Volume 1 | Issue 2 | September 2025

CyberPeace

CYBER FORENSICS (4N6)

DRONE SECURITY

EYES IN THE SKY, CLUES ON THE GROUND

CYBER (4N6) FORENSICS

OUR SUPPORTERS

SHAH & ANCHOR

CyberPeace
CENTER OF EXCELLENCE

Army Institute of Technology, Pune
Onward to Glory

PARTNERS

Autobot Infosec

SysTools®
Simplifying Technology

Cyber 4N6 Consultants

OUR TEAM

OUR FOUNDERS

Maj. Vineet Kumar

Founder and Global President CyberPeace

OUR MENTORS

Shri SN Pradhan

IPS (Retd), Global CEO, CyberPeace
Former DG, Narcotics Control Bureau

Lt Gen (Dr.) Rajesh Pant (retd)

Global Advisor CyberPeace, PVSM, AVSM, VSM
Former National CyberSecurity Coordinator

TECHNICAL COMMITTEE

Mr. MAKP Singh,

former Ministry of Power, Govt. of India

Dr. Nilakshi Jain,

HoD, Shah &Anchor Kutchhi Engineering College, Mumbai

Suresh Behra,

Chief Technical & Training Officer CyberPeace

Col. Harkamal Sidhu,

Vice President, Autobot Infosec

EDITORS-IN-CHIEF

Lt. Col. (Dr.) Santosh Khadsare (Retd.)

Chief Business Officer- Cybersecurity, SysTools

Maj. Vineet Kumar

Founder and Global President CyberPeace

COPYEDITOR

Ms. Ayndri

Research Analyst, Policy & Advocacy, CyberPeace

DESIGN

Ms. Tannu Priya
Concept & Design

Associate- Media & Design, CyberPeace Foundation

HEAD OUTREACH

Lt Cdr Seema Gupta (Retd.)

Head, Outreach Program & Admin , CyberPeace

Editor's Note

Lt Col (Dr) Santosh Khadsare

GUEST EDITOR

The drone warfare witnessed during Operation Sindoor (India-Pak Conflict) in 2025 underscored a new reality: drones are now pivotal instruments of modern conflict, blending commercial innovation with strategic military application. With Pakistan deploying over 600 drones in coordinated swarm attacks, India's layered defense—combining indigenous missile systems, electronic warfare, and real-time command networks—successfully neutralized the threat, marking a benchmark for South Asian aerial security.

Globally, drone technology is transforming warfare and commerce at an unprecedented pace. According to recent analyses, over 2.5 million drones are forecasted to be produced in Ukraine alone in 2025, as AI-powered unmanned platforms redefine asymmetric conflict. The global drone market—valued at roughly $25 billion in 2024—is projected to surpass $40 billion by 2030, driven by advances in AI, 5G connectivity, and swarm autonomy. Countries like the U.S., China, and Turkey are deeply investing in drone R&D, with China dominating civilian drone manufacturing and the Asia-Pacific region emerging as the fastest growing market globally. This proliferation intensifies the challenge of drone misuse: states and non-state actors now have affordable, high-impact tools capable of precise strikes or covert operations. This has made drone forensics indispensable. India's investment in forensic capabilities — enables recovery of flight logs, RF signatures, and cloud data to attribute attacks and inform countermeasures. India's regulatory framework, shaped by the Drone Rules 2021 and facilitated via the Digital Sky platform, is evolving to enable safer skies without stifling innovation. Importantly, under Prime Minister Narendra Modi's Atmanirbhar Bharat vision, India is fostering a robust indigenous drone ecosystem—from manufacturing to counter-drone technologies—reducing dependency on foreign suppliers and enhancing strategic autonomy. Looking ahead, next-generation drones will be AI-enhanced, swarm-capable, and increasingly autonomous, demanding adaptive defense and forensic technologies. India's experience in Operation Sindoor illustrates how integrated sensor networks, layered defenses, and forensic precision can counter evolving aerial threats. In tandem with global trends towards automation, expanded Beyond Visual Line of Sight (BVLOS) operations, and regulatory harmonization, India is poised to lead not only in drone development but also in securing the digital airspace of the future. As drone technology reshapes global conflict and commerce, India's blend of innovation, regulation, and forensic readiness offers a compelling model—one that combines technological self-reliance with strategic foresight to secure the skies in this new digital age.

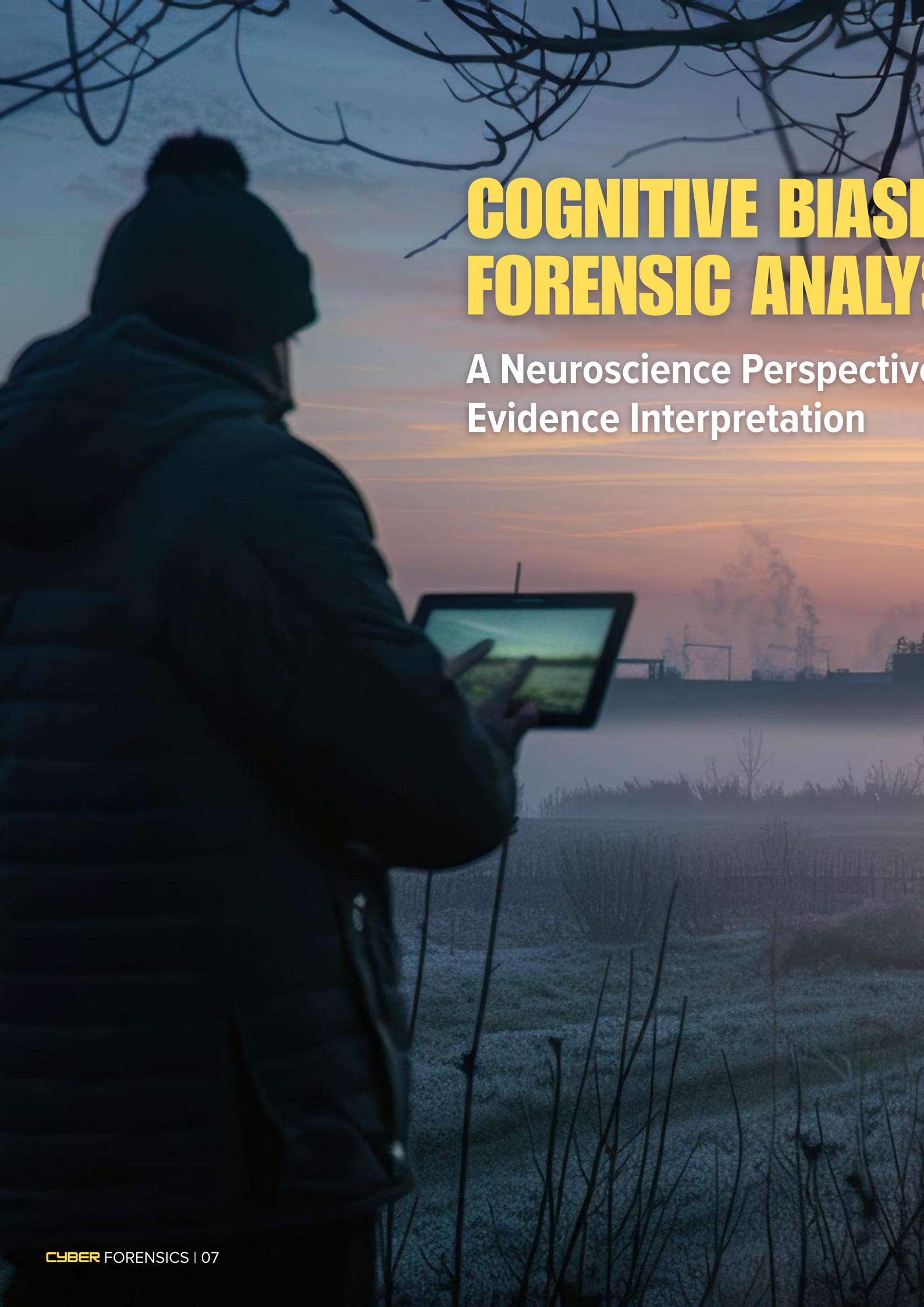
Lt Col (Dr) Santosh Khadsare

Founder & Editor-in-Chief

TABLE OF CONTENTS

TABLE OF CONTENTS

CYBER (4N6) FORENSICS



COGNITIVE BIAS
FORENSIC ANALY

A Neuroscience Perspectiv
Evidence Interpretation

ES IN DRONE SIS:

e on Digital

Unmanned aerial vehicles (UAVs) have radically changed the scenario of the ordinary business, as well as crime across the globe. Whether it is a complex surveillance operation or the cross-border smuggling operation, drones have become a much-diversified tool, which has posed unprecedented challenges to law enforcement and the national security agencies. Nevertheless, the technical nature of the drone-involved digital evidence has put tremendous mental dexterity requirements on forensic investigators, including flight logs, telemetry data, onboard status, and communications measures. In contrast to conventional digital forensics, the interpretation of the drone evidence can result in the practitioner having to reco -ncile multidimensional data streams under considerable time-constrained circumstances, especially when dealin -g with an active security threat or time-sensitive intelligence task. This mental load leaves fertile soil to systematic biases that can constitute the basic flaw of the investigation efficiency and court decisions.

Even in the face of increasing awareness about human issues in the cybersecurity field, the forensic community has not fully embraced the findings of the cognitive neuroscience field into the protocols followed in investigating drones. Cognitive psychology and neuroscience research has proved that predictable biases always dominate decision-making of the human mind especially in the situation when analysing complex, ambiguous, or high-stake information most drone forensic analysis situations involve.

This article focuses on the intersection of cognitive neuroscience and drone forensic analy -sis considering the most critical biases in the analysis of digital evidence and suggesting the methods of its minimization based on available evidence encountered by law enforcement agen -ts analyzing UAV-related crime based on the existing evidence of the application of neuroscie -nce principles to practical forensics.

Drone Forensics and Human Cognition

Advanced drone forensics covers advanced digi tal evidence, such as their GPS location and flig -ht outline, telemetry data that saves the elevator and heading changes, drone-ground communica tions, and multimedia that captures images and videos by embedded sensors. The extraction pr -ocedure is forensic which involves using propri -etary data dump tools-DJI Drones encrypt flight information in . DAT files that use specifically des -igned decryption algorithms whereas other man -ufacturers use entirely different protocols. Inves -tigators will need to relate different data stream -s to be able to build coherent stories of the drone activity and determine differences betwee -n the legitimate and suspicious flight patterns due to certain behavioural signs.

This is a process that needs professional judgment to detect anomalies and then combine technical evidence with the wider contexts of the investigations. The mental workload is especially high due to the necessity of the investigators to operate both quantitative (coordinates, timestamps, sensor data) and qualitative data(patterns of behaviour of flights and operations of context). The study of cognitive neuroscience has determined that such dual processing demands deploy multiple neural networks in parallel, further adding to the chances of cognitive overload, which leads to the use of mental shortcuts that result in the formation of systematic biases. The executive functions and working memory are processed by the prefrontal cortex, which when faced with loads of complex information becomes highly unreliable - a scenario often common in the investigation of drones that involves a large number of multiple flight sessions or an organized network.

Key Cognitive Biases in Drone Forensic Analysis

Confirmation Bias- Confirmation bias is the most common risk in objective drone forensics and describes itself through the inclination of examiners to pursue facts maintaining the preset conceptions besides escaping opposing facts.Using neuroimaging, it has been found that confirmation bias involves reward impulses being triggered by the brain sequenti ally traversing the ventral striatum when people see information that confirms their beliefs, and this causes a neurochemical feedback loop that creates an experience of reinforcement occurring and thus makes objectivity more challenging. When indications of smuggling appear on preliminary analysis, the flight patterns may be unconsciously determined to be evasive by the investigators without considering other possibilities like weather patterns or failures of equipment.

Availability Heuristic

Pattern recognition errors and Anchoring Bias

Anchoring bias can be defined as overreliance of investigators on initial information they come across in the course of analysis, this is used as a cognitive anchor and it disproportionally affects future interpretations. This is typical in a drone forensic scenario where investigators need to reconstruct the timeline and become tied to the first timestamp found and then interpret all further logged data with respect to an initial origin, causing unintended errors when determining an operational sequence. Pattern recognition bias or apophenia is the biased way of finding patterns in random or ambiguous data, where no apparent pattern is present. The specified phenomenon is also highly applicable in the context of the multidimensional character of the UAV operational data. Researchers can detect synchronized operations among separate drone services or they can detect stalking across regular flying habits. Due to the three dimensions of the flight paths of drones, the recognition of a pattern forms especially intricate problems, where investigators might see a meaningful geometrical relation, which in reality is a response in the environment or some sort of restriction.

The availability heuristic explains the subjective per -ception that bases the probability of achievement of an event on the degree to which associated eve -nts can be recalled associated events. Such bias is undesirable in that up-to-date case-based experien -ces of investigators can adversely affect the current evidence analysis. The practical implication -s of it are having the predisposition to overestimat -e some of the patterns of threats on the basis of freshly observed instances, thus failing to recogniz -e the right of the drone activities themselves.

Neurological Factors Affecting Decision-Making Cognitive Load and Stress Response

The working memory mechanism of the human bra -in possesses intrinsic capacity constraints that pro -ve to be a serious bottleneck under more intricate scenarios that require conducting drone forensics. Working memory is able to process, successfully th -ough, only about seven discrete pieces of informa -tion at once, although drone investigations regular -ly involve managing tens of information streams. The drone investigations conducted in high-stakes scenarios impose great time pressure usually precipitating stress reaction that releases cortisol

and other hormones that completely alter cognitive functioning. Acute stress also provides a short-term increase in attention and negatively affects the executive functions of the prefrontal cortex, such as working memory, mental mobility, and the ability to recognize bias. Forensic research studies indicate that higher levels of cortisol actually damage the capacity of the investigator to regard alternative hypotheses and combine contradictory facts, which among cogniti - on skills is the most important in accurate drone forensics analysis.

