse can

be attributed and regulatory or legal action can be sustained. By strengthening visibility, attribution and accountability, India can reduce the likelihood of strategic surprise and manage the risks associated with the rapid proliferation of unmanned systems.

Declaration

I declare that this manuscript is being submitted exclusively to CENJOWS for publication consideration, is original, and has not been published or submitted elsewhere. I further certify that it contains no classified, restricted, or sensitive information and is based entirely on open-source material suitable for publication in the public domain.

ENDNOTES

[1] Directorate General of Civil Aviation, *The Drone Rules, 2021* (New Delhi: Ministry of Civil Aviation, Government of India, August 25, 2021).

[2] Bureau of Civil Aviation Security, *Counter-Rogue Drone Guidelines* (New Delhi: Ministry of Civil Aviation, Government of India, 2019).

[3] Ministry of Home Affairs, *"Counter-Drone Technology: SOPs for Security Forces"* (Office Memorandum No. VI-23014/209/IND/2018-VS, New Delhi: Government of India, May 10, 2019).

[4] James M. Rogers and Aaron P. Brantly, “Drone Warfare and the Challenge of Regulation,” *Defence Studies* 20, no. 3 (2020): 197–215.

[5] Paul Scharre, *Army of None: Autonomous Weapons and the Future of War* (New York: W.W. Norton & Company, 2018).

[6] Conflict Armament Research and United Nations Office of Counter-Terrorism, *Acquisition, Weaponization, and Deployment of Unmanned Aerial Systems by Non-State Armed Groups: Global Report* (New York: United Nations, 2024).

[7] United Nations Institute for Disarmament Research, *The Use of Uncrewed Aerial Systems by Non-State Armed Groups in Africa* (Geneva: UNIDIR, 2024).

[8] Andrea Calcara, R. David Edelman, and Ben Buchanan, “Drone Proliferation and International Security,” *International Studies Review* 25, no. 4 (2023).

[9] Maaike Verbruggen, "The Role of Civilian Innovation in the Military Drone Revolution," *Global Policy* 12, no. 1 (2021): 5–14.

[10] Akshat Upadhyay, “Countering Drone Threats: Policy and Technological Challenges for India,” *Journal of Defence Studies* 16, no. 4 (October–December 2022): 157–180.

[11] Department-Related Parliamentary Standing Committee on Home Affairs, *Report on Border Security Challenges and Drone Threat Management* (New Delhi: Rajya Sabha Secretariat, Government of India, 2024).

[12] Don Rassler and Yannick Veilleux-Lepage, "On the Horizon: The Ukraine War and the Evolving Threat of Drone Terrorism," *CTC Sentinel* 18, no. 3 (March 2025): 12–21.

[13] Jack Watling and Nick Reynolds, *Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine* (London: Royal United Services Institute, December 2022).

[14] Stacie L. Pettyjohn, "The Evolution of Drone Warfare and the Lessons of Ukraine," *Survival* 65, no. 3 (2023): 7–32.

[15] Ministry of Home Affairs, *Annual Report 2024–25* (New Delhi: Government of India, 2025).

[16] Andrea Coluccia et al., "Drone Detection and Discrimination Systems: Survey and Future Directions," *IEEE Access* 9 (2021): 103746–103770.

[17] Peter Molchanov et al., "Multi-Sensor System for Drone Detection and Tracking," in *Proceedings of the IEEE International Conference on Advanced Video and Signal-Based Surveillance* (Seoul: IEEE, 2014), 1–6.

[18] Vladimir C. Chen et al., "Micro-Doppler Effect in Radar: Phenomenon, Model, and Simulation Study," *IEEE Transactions on Aerospace and Electronic Systems* 42, no. 1 (2006): 2–21.

[19] u-blox AG, *u-blox GNSS Receiver Description Including Protocol Specification* (Thalwil, Switzerland: u-blox AG, latest edition), accessed June 14, 2026, https://www.u-blox.com.

[20] DJI Technology Co., Ltd., *DJI O3 Air Unit User Manual* (Shenzhen: DJI Technology Co., Ltd., latest edition), accessed June 14, 2026, https://www.dji.com/o3-air-unit/downloads.

[21] Emre Unlu et al., "Deep Learning-Based Strategies for the Detection and Tracking of Drones Using Several Cameras," *IPSJ Transactions on Computer Vision and Applications* 11, no. 7 (2019): 1–13.

[22] PX4 Development Team, *PX4 User Guide and Developer Documentation* (PX4 Autopilot Project), accessed June 14, 2026, https://docs.px4.io.

[23] ArduPilot Development Team, *ArduPilot Documentation* (Open Source Autopilot Project), accessed June 14, 2026, https://ardupilot.org

[24] Muhammad Ayub et al., "UAV Forensics: A Review of Forensic Procedures and Challenges," *Forensic Science International: Digital Investigation* 42 (2022): 301–315.

[25] Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, nos. 1–2 (2015): 4–37.

[26] Herbert Lin, "Attribution of Malicious Cyber Incidents: From Soup to Nuts," *Journal of International Affairs* 70, no. 1 (2016): 75–137.

[27] Matthias Strohmeier et al., "Security of ADS-B and Remote Identification Systems," *IEEE Communications Surveys & Tutorials* 17, no. 2 (2015): 1062–1087.