Fatigue and Circadian Effects

Long surveillance activities of drones sometimes subjects the investigators to work off normal circadian rhythms, further exposing neurobiological weakness. The prefrontal cortex, which carries out the executive control process explaining why sleep deprivation and circadian disruption happen, and the hippocampus, which is important in memory consolidation, also become impacted.

Future Directions and Policy Implications

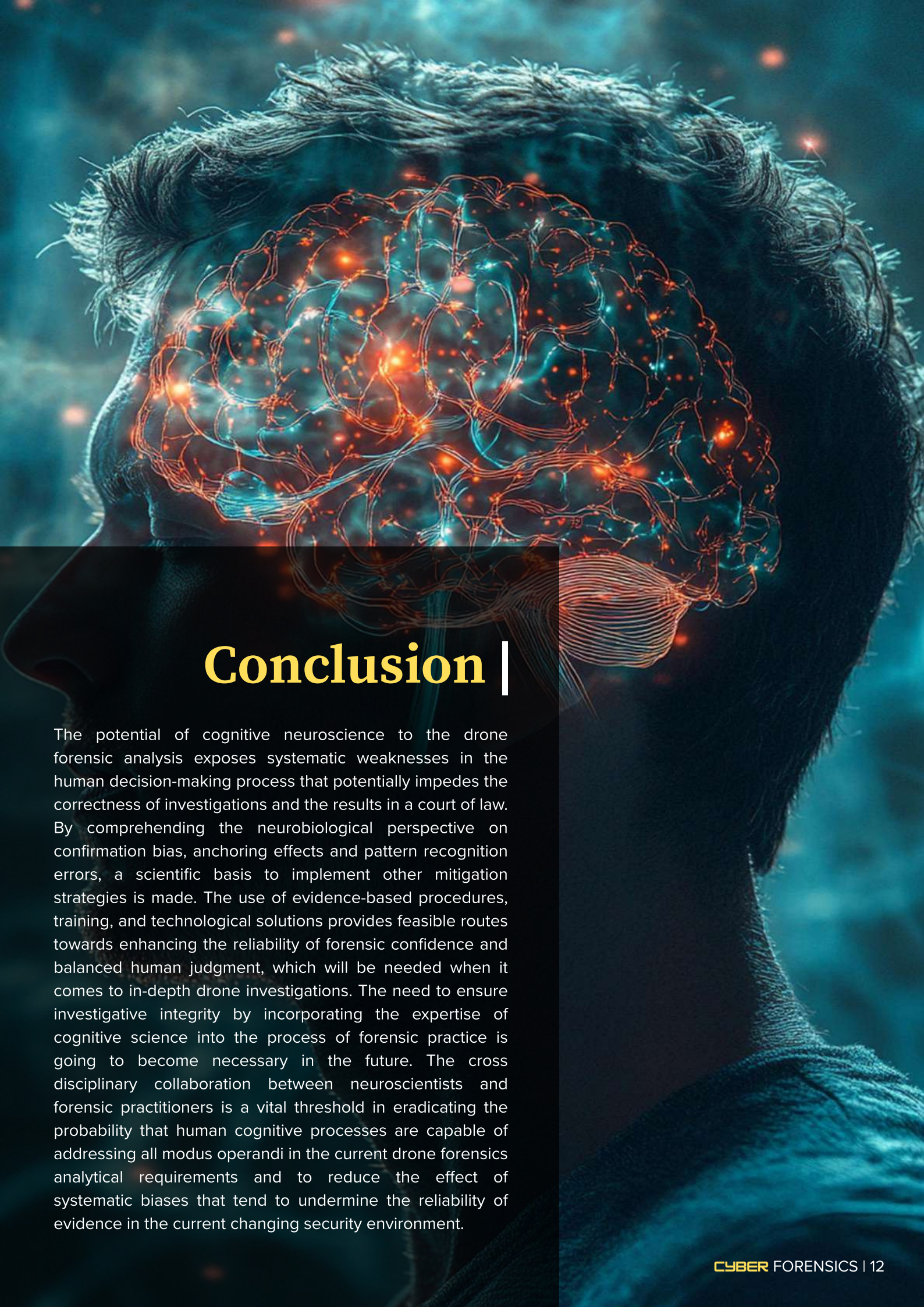
The application of knowledge based on neuroscience in the field of drone forensics is an emerging discipline that has vast research and practical implications. Additional work should be done on the creation of real-time monitoring systems of the cognitive state that would notify investigators when in a state that has been linked to having higher chances of being biased. Studies must consider the strategy of adaptive analysis interface in which it changes and adapts the information presentation on the basis of the cognitive status of investigators and the vulnerability of bias in them. The policy merits of these findings imply that it may be necessary to have uniformity in bias mitigation procedures in law enforcement agencies that engage in investigating drones. Cognitive science should be applied in training standards and systematic auditing of bias should be included in the quality assurance procedure. However, the establishment of a forensic reliability of these standards based on international cooperation could facilitate reliable forensic reliability consistency between jurisdictions irrespective of the cross-border aspect of most security threats involving drones.

Kritika,

B. Tech student (Artificial Intelligence and Machine Learning) at Netaji Subhash Engineering College, Kolkata.

About the Author:

Kritika is an award-winning cybersecurity researcher exploring the human side of digital risk through the emerging field of neuro-cybersecurity—where brain science meets digital security. With 30+ publications and features in platforms like ISACA, CXO DigitalPulse, and IGI Global, she has also delivered 10+ keynote sessions worldwide. Her work focuses on how cognitive vulnerabilities shape cyber behaviour and on designing human-centered, ethical solutions for future threats. Her contributions have earned her global recognition, including the Young Engineer Award and Young Researcher Award. Connect with her on Linked.



Conclusion |

The potential of cognitive neuroscience to the drone forensic analysis exposes systematic weaknesses in the human decision-making process that potentially impedes the correctness of investigations and the results in a court of law. By comprehending the neurobiological perspective on confirmation bias, anchoring effects and pattern recognition errors, a scientific basis to implement other mitigation strategies is made. The use of evidence-based procedures, training, and technological solutions provides feasible routes towards enhancing the reliability of forensic confidence and balanced human judgment, which will be needed when it comes to in-depth drone investigations. The need to ensure investigative integrity by incorporating the expertise of cognitive science into the process of forensic practice is going to become necessary in the future. The cross disciplinary collaboration between neuroscientists and forensic practitioners is a vital threshold in eradicating the probability that human cognitive processes are capable of addressing all modus operandi in the current drone forensics analytical requirements and to reduce the effect of systematic biases that tend to undermine the reliability of evidence in the current changing security environment.

UNVEILING DIGITAL TRAILS:

A Student's Reflections on Drone Forensics in the Era of Autonomous Systems

Nabil Ahmed,

Department of Artificial Intelligence and Machine Learning, Netaji Subhash Engineering College, Kolkata

Executive Summary- Derived from experience working on autonomous flood-rescue drone as part of the National Innovation Challenge for Dr -one Application & Research (NIDAR) disastermanage ment challenge, this paper explores the complex inter -play between advanced drone functionalities and the digital evidence they produce. This is an emerging are -a that digital forensic investigators must increasingly understand and manage. This paper assesses critical data sources, the forensic challenges posed by AI integration and multi-agent missions, real-world misus -e cases, and the evolving legal frameworks in India. It further advocates design principles that embed forens -ic accountability and privacy protections to ensure reliable, admissible evidence while advancing autonomous drone capabilities.

Data Sources and Extraction Methods

Modern Unmanned Aerial Vehicles (UAVs) deployed for disaster management function much like compact data centers in the sky. Our NIDAR platform integrates multiple complex data streams:

- **Flight Controller Logs:** Proprietary files (.DAT, .TXT) stored on onboard SD cards that record every control input, sensor reading, and GPS coordinate.
- **Edge-Processed Video:** High-resolution camera feeds are analyzed in real time by onboard AI systems, which generate temporary caches and inference logs that capture detected objects, rescue-priority scores, and decision thresholds.
- **Telemetry Streams:** Continuous uplink/downlink channels transmit control signals and metadata, including battery health and mission flags, that must be captured quickly before being overwritten.

Extracting this data requires a blend of traditional forensic tools like Autopsy and FTK Imager, alongside custom scripts to parse AI-layer caches and query live telemetry streams before data rotation occurs. I utilize Python utilities to decode binary logs into human-readable JSON and correlate those records with flight paths to reconstruct autonomous decision sequences.

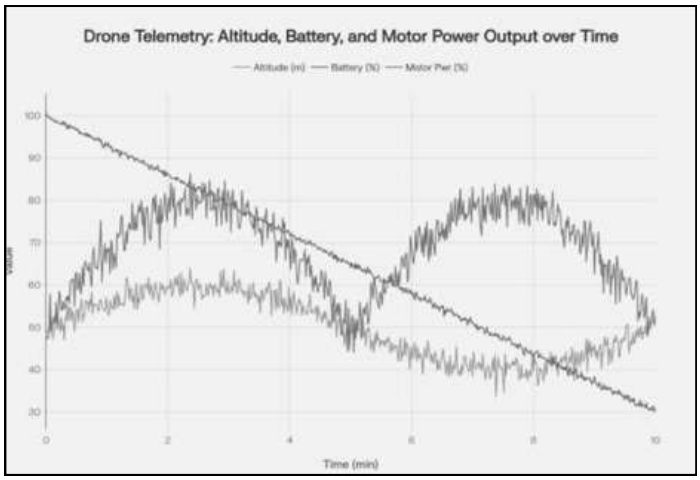


Fig 1.1: Drone telemetry showing altitude, battery percentage, and motor power output over a 10-minute flight period with mission phase markers

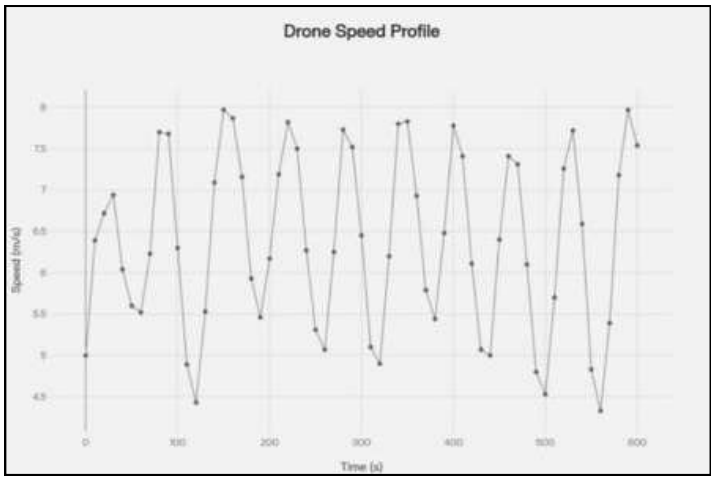


Fig 1.2: Drone speed/velocity profile over a 10- minute mission sampled every 10 seconds

AI-Driven Artifacts and Collaborative Missions

Integrating machine learning models adds a new layer of forensic complexity. Each model, whether a victim-de -tection convolutional neural network or a path-planning recurrent network, leaves a distinct digital signature:

- **Checksum Records:** Cryptographic hashes of traini -ng datasets and model weights, stored on the controller to verify integrity during runtime.
- **Inference Confidence Logs:** Time-stamped entries documenting specific detections and the correspon -ding commands, such as “human at 12 o’clock, confidence: 0.87,” followed by “hover, drop life vest.”

- **Inter-Drone Communication Logs:** In multi-agent missions, drones share map overlays and survivor location vectors; these files must be reconciled to fully reconstruct coordinated operations.

In a recent pilot run, a drone swarm divided work across mapping floodplains, relaying survivor locations , and delivering supplies. Each drone's local cache con tained only a fragment of the overall mission. Piecing together the full narrative requires synchronizing times tamps and merging logs from all devices.

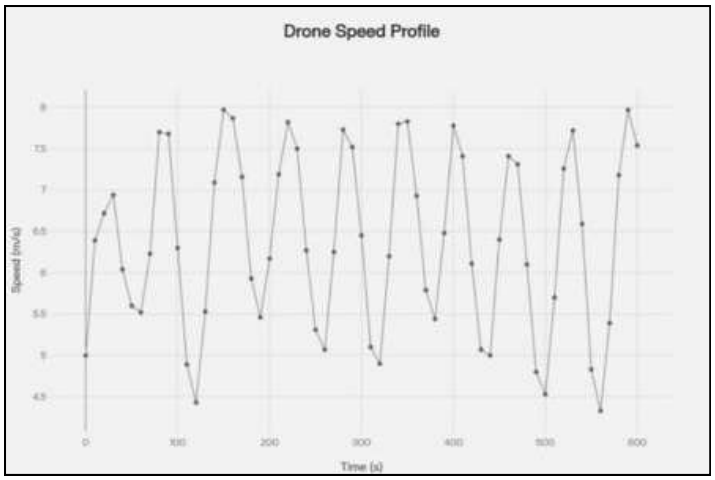


Fig 2.1: Drone's Flight Path showing GPS coordinate connected points representing a drone's trajectory during a test flight

Fig 2.2: Annotated confidence scores of humans as conducted during a test flight by our team

Real-World Crime Cases Highlighting Forensic Challenges

Despite their life-saving purposes, these capabilities can be exploited maliciously. Some notable real-life inci -dents include:

- **Cross-Border Smuggling (Punjab):** Investigation of contraband-carrying drones revealed firmware patc -hes correlating anomalous GPS jumps to specific operators.
- **Telemetry-Based Data Exfiltration (Karnataka):** Indus -trial espionage efforts used drones with covert com -munication channels; forensic teams intercepted live data mid-mission, then analyzed discrete firm ware logs for protocol alterations.

- **Prison-Smuggling Networks (West Midlands):** Motor-control log -s timestamped drop actions to the millisecond, linking operation -s through consistent build configurations.
- **Unauthorized Surveillance:** Consumer drones with facial recogni -tion left hidden caches of images and confidence scores, constit -uting unlawful databases. These cases emphasize the importanc -e of designing forensic readiness into drone systems through sta -ndardized, well-documented, and digitally signed Logs to enable reliable evidence authentication.

Forensic Challenges of DIY Drone Architectures

Beyond commercial platforms, DIY drones introduce additional compl -exities. UAVs can now swap sensors, cameras, and communication modules, ideal for flexible disaster response but challenging for forensic analysis:

- **Hardware Diversity:** Custom builds feature varied storage interfa -ces like micro-SD slots, hidden USB ports, networked partitions, necessitating thorough physical examination before data imaging.
- **Firmware Fragmentation:** Open-source controllers like ArduPilot allow personalized log formats, requiring forensic analysts to reverse-engineer parsers on a case-by-case basis.
- **Distributed Evidence Chains:** Collaborative multi-drone missions scatter data across multiple devices, demanding careful correlation of communication logs and shared map data.

Furthermore, offline-trained machine-learning models introduce “artifacts about artifacts”, i.e., version identifiers, dataset hashes, and inference thresholds that aid authenticity verification if properly captured and timestamped.

Evolving Legal and Regulatory Landscape in India

India is taking steps to address emerging challenges in drone forensics:

- Bharatiya Sakshya Adhiniyam (2023) mandates integrity and authenticity of digital records; for AI-equipped drones, this involves digitally signing logs at creation and maintaining tamper-evident records.
- The Puttaswamy Judgment (2017) enshrines privacy as a fundamental right, requiring investigators to balance evidence needs with robust protections against unnecessary data collection during rescue missions.

References:

Centre for Internet and Society. (2021). Drone Rules, 2021. Ministry of Civil Aviation, Government of India.

Government of India. (1872). Indian Evidence Act. Ministry of Law and Justice. Justice K. S. Puttaswamy (Retd.) vs Union of India (2017). Supreme Court of India, WP (Civil) No. 494 of 2012.

Kumar, S., & Singh, H. (2020). Digital forensic challenges in UAVs with AI integration. International Journal of Cyber Forensics, 15(3), 45-62.

Mishra, R., & Das, P. (2022). Telemetry-based data exfiltration techniques in unmanned aerial vehicles. Journal of Information Security and Applications, 58, 102822.

Raj, A., & Patel, V. (2019). Forensic analysis of drone-based prison contraband delivery system. Law Enforcement Technology, 46(4), 28-35.

Singh, T., & Khanna, R. (2021). Privacy concerns and legal challenges in drone surveillance technology in India. Journal of Privacy and Security Studies, 9(2), 113-130.

Nabil Ahmed,

Department of Artificial Intelligence and Machine Learning, Netaji Subhash Engineering College, Kolkata

About the Author:

As a fourth-year B.Tech student specializing in Artificial Intelligence and Machine Learning at Netaji Subhash Engineering College, Nabil is currently engaged in developing an autonomous flood-rescue drone as part of the National Innovation Challenge for Drone Application & Research (NIDAR) disaster-management challenge. Passionate about machine learning, he has completed several projects in the field. Nabil seeks to share his growing understanding and inspire others by making complex topics approachable for fellow learners and the broader tech community. He can be found on LinkedIn

At present, enforcing agencies face skill gaps in handling AI-integrated forensic processes, highlighting the need for interdisciplinary training programs that blend engineering and digital-forensics expertise.

Toward Forensic-Aware Autonomous Systems

From my ongoing work with NIDAR, my team has identified key principles for embedding forensic accountability early in the design lifecycle:

- Use standardized, human-readable log formats (e.g., JSON with defined schemas) covering flight paths, sensor data, and AI inferences.
- Apply cryptographic digital signatures to logs at the point of creation to ensure tamper detection.
- Implement GPS-synchronized secure clocks across all devices to maintain consistent, trustworthy timestamps. Incorporating these design elements will reduce investigative overhead and strengthen the evidentiary value of drone data in real-world legal contexts.

Conclusion

Being a part of the NIDAR autonomous flood-rescue drone project continues to deepen my understanding of the detailed digital footprints such systems leave behind. These drones don't just save lives—they generate rich data trails that, when misused, can expose illicit activities or privacy violations. As future engineers, our responsibility goes beyond building capable systems. We must anticipate the forensic demands of these autonomous agents and embed transparency, security, and legal compliance into their very architecture. Only through this integrated approach can we ensure drones serve humanity safely, ethically, and with full accountability.

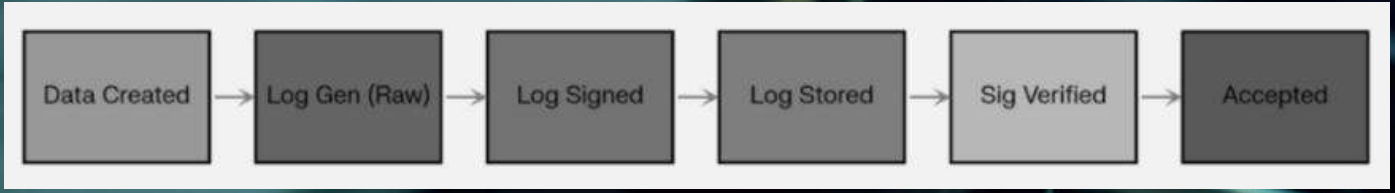


Fig 3.1: Flowchart illustrating the digital signature process for drone forensic logs, from data creation to verification during forensic investigation

Introduction - Drones are being used more and more in both civilian and security settings. They help industries like logistics, agriculture, media, and public safety, but they also make it easier for criminals to carry out smuggling and spying operations. Incidents near US airports and along India's borders show that people are using them more and more. Captured drones have useful digital evidence (logs, telemetry, communications), but it's hard to extract it because of encryption and proprietary systems. Drones are now key tools for organised crime and state actors; conventional forensic methods are insufficient, requiring skills in AI, RF analysis, cryptography, and embedded systems. This report looks at how drones are currently used in forensic investigations, the types of evidence they collect, the methods they use to extract evidence, relevant cases from 2023 to 2025, India's response, and suggests a more advanced forensic framework for dealing with global problems.

UAV Evidence Anatomy

Drone forensics is the in-depth study of evidence from the drone itself, its ground control station, and relevant cloud services to figure out what the drone was doing.

2.1 Flight Log Analysis

Drone flight controller logs are very important for investigations because they give detailed mission data. But the way logs are formatted, how easy they are to get to, and how they are encrypted are very different between commercial and open-source systems. This affects the forensic workflow. Finding out what kind of flight controller and log you have is very important because it determines what tools and skills you need. DJI drones are hard to decrypt, and DIY drones with ArduPilot need to parse a lot of open-format data. To do this, forensic labs need different sets of skills and tools.

TRACING DRONES:

Modern Forensics for Airspace Security

Darshil Raval

Security Researcher from Gujarat, India

2.1.1 DJI LOGS-

DJI uses two main flight log types:

TXT files from companion apps (DJI GO, DJI Fly, DJI Pilot), saved on the mobile device/controller; these summarize flight data.

More detailed .DAT files stored on drone's internal memory or microSD card.

TXT file structure:

100-byte header, telemetry records, details area.

Uses little-endian format for multi-byte numbers.

Recent log versions:

Add payload scrambling (XOR obfuscation).

From version 13, core records use AES encryption; decryption needs a keychain from DJI servers via their API.

Getting the required apiKey for AES decryption:

Needs developer registration with DJI.

Not fast or easy for many law enforcement agencies.

Common tools:

PhantomHelp Log Viewer and Airdata decrypt/parse .TXT logs.

DatCon and dji-log-parser (Python) for .DAT logs—if API keys are available.

As of mid-October 2024:

DJI has stopped syncing flight logs to US servers for its apps.

Local acquisition from devices becomes even more crucial.

2.1.2 OPEN-SOURCE LOGS

Unlike DJI, open-source drones (ArduPilot/Pixhawk, PX4) log flight data in open formats. Ground Control Stations save MAVLink telemetry logs (.tlog), while onboard systems record high-frequency sensor data in DataFlash logs (.bin for ArduPilot, .ulg for PX4). Mission Planner or MAVProxy view ArduPilot logs; logs.px4.io or PlotJuggler view PX4 logs. ArduPilot log settings are customizable via parameters like LOG_BACKEND_TYPE. Programmatic analysis is possible with tools such as MATLAB's ardupilotreader.

Table 1: Detailed Comparison of UAV Log File Formats

DJI VS. ARDUPILOT/ PX4 FEATURE COMPARISON

	DJI Logs	ArduPilot/PX4 Logs
Storage Location	.TXT/.DAT files	.tlog/.bin files
Data Format	Proprietary binary structure	.tlog: MAVLink, .bin: Raw binary
Encryption/Obfuscation	Payload scrambling, AES encryption	None
Key Data Fields	GPS, IMU, battery, gimbal, controller	GPS, IMU, ATT, NTUN, CURR, CAM
Logging Frequency	.TXT: ~10 Hz, .DAT: >50 Hz	.bin: High frequency
Common Analysis Tools	PhantomHelp, DatCon, DroneXtract, dji-log-parser	Mission Planner, QGroundControl, MAVProxy, ardupilotreader
Forensic Challenges	Decrypting, parsing proprietary formats	Managing data volumes, correlating messages

3. Advanced Data Extraction

When drones are forensically inaccessible via software , investigators must use advanced hardware extraction . This is a response to manufacturers' proprietary interf -aces and encryption, offering a "last resort" for compl ete memory data recovery.

3.1 Physical Memory Acquisition

Physical acquisition makes an exact copy of a storage device, getting back files, fragments, and data from unallocated space that have been allocated and deleted. For drones, this means being able to get to the internal eMMC flash memory chip directly.

Table 2: Physical Acquisition Techniques - JTAG, ISP, and Chip-Off

DRONE FORENSICS TECHNIQUES COMPARISON

Characteristic	JTAG	ISP	Chip-Off
Description	Connects to Test Access Ports.	Connects to eMMC memory chip pins.	Desolders memory chip for external reading.
Destructive?	No	No	Yes
Required Skills/Tools	Intermediate soldering, JTAG box, TAP knowledge.	Advanced soldering/probing, eMMC pinouts, ISP adapter.	Expert soldering, rework station, chip reader.
Pros	Non-destructive, bypasses USB, full image.	Non-destructive, direct access, works on devices.	Guaranteed image, bypasses security, works damaged.
Cons	TAPs disabled/hard, requires supported processor.	Requires small points, risk of shorting.	High risk of destroying chip, expensive.
Drone Applicability	High	High	High

3.2 RF Signal Analysis

Radio frequency analysis, or SIGINT, extracts drone evidenc -e remotely by capturing and decoding communication sign als with specialized equipment.

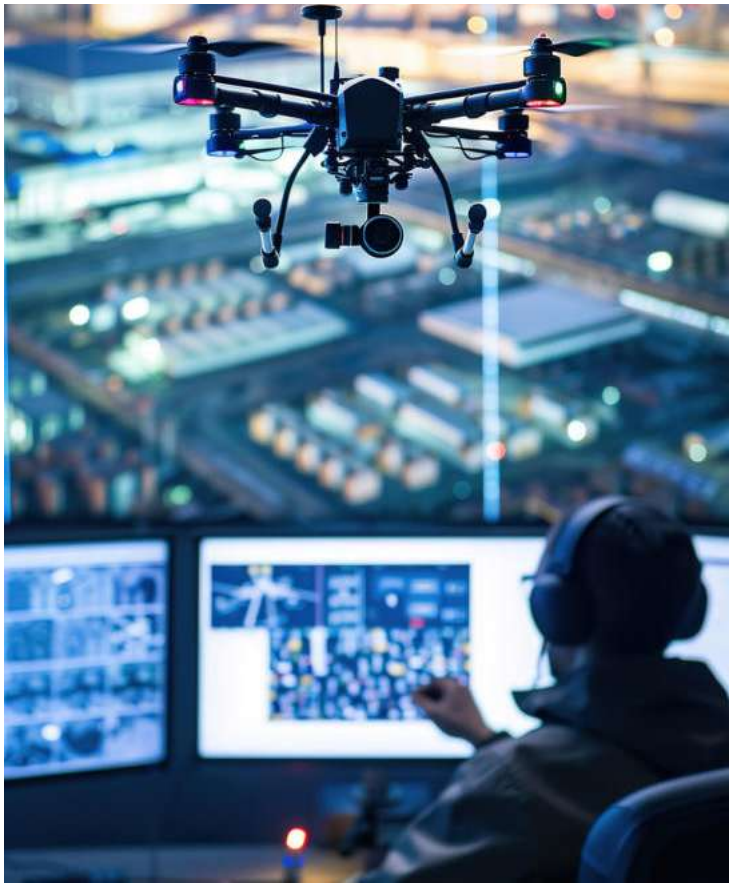
3.2.1 SDR Capture

Software-Defined Radio (SDR) is important for RF forensics because it lets investigators capture and analyse raw drone signals on bands like 2.4 GHz and 5.8 GHz using devices like HackRF One or USRP B210. GNU Radio and SDR++ are examples of tools that can help you see, identify, and maybe even decode these signals. This makes it possible to do detailed signal analysis and gather intelligence in real time.