[28] Federal Aviation Administration, *Remote Identification of Unmanned Aircraft Final Rule* (Washington, DC: U.S. Department of Transportation, January 2021).

[29] ASTM International, *ASTM F3411-22a: Standard Specification for Remote ID and Tracking* (West Conshohocken, PA: ASTM International, 2022).

[30] National Institute of Standards and Technology, *Foundational Cybersecurity Activities for IoT Device Manufacturers* (Gaithersburg, MD: NIST, 2020).

[31] Trusted Computing Group, *Trusted Platform Module Library Specification, Family 2.0, Level 00, Revision 1.59* (Beaverton, OR: Trusted Computing Group, 2023).

[32] National Institute of Standards and Technology, *Zero Trust Architecture*, Special Publication 800-207 (Gaithersburg, MD: NIST, 2020).

[33] Jiyoung Seo et al., "Drone Detection and Identification Using Acoustic Signature Recognition," in *Proceedings of the IEEE International Symposium on Technologies for Homeland Security* (Woburn, MA: IEEE, 2018), 1–5.

[34] Muhammad Saqib et al., "UAV Detection in Complex Background Scenes Using Deep Learning," in *Proceedings of the International Conference on Digital Image Computing: Techniques and Applications* (Sydney: IEEE, 2017), 1–8.

[35]Gareth Horsman, "Unmanned Aerial Vehicles: A Preliminary Analysis of Forensic Challenges," *Digital Investigation* 16 (2016): 1–11.

[36] ExpressLRS Development Team, *ExpressLRS Documentation* (Open Source Long-Range Radio Control Project), accessed June 14, 2026, https://www.expresslrs.org.

[37] Team BlackSheep, *TBS Crossfire Documentation and Product Manuals* (Hong Kong: Team BlackSheep), accessed June 14, 2026, https://www.team-blacksheep.com.

[38] Defence Research and Development Organisation, *DRDO Anti-Drone Systems Capability Brief* (New Delhi: DRDO, 2023).

[39] National Aeronautics and Space Administration, *Unmanned Aircraft System Traffic Management Reference Architecture* (Washington, DC: NASA, 2022).

[40] European Union Aviation Safety Agency (EASA), *Drones and Counter-UAS in Civil Aviation: Regulatory and Security Considerations* (Cologne: EASA, 2022).

[41] Geneva Centre for Security Policy, *Building Resilience Against Terrorist Attacks Involving Unmanned Aerial Systems* (Geneva: GCSP, 2024).
[42] Geneva Centre for Security Policy, *Protecting Critical Infrastructure from Unmanned Aerial Threats: European Approaches and Lessons* (Geneva: GCSP, 2023).

[43] United Nations Institute for Disarmament Research, *Countering the Proliferation and Misuse of Commercial Drones: Emerging Responses in Europe* (Geneva: UNIDIR, 2023).

[44] United Nations Institute for Disarmament Research, *Increasing Transparency, Oversight and Accountability of Armed Unmanned Aerial Vehicles* (Geneva: UNIDIR, 2023).

[45] Government of India, *The Bharatiya Sakshya Adhiniyam, 2023* (Act No. 47 of 2023, New Delhi: Government of India, December 2023).

[46] National Institute of Standards and Technology, *Guide to Integrating Forensic Techniques into Incident Response, SP 800-86* (Gaithersburg, MD: NIST, 2006).

[47] European Union Agency for Law Enforcement Cooperation (Europol), *Facing Reality? Law Enforcement and the Challenge of Emerging Drone Technologies* (The Hague: Europol Innovation Lab, 2022).

[48] European Union Agency for Law Enforcement Cooperation (Europol), *The Unmanned Future(s): The Impact of Robotics and Unmanned Systems on Law Enforcement* (The Hague: Europol Innovation Lab, December 2025).

[49] International Institute for Strategic Studies, "Energy: Saudi Oil Under Attack—Analysis of the Abqaiq–Khurais Incidents," *Strategic Comments* 25, no. 8 (2019): iii–vi.

[50] Global Internet Forum to Counter Terrorism (GIFCT), *AI and Terrorism: Emerging Threats and Policy Considerations* (Washington, DC: GIFCT, 2025), accessed June 14, 2026.

[51] China Aerospace Studies Institute, *PLA Aerospace Power: A Primer on Trends in China's Military Air, Space, and Missile Forces*, 4th ed. (Maxwell Air Force Base, AL: Air University Press, July 2024).

[52] Michael C. Horowitz et al., "Strategic Competition in an Era of Artificial Intelligence," *Texas National Security Review* 1, no. 3 (2018): 19–44.

[53] Ulrike Franke and Georgia Hinds, “Cheap Drones, Costly Consequences: The Legal and Humanitarian Risks and Outcomes of Low-Tech Drone Warfare,” *The RUSI Journal* 170, no. 2 (2025): 24–39.

[54] R. Kweera, “Drones in Modern Warfare: Utilization in India-Pakistan Cross-Border Terrorism and Security Implications,” Strategic Analysis 47, no. 4 (2023): 376–388.https://doi.org/10.1080/09700161.2023.2288989