Table 3: Analysis of DJI OcuSync & DroneID Protocol Characteristics

OCUSYNC AND DRONEID COMPARISON

	OcuSync	DroneID
Purpose	Robust control/video transmission	Regulatory compliance
Frequency Bands	2.4/5.8 GHz, dual-band	2.4/5.8 GHz, predefined
Modulation	OFDM	OFDM with QPSK
Hopping Mechanism	DFS/FHSS	Hops after emissions
Encryption	Yes, robust	No, cleartext
Key Data Transmitted	Encrypted control/video	Location and serial number
Forensic Exploitability	Very difficult	High



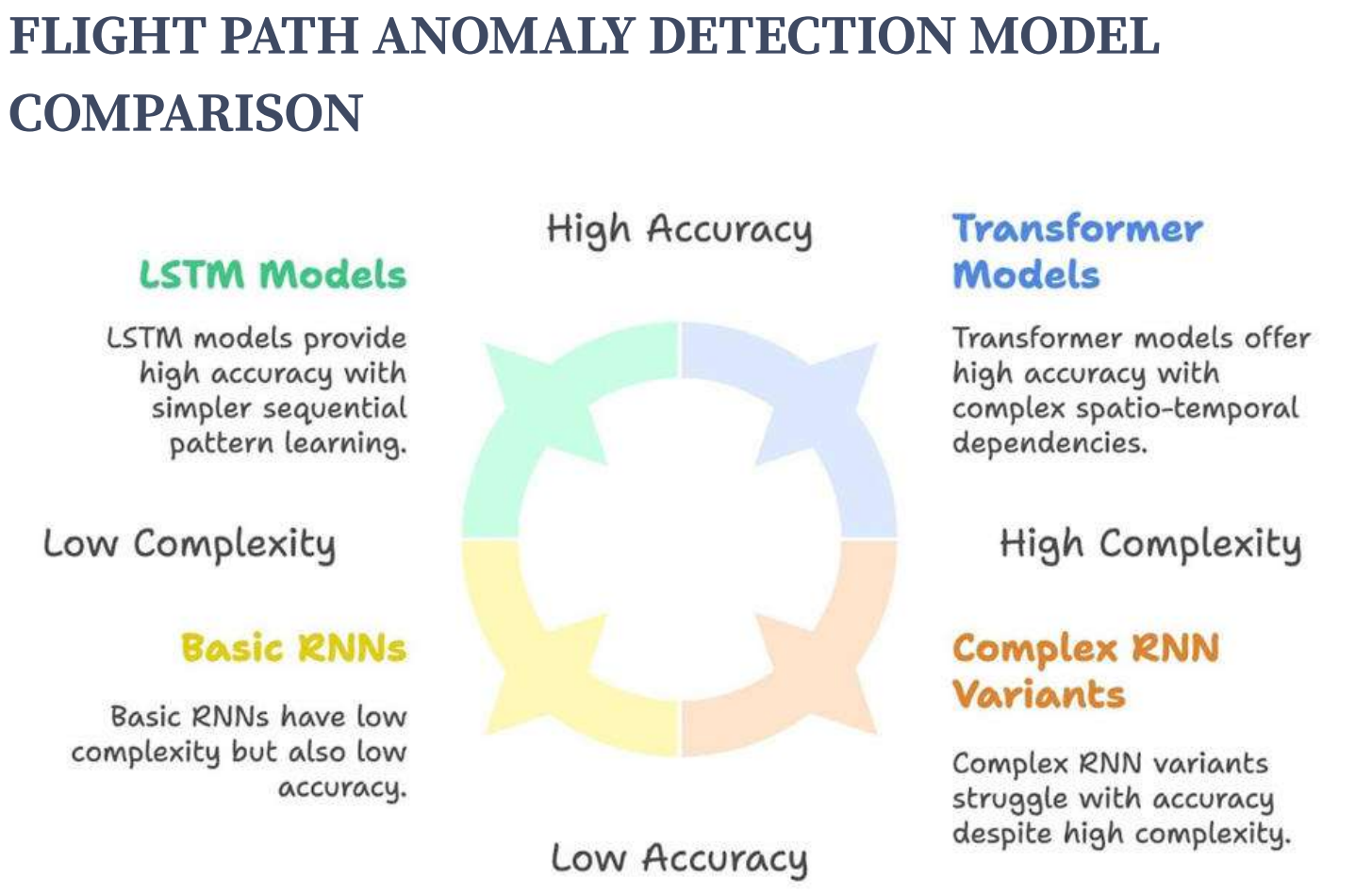
3.2.2 DJI Protocols

SDR can easily pick up the unencrypted DJI DroneID broadcast, which gives investigators access to important flight information like location, altitude, speed, and serial number without breaking OcuSync's AES-encrypted link. DroneID uses OFDM, hops between frequencies, and sends out packets with OFDM symbols and Zadoff-Chu sequences for sync for about 600 milliseconds per channel. Open-source MATLAB or Python tools can be used for forensic analysis to extract and decode this data. This gives forensic investigators a great chance to do their work, even when the main control link is still safe.

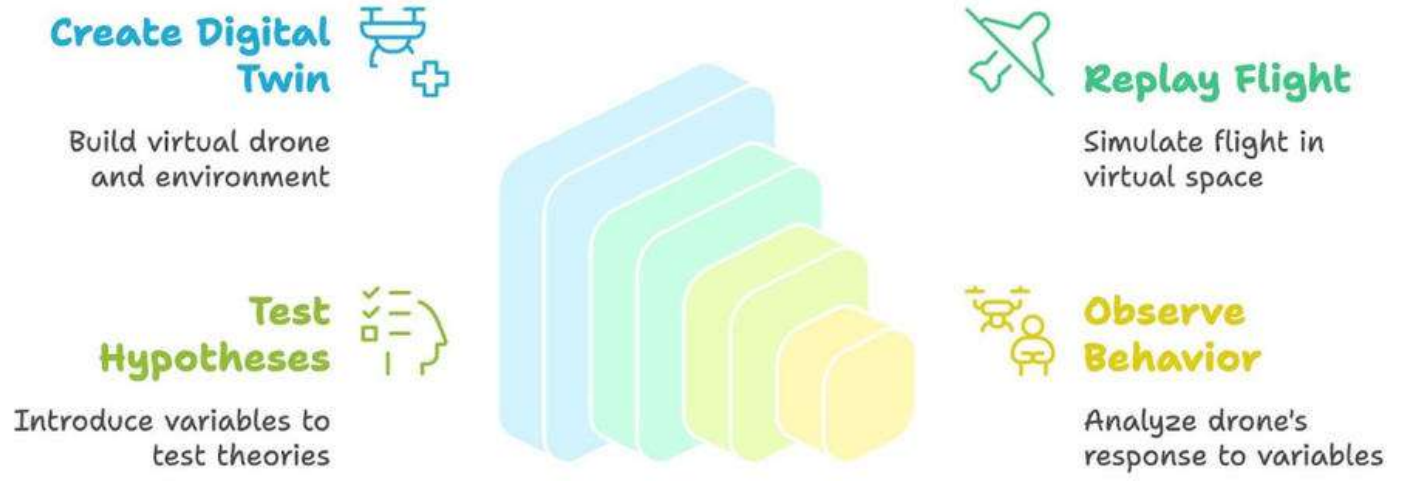
3.3 AI/ML Analysis

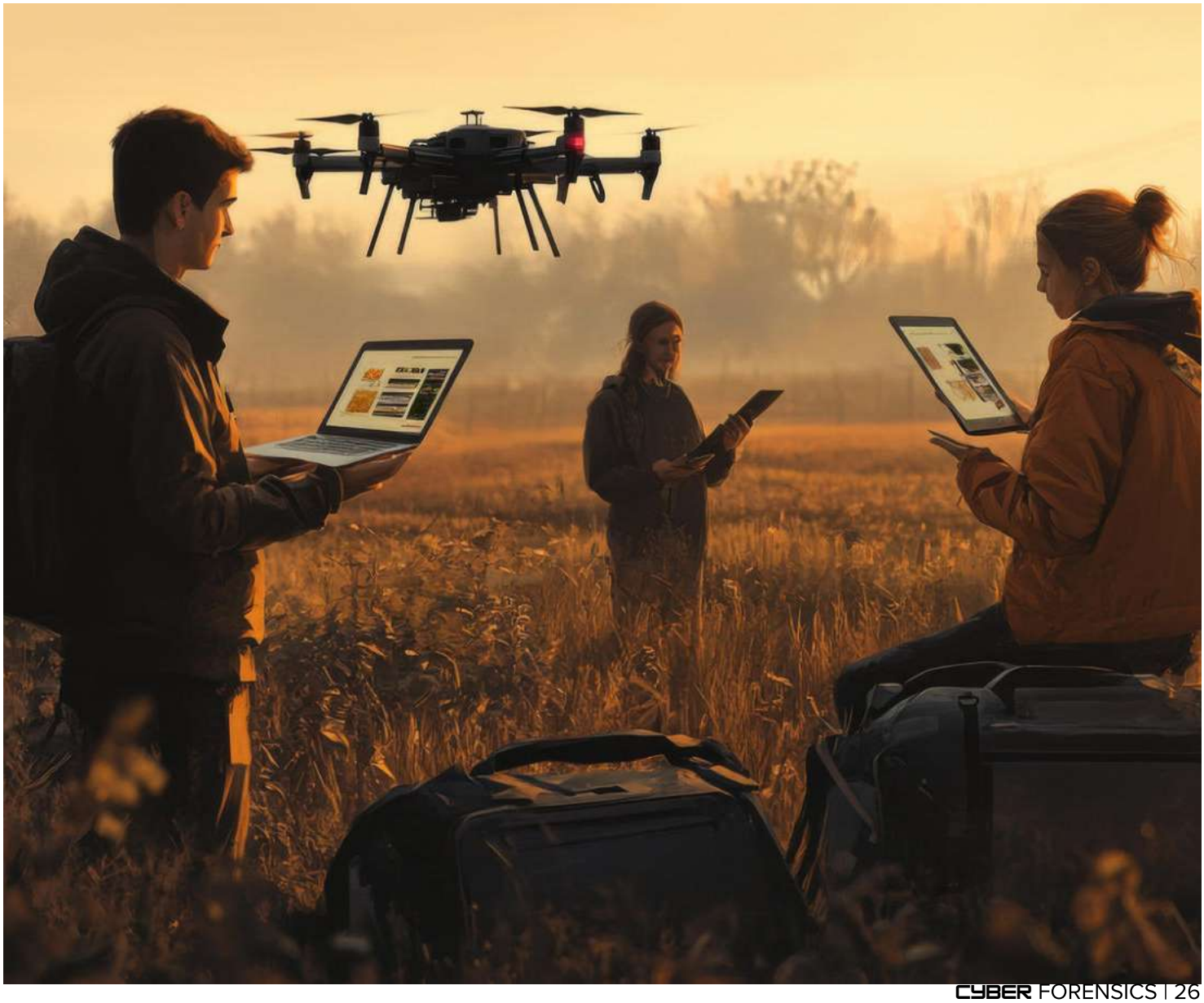
Growing drone data complexity makes manual analysis impractical. AI and ML automate analysis, detect patterns, and reconstruct events.

3.3.1 LSTM and Transformer Models for Flight Path Anomaly Detection



DIGITAL TWIN ACCIDENT RECONSTRUCTION PROCESS





4. Case Studies in Drone Misuse (2023-2025)

The increase in drone-related crimes from 2023 to 2025 highlights the real-world use of forensic techniques.

Recent (2023-2025) Drone-Related Security Incidents:

DRONE INCIDENTS RANGE FROM MINOR DISRUPTION TO STRATEGIC IMPACT

5. India Drone Forensics Ecosystem

India has come up with a complete "whole-of-government" drone forensics plan that combines new legal frameworks, institutional capacity at the national and state levels, and operational feedback to make a closed-loop system that is both responsive and strong.

5.1 Regulatory Framework (Bharatiya Nyaya Sanhita and BSA 2023):

In 2023, India updated its laws and replaced the old Indian Evidence Act with the Bharatiya Sakshya Adhiniyam (BSA), 2023. This new law stipulates that electronic and digital records, such as data from drones, controllers, and other related devices, can be used as legal evidence. The Bharatiya Nyaya Sanhita (BNS), 2023, goes into more detail about digital crime, such as fake electronic records, and sets a clear legal basis for drone forensic data.

5.2 Key Institutions:

Specialised institutions help the legal system and push the development of practical drone forensics.

The National Forensic Sciences University (NFSU) is in charge of national drone forensics. As of May 2025, it had a "digital threat library" that listed over 35 drone models and 5,000 parts. This resource lets investigators find and extract data from even damaged drones, and it helps them train and make tools for their work.

Kerala Police Drone Forensic Lab: This is India's first state-level lab for drone forensics, and it opened in 2021. It has sections for recovering drone evidence that has been approved, researching anti-drone technology, developing indigenous UAVs, and AI-powered research and development. The lab has helped figure out who was flying intercepted drones and who was behind them, which has built up important local knowledge.

Border Security Force (BSF) C-UAS Operations: The BSF has put in place a three-part plan to deal with the frequent drone smuggling incidents it faces. This plan includes drone interception, forensic hardware analysis, and arrests on the ground. In 2024 alone, more than 200 recovered drones were able to have their flight logs, GPS data, and encrypted communications analysed in real time using tools like the Skynet Intel forensic platform. The NFSU library gets information from forensic results, which helps with new counter-drone strategies and technology upgrades.

India's proactive and adaptable drone forensic and counter-drone capabilities are based on this ecosystem, which includes updated laws, national and state institutions, and operational field data.

References

Al-Saba, M. F., Douligeris, C., & Al-Saba, T. R. (2024). Drone forensics: An innovative approach to the forensic investigation of drone accidents based on digital twin technology. *Drones, 12*(1), 11. https://www.mdpi.com/2227-7080/12/1/11

ArduPilot. (n.d.). *Downloading and analyzing data logs in Mission Planner*. Retrieved August 4, 2025, from https://ardupilot.org/copter/docs/common-downloading-and-analyzing-data-logs-in-mission-planner.html

ASIS International. (2025, March). Drone-assisted corporate espionage. *Security Management Magazine*. https://www.asisonline.org/security-management-magazine/latest-news/today-in-security/2025/march/drone-corporate-espionage/

Azhar, H. (2019). Challenges and techniques in drone forensics [Conference presentation]. CYBER 2019, The Fourth International Conference on Cyber-Technologies and Cyber-Systems, Porto, Portugal. (https://www.iaria.org/conferences2019/filesCYBER19/HannanAzhar_Tutorial_ChallengesAndTechniques.pdf)

Bureau of Police Research & Development. (2024, January 29). Use of technology in new criminal laws. (https://bprd.nic.in/uploads/pdf/20240129040422119463 4UseofTechnology.pdf)

DJI. (n.d.). DJI Transmission - Specs. Retrieved August 5, 2025, from https://www.dji.com/transmission/specs

DroneDesk. (n.d.). DJI flight log. Retrieved August 6, 2025, from https://blog.dronedesk.io/dji-flight-log/

European Union Aviation Safety Agency. (n.d.). Understanding European drone regulations and the aviation regulatory system. Retrieved August 6, 2025, from(https://www.easa.europa.eu/en/domains/drones-air-mobility/drones-air-mobility-landscape/Understanding-European-Drone-Regulations-and-the-Aviation-Regulatory-System)

Federal Aviation Administration. (n.d.). Become a certificated remote pilot. Retrieved August 6, 2025, from https://www.faa.gov/uas/commercial_operators/become_a_drone_pilot

Federal Aviation Administration. (n.d.). Understanding your authority: Handling sightings and reports. Retrieved August 6, 2025, from https://www.faa.gov/uas/public_safety_gov/sightings_reports

Federal Law Enforcement Training Centers. (n.d.). JTAG chip off for smartphones training program. Retrieved August 5, 2025, from https://www.fletc.gov/jtag-chipoff-smartphones-training-program

Government of India. (2023). The Bharatiya Nyaya Sanhita, 2023. Ministry of Home Affairs. https://www.mha.gov.in/sites/default/files/250883_english_01042024.pdf

Intelligence Fusion. (n.d.). India-Pakistan border: Chinese drones fuelling arms and drugs trafficking. Retrieved August 5, 2025, from https://www.intelligencefusion.co.uk/insights/resources/article/india-pakistan-border-chinese-drones-arms-drugs-trafficking/

Kerala Police Cyberdome. (n.d.). Kerala Police drone forensic lab & research centre. Retrieved August 4, 2025, from https://drone.cyberdome.kerala.gov.in/cyberdome/

Kumar, A., Singh, A., & Singh, A. (2024). A blockchain-based chain of custody framework for digital evidence management. Journal of Emerging Technologies and Innovative Research (JETIR), 11(6), h349-h354.(https://www.jetir.org/papers/JETIR2406739.pdf)

Li, Y., Wang, J., Zhang, Y., & Liu, Y. (2023). Anomaly detection of fixed-wing unmanned aerial vehicle (UAV) based on cross-feature-attention LSTM network. Aerospace, 10(11), 949. https://doi.org/10.3390/aerospace10110949

Live555. (n.d.). Documenting the format of DJI log files. Retrieved August 6, 2025, from http://djilogs.live555.com/

Navrat Stratagic Analytics. (2025). Counter-unmanned aerial system (C-UAS) market. https://navistratanalytics.com/report_store/counter-unmanned-aerial-system-c-uas-market/

Shastri, P. (2025, May 27). NFSU's 'digital threat library' to advance drone forensics. The Times of India. https://timesofindia.indiatimes.com/city/ahmedabad/nfsus-digital-threat-library-to-advance-drone-forensics/articleshow/121421019.cms

Vauvillier, L. (n.d.). dji-log-parser: A library to parse records from DJI.txt logs. GitHub. Retrieved August 6, 2025, from https://github.com/lvauvillier/dji-log-parser

Teel Technologies. (n.d.). What is JTAG, chip-off and ISP? Retrieved August 6, 2025, from https://www.teeltech.com/ufaqs/what-is-jtag-chip-off-and-isp/

Darshil Raval,

Security Researcher from Gujarat, India

About the Author:

Darshil Raval is a Security Researcher from Gujarat, India, specializing in vulnerability assessment, penetration testing, and digital forensics. With a background in Computer Science and Engineering focused on Cyber Security, he has worked as a contract Security Engineer for a Y Combinator-backed AI startup, where he identified and reported critical vulnerabilities in open-source projects. He also brings hands-on experience as a Digital Forensics & Incident Response Analyst Intern, analyzing digital artifacts and automating evidence collection. *He can be found on Linkedin. Darshil's blog: https://ciphersec.hashnode.dev/*

Conclusion

Drone forensics is at a crucial point because UAV technology is changing quickly, and drones are being used for both legal and illegal purposes. Digital forensic methods that used to work well are no longer enough because threats happen every day across borders, in critical infrastructure, and in sensitive airspace. To deal with these problems, we need a new, multidisciplinary set of investigative tools.

Forensic science for drones is changing. To get to encrypted data, investigators need advanced hardware methods like chip-off, JTAG, and ISP. To intercept real-time communication, they need RF analysis. AI and machine learning are making it easier to analyse telemetry data, find anomalies, and report suspicious activity. Blockchain makes sure that evidence chains cannot be tampered with. India's global strategies include updating the law, doing research, and training. But there aren't any standardised international procedures. The drone forensics market is likely to grow a lot because more UAVs are being used and crime is rising. To keep the airspace safe, we will need to spend money on specialised training, work together, and use next-generation tools.

Abstract- Drones are rapidly becoming a part of India's progress in areas like agriculture, security, logistics and other critical sectors. As they grow deeper into our ever-expanding digital landscape, it is becoming crucial to enhance the capability of our country to investigate incidents involving drones. This art -icle analyses global trends in drone forensics, id -entifies Indian-specific gaps and suggests grou -ndlevel steps towards innovation and policy ref -orm. Drawing on international evidence and best practice, it sets out inexpensive hardware, sophisticated training, and effective regulation as the building blocks of a strong forensic toolkit to confront these threats posed by the new dron -e technology.

Introduction- Drones are being used everywher -e across the globe, ranging from being used as basic recreational toys to essential security, busi -ness and critical public service tools. In India, the uses include agriculture, disaster relief, infras -tructure scanning, border surveillance, environ mental research, delivering goods and much mo -re. They have been extremely effective in enhan -cing operational efficiency, minimising man exp -osure, and providing services in areas previousl -y inaccessible by humans. But the same reason -s that make drones versatile also make them vulnerable to misuse. From smuggling contraban -d and conducting illegal surveillance to targeted attacks, the risk of misuse is present and growin -g. Such risks prompt the need for clear regulatio -ns and active enforcement. India's current regulatory framework, led by the Directorate General of Civil Aviation's (DGCA) Drone Rules 2021, governs operational permission and safety guidelines. These regulations form a healthy basis for legal use of drones, but fail to give investigating agencies sufficient resources and powers to carry out follow-up investigations in the event of an incident. Drone forensics, the recovery, processing, and analysis of evidence from drones, is in its early stages in the nation. International findings could help India formulate an adapted forensic capability to match its fast-evolving drone environment.

Worldwide Practices in Drone Forensics

On the world stage, drone forensics science is advan ing using formal models, expert tools, and cross-doma -in knowledge sharing. The Comprehensive Collectio n and Analysis Forensics Model (CCAFM) introduces a formal process for evidence collection, analysis, and reporting that preserves evidentiary integrity through out. The Drone Forensics Readiness Framework (DRF RF) extends this with a focus on readiness prior to inci -dents, pre-configured data collection tools, common logging formats, and response teams. Drone analyses of best-selling drones, including DJI and Parrot, have uncovered a range of recoverable data, such as GPS coordinates, flight patterns, height data, battery life, operator names, and internal image metadata. Such information is invaluable when it comes to reconstru cting events and assessing fault. However, challenges remain. Stored encryption renders vital evidence inac -cessible without decryption keys. Unconventional log files hinder analysis across vendors. Proprietary firm ware prevents third-party analysis and occasionally overwrites sensitive logs upon rebooting the system. Machine learning also holds the potential to enhance drone forensics. By examining flight behaviour and telemetry information, algorithms identify suspicious behaviour. For example, drastic changes in direction or a decrease in altitude would signal possible GPS spoofing, signal jamming, or unauthorised command inputs. These anticipatory measures can enable investigators to locate malicious activity sooner and more accurately.

Gaps in the Indian Context

Even though India has been quickly developing its drone sector, it does not have a systemic process of drone forensics. India lacks an SOP or national standa rd for law enforcers, border guarding forces, or forens ic units for handling confiscated drones. Lack of guide lines means that evidence becomes contaminated, de stroyed, or lost, potentially compromising legal cases.

Arundhati Gupta

Mechanical Engineering student at the University of British Columbia, Canada

DRONE FORENSICS IN THE INDIAN CONTEXT:

Gaps, Innovation, and Policy Needs

Another area of challenge is the lack of specialised tools. Most of the agencies do not have Software Defined Radios (SDRs) for intercepting and analysing communication signals, telemetry log decoders to gain access to flight data, and firmware analysis tools to analyse embedded code. These tools are standard in developed forensic labs abroad but are still in limited numbers in India. The skills gap is also acute. Few researchers have experience with drone design, wireless protocol, or methods of evidence recovery. This shortage reduces the capacity to carry out effective investigations, particularly in time-sensitive cases where drones are relevant to criminal or national security matters. Legislative ambiguity contributes to the above gaps in operations. Current legislation is vague about data ownership, retention periods for drone flight records, or privacy regulations for data collected during investigations. Such vagueness makes it hard to prosecute offenders and protect civil rights.

Opportunities for Innovation

India's industrial capability and human capital in technology are well-positioned to fill such gaps. Inexpensive, open-source toolkits tied to a platform such as Raspberry Pi or ESP32 might make it possible for field agents to easily record logs and telemetry information without costly hardware. The latter can be included in handheld forensic kits to employ in far-flung or resource-constrained areas. Tamper-proof logging equipment, much like an airplane black box, would guarantee the integrity of vital information even in the case of damage or attempted erasures. They could record encrypted, timestamped logs accessible only to allowed investigators. Artificial intelligence and data analytics introduce a second capability level. AI platforms can scan vast amounts of telemetry and sensor data to identify patterns or anomalies that may not be caught by human validation. One such example is identifying a drone flying off course or entering a prohibited area with real-time alerts. Training and education are paramount. Including drone forensics courses in university, vocational school, and police academy curricula would provide a body of trained professionals to work with and move up in this area.

Policy Recommendations

In order to develop a strong forensic framework, India would need a national policy on drone forensics led by agencies like NTRO or CERT-In. The policy must include well-defined SOPs for the handling of evidence, from the moment of seizure at initial stages through examination and presentation in a court of law. Factory owners will be required to fit encrypted, tamper-proof logging subsystems into every drone on sale in India. This would not only aid forensic investigations but also discourage bad actors with knowledge of inescapable traceability.

References:

Al-Dhaqm, A., et al. (2022). A comprehensive collection and analysis model for the drone forensics field (CCAFM). *ResearchGate*.https://www.researchgate.net/publication/363098113

Alotaibi, F. M., et al. (2022). Drone forensics readiness framework (DRFRF). *PubMed Central*.https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8901304/

Baig, Z., et al. (2022). Drone forensics and machine learning: Sustaining the investigation process. ResearchGate. https://www.researchgate.net/publication/360072198

Adel, A. (2024). Watch the skies: A study on drone attack vectors. MDPI. https://www.mdpi.com/1999-5903/16/7/250

Taylor, A. (2023). Forensics case study of DJI Mini 3 Pro. arXiv. https://arxiv.org/abs/2309.10487

Directorate General of Civil Aviation. (2021). Drone Rules, 2021. DGCA. https://dgca.gov.in

Ministry of Civil Aviation. (2021). Digital Sky Platform. https://digitalsky.dgca.gov.in

Indian Computer Emergency Response Team. (2023). Advisory on secure UAV operations. CERT-In. https://www.cert-in.org.in

Arundhati Gupta,

Mechanical Engineering student at the University of British Columbia, Canada

About the Author:

Arundhati Gupta is a Mechanical Engineering student at the University of British Columbia, Canada, with an interest in cybersecurity and emerging technologies. Drawing on her background in hardware systems and a strong foundation in problem-solving, she is exploring how engineering principles can strengthen digital security, particularly in areas like the Internet of Things (IoT), where physical devices and software intersect.

Public-private partnerships can facilitate indigenous forensic capabilities to be designed at a quick pace. Partnerships between government, academia, and industry can give rise to open standards for data formats, open-source analysis tools, and sophisticated training modules. Embracing and modifying best practices of global agencies such as the FAA, EASA, and ISO will enable India to embrace global standards while modifying them for local needs. This may include harmonising regulations with respect to data retention, requirements for operator identification, and reporting of incidents. Investments in freestanding forensic tools and facilities at the national and state levels, such as SDRs, analysis instrumentation, and secure storage units, will provide readiness to respond to high-profile or mass-gamut events. Periodic training of investigators, prosecutors, and technical specialists will maintain the nation's capabilities against the changing threats.

Conclusion

India's drone economy is on the cusp of expansion, with uses that can revolutionise industries and government services. But accountability will have to accompany it. Without simultaneous investment in forensic readiness, the nation risks being overwhelmed by misuse or ill intent on the part of drones. By adopting proven global models such as CCAFM and DRFRF, India can craft systems that offer evidence, make investigations affordable, and provide accountability. The path ahead requires the initial investment in technology, the establishment of specialty training programs, and the production of definitive legal guidelines.

SECURING CLOUD-CONNECTED DRONE FL OPERATIONS:

VYOM

LEET

A Comprehensive Framework for Next-Generation Autonomous Systems

Introduction- Autonomous drone fleets are reshapin -g industries from infrastructure inspection to enviro nmental monitoring. As operations scale to include dozens or hundreds of drones, ensuring the security of both the devices and their cloud-based coordination systems becomes paramount. Cloud-connected fleets introduce complex attack surfaces-spanning wireless links, edge devices in remote environments, and centralized cloud infrastructure-that must be protected without impeding real-time performance.

The Cybersecurity Challenge Landscape

COMMUNICATION PROTOCOL VULNERABILITIES

Drones commonly rely on protocols such as MAVLink for telemetry and command. By default, MAVLink messa ges are unencrypted, exposing them to eavesdropping, GPS spoofing, and command interception. Likewise, radio-frequency links operating on ISM bands can be jammed or hijacked, while Wi-Fi pathways risk man-in-the-middle exploits and deauthentication attacks.

CLOUD INFRASTRUCTURE ATTACK VECTORS

A cloud platform coordinating large fleets must manage multi-tenant isolation, secure API endpo -ints, and hardened serverless functions. Unres tricted access to cloud resources, insufficient input validation, or misconfigured identity permis sions can allow attackers to execute server-side request forgery (SSRF), escalate privileges, or move laterally across services.

EDGE COMPUTING SECURITY GAPS

Edge autonomy-enabling drones to continue missions during network disruptions-requires ro bust local security. Physically exposed hardware is at risk of tampering, and intermittent connect ivity can delay critical updates. Resource-constra ined processors may lack full-capability cryptogr aphy by default, creating potential integrity and confidentiality gaps for locally stored mission data.

Vyom IQ's Cloud Robotics Security Architecture

Vyom IQ's platform addresses these challenges through layered defenses tailored to autonomo us systems.

MESH NETWORKING WITH SECURE KEY EXCHANGE

Vyom IQ implements a hybrid mesh networking design, enabling drones to route data through peer nodes when line-of-sight links are unavailable. Each mesh node performs authenticated, encrypted exchanges using industry-standard methods. Secure key management ensures that communications remain protected even if individual nodes encounter anomalies.

AI-DRIVEN MONITORING AND RESPONSE

The platform continuously analyzes fleet telemetry for deviations from expected patterns. When anomalies-such as unexpected command sequences or erratic signal metrics-are detected, Vyom IQ automatically shifts drones to alternate communication channels and raises alerts on the operations dashboard. This automated detection and mitigation capability helps teams maintain uninterrupted operations.

END-TO-END DATA PROTECTION

All data flowing between drones and the cloud is encrypted in transit and at rest. Vyom IQ's buffer-upload mechanism ensures that sensor data collected during connectivity gaps is cryptographically signed and verified upon upload, preserving data integrity even in intermittent network conditions.

EDGE AUTONOMY WITH BUILT-IN SAFEGUARDS

VyomOS, Vyom's real-time operating system for drones, provides secure boot processes and enforces application isolation on each vehicle. These controls allow drones to execute mission logic locally without exposing critical system functions. Even when disconnected, drones maintain adherence to mission constraints and security policies.

ZERO-TRUST PRINCIPLES

Adopting a zero-trust mindset, Vyom IQ treats every device, user, and communication channel as untrusted until authenticated. Role-based access controls govern who can issue flight plans, adjust security settings, or retrieve sensitive logs-ensuring that no single compromised credential can undermine the entire fleet.

Future-Proofing Against Emerging Threats

Video heading:
Contributed Content:

Scan the QR to watch the Video

Scan the QR to watch the Video

▶ VYOM

Disclaimer:

The views and content expressed in contributed articles and accompanying media are solely those of the authors and do not necessarily reflect the views of Cyber4N6 or CyberPeace Foundation. Cyber4N6 does not assume liability for the accuracy of technical claims or product endorsements contained herein.

Vyom's architecture is designed to evolve alongside the threat landscape:

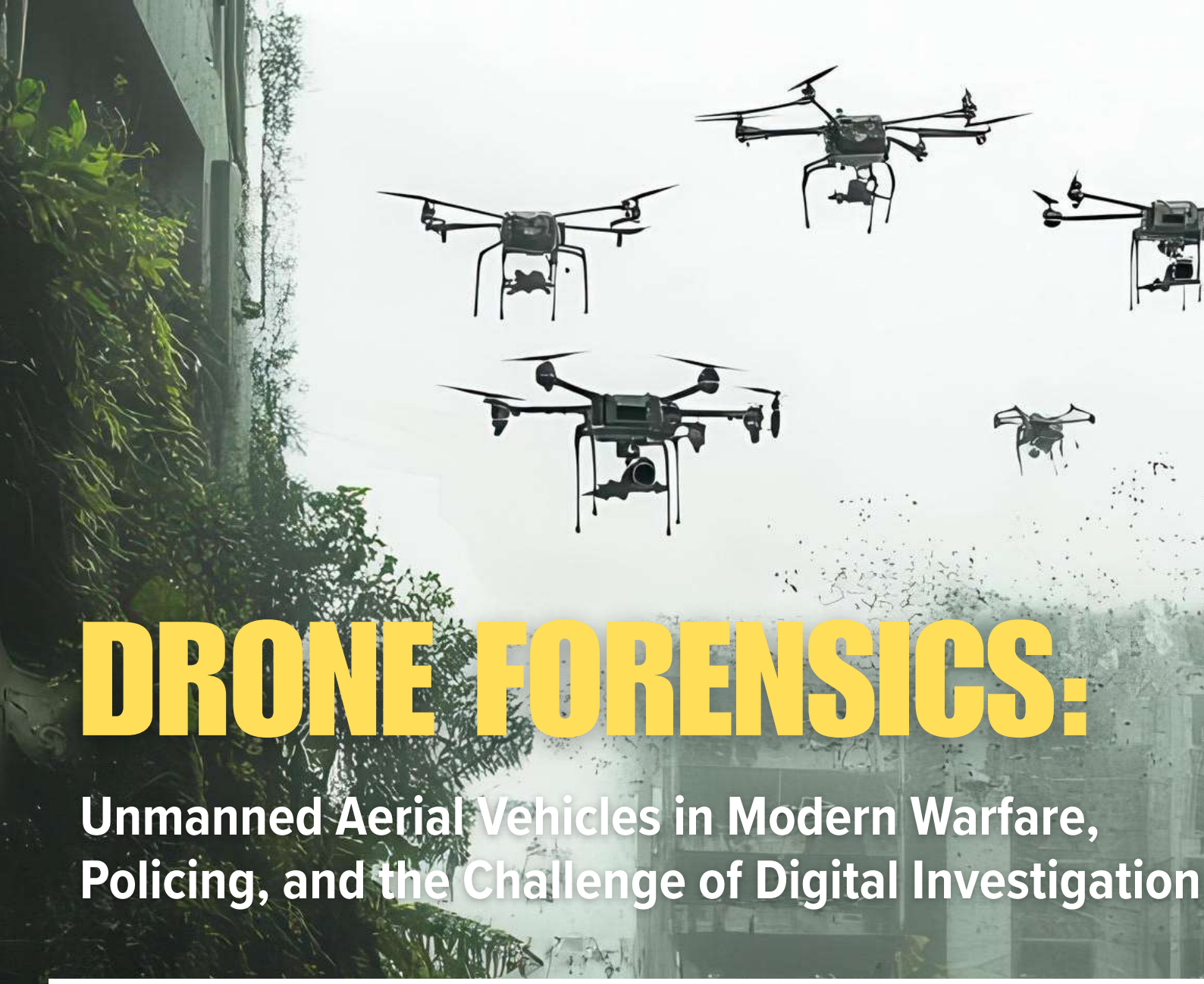
- **Extensible Protocol Support:** New encryption suites and authentication modules can be integrated via VyomOS's modular design.
- **Distributed Analytics:** Machine learning models for anom aly detection are updated seamlessly through cloud-base -d deployment, allowing rapid response to novel attack vectors.
- **Resilient Connectivity:** Mesh networking adapts dynamic -ally to link disruptions, maintaining security and perform ance without manual intervention.

Recommendations for Secure Fleet Deployment

- **Layered Defense:** Combine encrypted mesh communicati on, cloud-native access controls, and secure edge autonomy to cover all threat surfaces.
- **Continuous Monitoring:** Leverage real-time anomaly dete -ction to identify incomplete or malicious commands befo -re they impact missions.
- **Robust Update Mechanisms:** Ensure both cloud services and drone software receive timely patches, with fail-safe rollbacks for mission-critical operations.
- **Zero-Trust Access:** Implement strict role definitions and multi-factor authentication for all operational workflows.

Conclusion

Securing cloud-connected drone fleets demands an architecture that integrates device-level protections, network security, and cloud infrastructure hardening. Vyom IQ's cloud robotics platform and VyomOS operating system deliver these capabilities by design, enabling organizations to operate large-scale autonomous systems with confidence. By embracing layered security, real-time monitoring, and edge autonomy safeguards, teams can tackle emerging cyber threats effortlessly-keeping their fleets safe and their missions on course.



DRONE FORENSICS:

Unmanned Aerial Vehicles in Modern Warfare, Policing, and the Challenge of Digital Investigation

Introduction- Drones, or Unmanned Aerial Vehicle -s (UAVs), have revolutionized both commercial se -ctors and the military landscape in the Past decade. As their applications have expanded from aerial photogr -aphy and delivery services to leading offensive operati -ons and intelligence missions in contemporary conflicts -, the risks of their misuse have grown commensurately. This dual-use nature has created a pressing need for drone forensics: the systematic extraction and analysis of digital and physical evidence from drones and their associated infrastructure. As nations contend with cros s-border incursions, terrorism, smuggling, and evolving warfare strategies, drone forensics is rapidly becoming a cornerstone of digital security and law enforcement.

Uses of Drones: Commercial and Military

COMMERCIAL APPLICATIONS

Drones are widely used in various commercial sect ors, benefiting from their agility, cost-effectiveness, and ability to reach inaccessible locations:

- **Agriculture-** Crop monitoring, pesticide sprayin -g, and precision agriculture leverage drone-bas ed multispectral sensors, improving yields and lowering costs.
- **Logistics and Delivery-** Companies like Amazon and Zipline use drones for rapid parcel deliverie s, especially in remote or disaster-affected locat ions.
- **Surveying and Mapping-** Construction sites, mining operations, and urban planners use

Lt Col (Dr) Santosh Khadsare

Cyber Forensic Expert

"In the age of drone warfare and aerial surveillance, forensic science must evolve at the speed of innovation. The ability to dissect a drone's digital footprint isn't just about solving crimes—it's about preventing the next attack."

drones for real-time mapping and 3D modeling.

- **Disaster Management-** Drones provide aerial reconnaissance in disaster zones, assisting in search and rescue, damage assessment, and delivery of essential supplies.
- **Media and Entertainment-** Aerial cinematography, live broadcasting of events, and news journalism utilize drones for unique vantage points and coverage.
- **Infrastructure Inspection-** Power lines, pipelines, cellular towers, and bridges are inspected safely and efficiently.
- **Law Enforcement-** Crime scene reconstruction, surveillance, crowd monitoring, and traffic management, all benefit from real-time drone feeds.

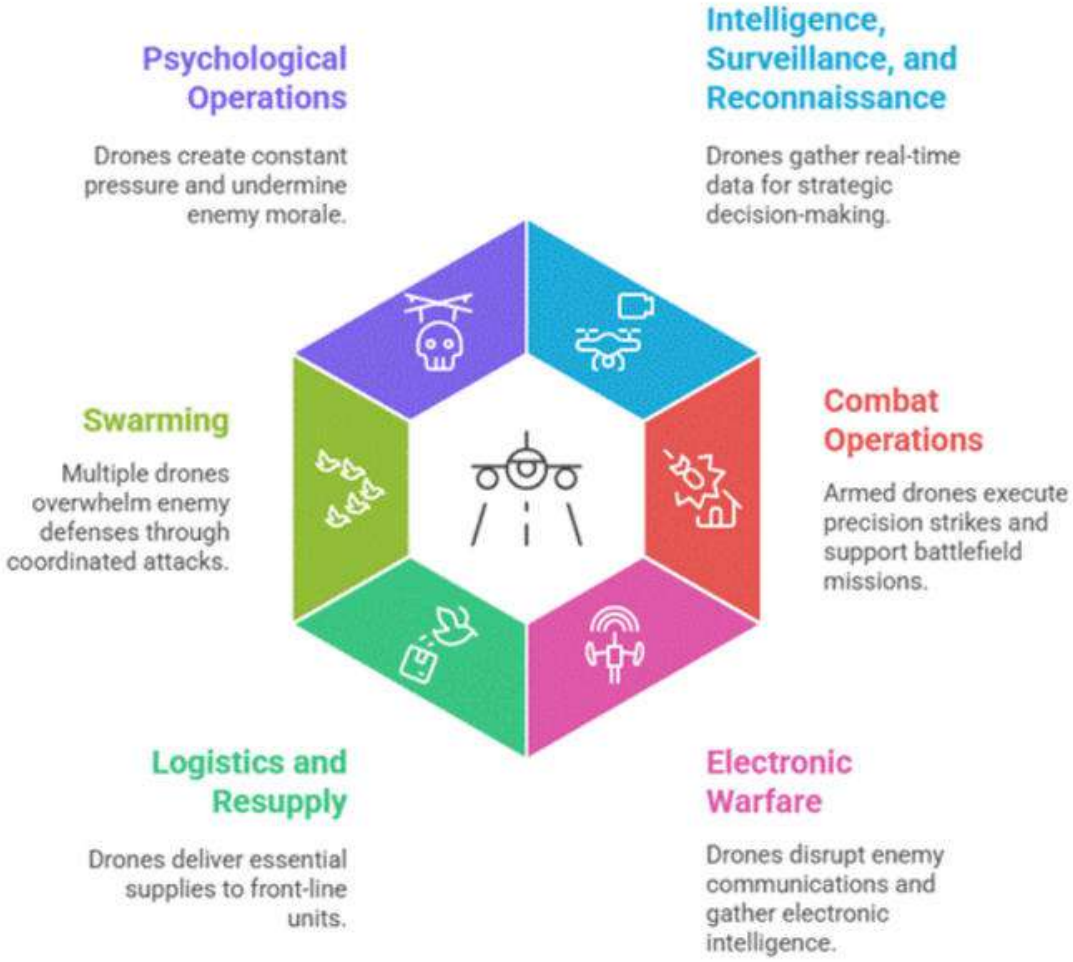
MILITARY USES

Military drones have evolved from surveillance platforms to core components of offensive and defensive strategies:

- **Intelligence, Surveillance, and Reconnaissance (ISR)-** Military drones conduct real-time monitoring, border surveillance, target acquisition, and pattern-of-life analysis, minimizing risks to personnel.
- **Combat Operations-** Armed UAVs deliver precision strikes, carry out assassination missions, and provide battlefield support (e.g., Bayraktar TB2, MQ-9 Reaper).
- **Electronic Warfare-** Jamming, decoy operation

Commercial Drone Applications

Military Drone Applications



s, and electronic intelligence gathering are possible with specialized UAVs.

- **Logistics and Resupply-** Drones transport supplies , ammunition, and medical equipment directly to fr -ont-line units.
- **Swarming-**Deployments of multiple autonomous, networked drones overwhelm enemy defenses.
- **Psychological Operations-** The persistent presenc -e of drones undermines adversary morale and creates constant pressure.

Drones in Recent Conflicts

RUSSIA-UKRAINE WAR

- Dubbed the first "full-scale drone war," both sides have used drones extensively for ISR, artillery spotting, and direct strikes.
- Civilian drones, alongside military-grade UAVs, are repurposed for reconnaissance and bombing missi -ons.
- The Ukrainian military has established a dedicated drone branch and ramped up domestic drone prod uction.
- Ukraine has leveraged drones for attacks inside Russian territory, including strikes on infrastructure and naval assets.
- Russia's Orlan-10 has become central in targeting and intelligence operations.

ARMENIA-AZERBAIJAN (2020 NAGORNO-KARABAKH WAR)

- Azerbaijani forces used Turkish and Israeli UAVs (e.g., Bayraktar TB2, Harop loitering munitions) to destroy Armenian air defenses, artillery, and armor.
- Drones decimated nearly 50% of Armenian air defense systems in the conflict's opening hours, shifting the battlefield swiftly.
- The conflict marked a pivotal shift, making UAVs decisive weapons rather than support tools.

INDIA-PAKISTAN

During Operation Sindoor—the 2025 India-Pakistan conflict—drones played a central operational role on both sides, marking the first major drone-centric military engagement between the two countries. After India's precision strikes on terror camps in Pakistan and Pakistan-occupied Kashmir in response to the Pahalgam terror attack, Pakistan retaliated by launching mass raids of drones—numbering over 600 —against Indian border towns, military facilities, and critical infrastructure.

KEY ASPECTS OF DRONE USE IN OPERATION SINDOOR:

- **Swarm tactics:** Pakistan deployed waves of low-co -st, low-tech drones in swarms over four days to overwhelm Indian air defenses, clutter radars, gath -er intelligence, and attempt to inflict damage on military and civilian targets.
- **Variety of drones:** The conflict saw not only conve -ntional UAVs but also decoy drones, loitering mun itions, and electronic decoys intended to exhaust Indian interceptor stocks and probe vulnerabilities.
- **Indian response:** India rapidly mobilized a layered air defense network—over 1,000 anti-aircraft guns and over 750 short- and medium-range surface-to-air missile systems—along the Line of Control and international border. The indigenous Akash surfac -e-to-air missile system, legacy platforms like Pech ora and OSA-AK, and real-time coordination by the Integrated Air Command and Control System enab -led interception of the drone waves.
- **Outcome:** Indian forces neutralized or destroyed more than 600 Pakistani drones, preventing signifi cant damage to intended targets157.

- This robust defense effectively countered the drone threat and safeguarded vital military and civilian infrastructure.

- **Shift in warfare:** Operation Sindoor established drones—especially in swarms—as pivotal tools of modern conflict in South Asia, underlining both their disruptive potential and the necessity of advanced counter-UAV capabilities.

Operation Sindoor serves as a clear example of dron es being used not just for surveillance, but for strikes, electronic warfare, and psychological operations withi n a major India-Pakistan engagement.

OTHER CONFLICTS

- **Syria conflict:** Syrian and Turkish forces, as well as non-state actors, have used drones for coordinate d attacks and targeted bombings.

- Terror groups have increasingly exploited cheap commercial drones for attacks, such as the Homs, Syria attack in 2023, killing over 89 people.

Drone Forensics: Definition and Scope

Drone forensics is the discipline focused on identifyin g, extracting, preserving, analyzing, and presenting digital and physical evidence from drones and associat ed systems. Its objectives are to:

- Identify drone make, model, and origin
- Recover flight logs, paths, and telemetry
- Trace ownership and link devices to operators
- Uncover payload details (e.g., whether a drone carried explosives or contraband)
- Aid attribution in crimes, military incidents, or security breaches359

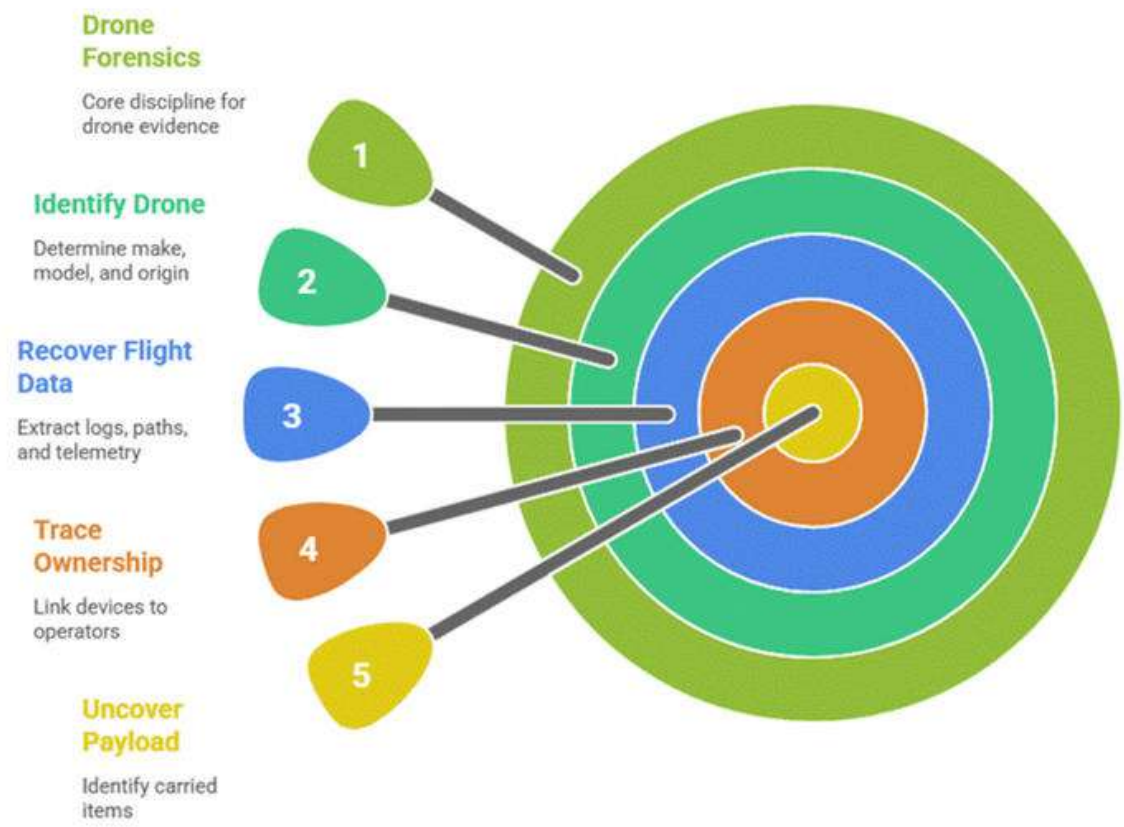
The forensic process typically includes not only the physical UAV but also remote controls, communication systems, ground control stations, and, increasingly, the drone's backend infrastructure and associated cloud services.

The Drone Forensics Process

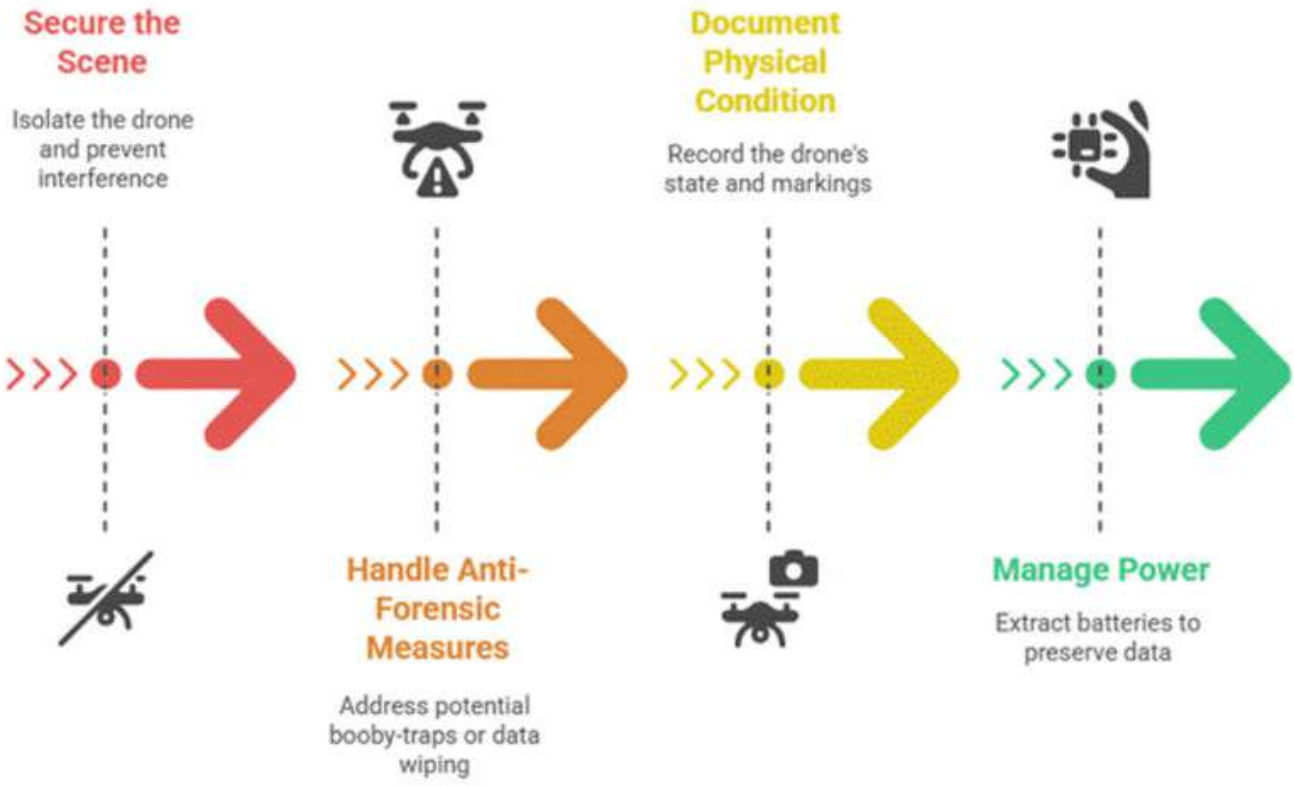
COLLECTION AND PRESERVATION

- **Securing the scene:** Avoiding signal interference and isolating the drone from its operator,

Drone Forensics: Definition and Scope



Collection and Preservation



especially in active threat scenarios (e.g., using RF jammers).

- **Handling anti-forensic measures:** Drones may be booby-trapped or employ memory wiping and self-destruction protocols.

- **Documenting physical condition:** Photographic and written records of condition, damage, and markings.

- **Power management:** Extracting batteries with proper precautions to prevent data loss from volatile memory.

PHYSICAL FORENSICS

- **Chassis/frame analysis:** Identifying manufacturer, model, modifications, and repairs.

- **Component inventory:** Examining propellers, motors, cameras, flight controllers, GPS modules, and payload mechanisms.

- **Serial numbers and custom chips:** Some drones have identifiable serial numbers or unique chips, which can be traced to vendors or operators.

DIGITAL FORENSICS

- **Flight Controller Data Extraction:** Flight controllers store logs on internal memory or SD cards, including GPS coordinates, altitude, speed, and sometimes video footage.

- **Telemetry & Communication Logs:** Extracting radio frequencies, Wi-Fi, Bluetooth, and cellular data—can trace communication to a ground station or operator's device.

- **Firmware, Software, and Settings:** Investigating firmware version, installed apps, custom scripts, and any evidence of tampering or malicious programming.

- **Peripheral and Network Forensics-** The mobile device, laptop, or custom controller used by the operator is forensically imaged and analyzed.

- **Cloud & Backend Analysis-** Most modern drones sync data to the manufacturer's cloud—retrieving user accounts, uploaded flight data, location history, and device associations is critical.

ANALYSIS AND ATTRIBUTION

- **Mapping Flights:** Reconstructing the drone's route, launch and landing points, and any actions taken (e.g., hover, drops).

- **Linking Devices:** Correlating controllers, phones, and even network traces to a person or group.

- **Payload Analysis:** Determining if the drone was used for illicit purposes, including explosives, surveillance gear, or smuggling.

Methods and Global Tools for Drone Forensics

ANALYTICAL METHODS

- **Chip-Off and JTAG Forensics-** For advanced forensics, memory chips are physically removed or accessed via debugging interfaces to recover deleted or protected data.

- **RF Analysis-** Spectrum analysis tools pinpoint communication frequencies and protocols, potentially identifying the operator or base station.

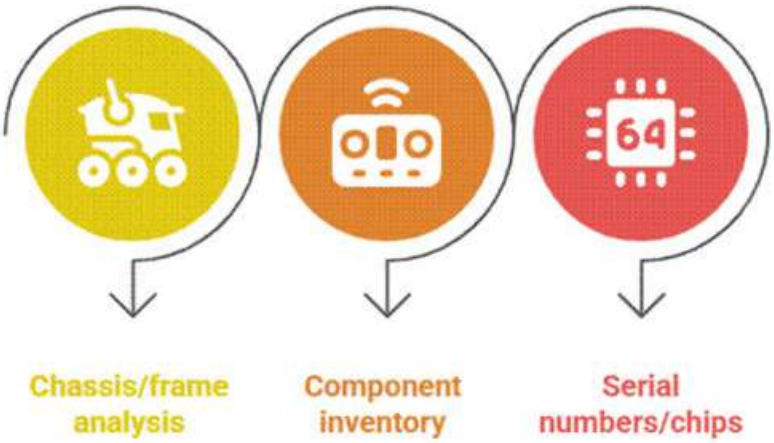
- **Reverse Engineering-** Firmware, custom software, or encrypted logs are reverse-engineered for deeper insights or to bypass security.

- **Image and Video Forensics-** Embedded cameras can retain video; metadata analysis yields geographic and chronological context.

GLOBAL TOOLS AND FRAMEWORKS

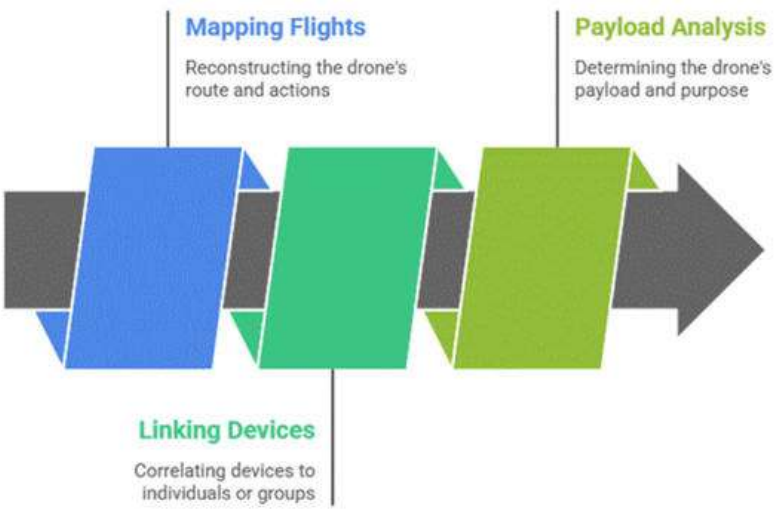
- **Open-source Forensic Suites-** Tools such as Autopsy, Magnet AXIOM, FTK Imager, and X-Ways can be adapted for drone memory analysis.

Drone Physical Forensics



Digital Forensics

Drone Analysis and Attribution Process



- **Specialized Drone Forensics Tools**

    - DJI's Flight Data Viewer and Blackbox Extracto r: For extracting and visualizing logs from the w orld's most popular drone brand.
    - Cellebrite and Oxygen Forensics: Mobile foren sic solutions that increasingly incorporate dron e controller support.
    - RF Signal Analysis Platforms (e.g., HackRF, SD R-based solutions): Capture and analyze drone communications.
    - DroneID databases and Digital Threat Librarie s: Maintain fingerprinted profiles of drone fram es, chips, and communication signatures.
    - Custom National and agency-specific software: Bilt for integration with law enforcement and military forensics labs.

COLLABORATION AND TRAINING

- **Integrated forensic training programs:** Police, military, and paramilitary forces are being equipped for hands-on drone forensics.

- **Public-private partnerships:** Collaboration with academia and cybersecurity industry accelerates research and tool development.

The Future of Drone Forensics

Drone forensics is poised for exponential growth and sophistication, driven by several factors:

- **Proliferation of Drones-** As both military-grade and commercial-off-the-shelf (COTS) drones become ubiquitous, so does the scope for their misuse and the complexity of forensic investig ation.

- **Autonomous & Swarm Drones-** Forensics will have to address communication within

autonomous swarms, distributed control, and dece ntralized decision-making.

- **AI-Powered Drones-** The use of AI can automate Evasion techniques, route planning, and target sele -ction, challenging conventional forensic approac hes.

- **Covert Communications & Anti-forensic Technolo gy-** Expect adoption of encryption, frequency hopp ing, and custom-coded self-wiping mechanisms, necessitating advanced reverse engineering and signal interception tools.

- **Cloud-Connected Ecosystems-** Forensics will exte nd into cloud infrastructure, requiring cross-jurisdic tion cooperation and advanced digital rights mana gement bypass tools.

- **Legal and Regulatory Evolution-** Nations will refin e drone laws, require operators to pre-register fligh t plans (e.g., via platforms like India's Digital Sky), and define evidentiary standards for drone-derived digital evidence.

- **International Standards-** Moves are afoot to draft global frameworks and inter-operable standards for drone forensics, much as with mobile and network forensics.

India's Approach to Drone Forensics: Governmental and Technological Initiatives

India faces acute security risks from drones, given its hostile borders and internal security challenges. The government's response straddles policy, techn ological investment, and institutional innovation.

Legislative and Regulatory Initiatives

- **Central and State Legislative Reform-** Under the Aircraft Act, 1934 and the Drone Rules 2021 , the Central government regulates drone use. There are proposals for amending rules to dec entralize enforcement, letting states police loca l infractions, and requiring operators to pre-register their purposes on platforms like Digital Sky for enhanced transparency and security.

- **Enforcement SOPs-** Drafting uniform standard operating procedures (SOPs) empowers police to promptly respond to drone rule violations and potential attacks.

Forensics and Law Enforcement Integration

- **National Forensic Sciences University (NFSU) Threat Library-** NFSU is building a comprehens ive "digital threat library" to identify UAVs by fr ame, controller, and chips, enabling attributions even when drones are partially destroyed or customized for illegal purposes.

- **Kerala Drone Forensics Lab-** Kerala's Drone Forensic Lab and Research Centre can identify drones, analyze their flight paths, recover delet ed data, and assist in neutralization and count er-UAV operations.

- The repository assists not just in military foren sics but in crime-solving and the protection of VVIPs and critical infrastructure.

- NFSU also trains police, military, and paramilit ary forces in digital and drone forensics.

R&D and Industrial Promotion

- **Drone Shakti and Allied Schemes-** Government schemes like Drone Shakti promote domestic start ups in drone manufacturing, design, and Drone-as-a-Service (DrAAS), with an emphasis on self-relianc e and indigenous innovation.

- **Anti-Drone and Counter-UAS Technologies-** India is investing in indigenous counter-drone systems—capable not only of detection and neutralization, but also forensic follow-up.

Challenges and Limitations

- **Rapid Technological Pace-** Drones' rapid technological advances oft en outstrip law enforcement and forensic capabilities.

- **Jurisdictional Complexities-** Drones cross state and national boundar ies effortlessly, complicating attribution and prosecution.

- **Encryption and Data Security-** Proprietary technology, encrypted co mmunication, and custom firmware can hinder forensic access.

- **Legal Admissibility-** Standards for chain of custody, evidence extrac tion, and privacy protection are being debated and refined.

References

- https://timesofindia.indiatimes.com/city/lucknow/empowering-state-police-to-enforce-drone-regulations-a-legislative-need-in-indias-evolving-space/articleshow/122189423.cms
- https://www.vifindia.org/print/12451?slide=%24slideshow%24
- https://www.dsci.in/files/content/knowledge-centre/2024/Drone_Forensics_Investigation.pdf
- https://www.visionofhumanity.org/how-drones-have-shaped-the-nature-of-conflict/
- https://timesofindia.indiatimes.com/city/ahmedabad/nfsus-digital-threat-library-to-advance-drone-forensics/articleshow/121421019.cms
- https://www.journalofpoliticalscience.com/uploads/archives/6-1-79-436.pdf
- https://vaimanikaaerospace.com/5-government-schemes-supporting-drone-tech-you-should-know/
- https://research.unl.pt/ws/portalfiles/portal/85371059/Sarkin_Drones-on-the-Frontline.pdf
- https://www.medianama.com/2021/08/223-kerala-government-launches-drone-forensic-lab-2/
- https://www.orfonline.org/expert-speak/the-use-of-drones-marks-a-new-phase-in-india-pakistan-hostilities
- https://www.unmannedairspace.info/latest-news-and-information/indias-border-security-force-deploys-skynet-intel-forensic-c-uas-technology-to-counter-drone-smuggling/
- https://www.indiatoday.in/india/story/india-pakistan-drone-attack-operation-sindoor-air-defence-army-2726277-2025-05-17 13. https://vajiramandravi.com/current-affairs/autonomous-warfare-in-operation-sindoor-india-pakistan-drone-conflict/
- https://www.indiatoday.in/india/story/india-pakistan-drone-attack-operation-sindoor-air-defence-army-2726277-2025-05-17 13. https://vajiramandravi.com/current-affairs/autonomous-warfare-in-operation-sindoor-india-pakistan-drone-conflict/
- https://www.pib.gov.in/PressReleasePage.aspx?PRID=2129453
- https://indianexpress.com/article/explained/drone-warfare-came-home-during-op-sindoor-where-does-india-stand-10061470/
- https://timesofindia.indiatimes.com/india/operation-sindoor-over-600-pakistan-drones-killed-by-army-air-defence-units/articleshow/121221694.cms
- https://www.ndtv.com/india-news/our-cities-had-a-mass-raid-of-drones-in-waves-air-force-on-operation-sindoor-8387912
- https://www.moneycontrol.com/news/india/over-600-pakistani-drones-shot-down-by-indian-army-amid-border-tensions-13029865.html
- https://www.pib.gov.in/PressReleasePage.aspx?PRID=2128746
- https://en.wikipedia.org/wiki/2025_India%E2%80%93Pakistan_conflict
- https://timesofindia.indiatimes.com/india/neutralised-pakistani-drones-through-cds-anil-chauhan-shares-new-details-on-operation-sindoor-pitches-for-local-tech/articleshow/122554205.cms

Lt Col (Dr) Santosh Khadsare

Cyber Forensic Expert

About the Author:

Lt Col (Dr) Santosh Khadsare (Retd.) is a distinguished expert in Digital Forensics, Cybersecurity, and Incident Response, with over three decades of combined experience in the Indian Army and the technology sector. A Certified Ethical Hacker (CEH) and ISO 27001 Lead Auditor, he has served as Head of Department (HOD) of Digital Forensics at Rashtriya Raksha University and is a sought-after speaker and mentor in the field. He can be reached via LinkedIn at linkedin.com/in/santosh-khadsare-3539a818, by email at santoshkhadsare@gmail.com, or on Twitter as @4N6_Farmer.

Conclusion

Drone forensics sits at the confluence of aviation, cybersecurity, criminal justice, and data science. As drone technology permeates new sectors and conflict theaters, states like India are recognizing the urgency of robust forensic infrastructure—supported by specialized laws, advanced laboratories, and an ecosystem of public and private stakeholders.

Moving forward, the success of drone forensics will rest on international cooperation, continuous upskilling, open-source tool development, and adaptive regulation. Nations that invest in these capabilities, integrate law enforcement with cutting-edge research, and balance security with civil liberties will be best placed to meet the challenges of the drone age.

ADMISSIBILITY OF DRONE-CAPTURED EVIDENCE

An Examination of Privacy Concerns and Regulatory Frameworks

Drones or unmanned aerial vehicles (UAVs), hav e become an accepted part of journalism, polic ing, disaster relief and commercial work. Their capacity to record high-definition images and video has made them useful tools for evidence gathering. But the admissibility of evidence obtained using drones, its effect on privacy and the sufficiency of present regulato ry regimes are still issues unresolved in most juris dictions. This article analyses the legal requirements for the admissibility of drone footage in court based on important factors like authenticity, chain of custody and adherence to governing laws. The article further analyses privacy concerns related to intrusion into private areas, adherence to data protection laws and the social implications of pervasive drone surveillance. The regulatory environment is discussed across various jurisdictions like India, the United States, the European Union and China. The article concludes by proposing an equilibrium balance of legal clarity, technical protection and public awareness to make drones a robust yet ethical means of evidence collection.

In the last decade, drones have evolved from speci alized equipment for hobbyists and military person nel to the mainstream platforms used by commer cial, governmental and humanitarian organizations. Armed with sophisticated cameras and sensors, the y are increasingly utilised by law enforcement, sear ch-and-rescue teams and investigative journalists. Their capacity for capturing distinctive overhead vie ws provides serious evidentiary value during litigati on. Nevertheless, their increasing adoption provo kes serious legal and policy concerns: How can the evidence captured by drones be admitted at trial while preserving privacy rights? What laws ensure public safety and innovation? This paper delves into these matters by examining admissibility norms, privacy issues, and regulatory structures.

Admissibility of Drone-Captured Evidence

Harshita Sonkar

Master's Student in Cyber Law and Information Security, NLIU Bhopal

LEGAL STANDARDS FOR ADMISSIBILITY

Courts need evidence to be authentic, pertinent and legally collected. For aerial imagery using drones, authenticity may be proven by metadata such as timestamps, GPS readings and operator data along with forensic verification. A sound chain of custody from the capture time right through to the court presentation is required to avoid suspicions of tampering.

JUDICIAL DISCRETION AND CASE LAW

Lower courts in the United States have extended Fourth Amendment doctrines to drone surveillance, at times mandating warrants where there is an expectation of privacy. No precedent-setting drone cases have gotten as high as Indian higher courts but under Justice K.S. Puttaswamy vs. Union of India (2017), the constitutional privacy right would guide admissibility judgments. Judicial discretion is crucial in both nations, with judges balancing evidence value against invasions of rights.

Privacy Concerns

INTRUSION INTO PRIVATE SPACES

Unmanned aircraft vehicles have the ability to take high-resolution images from significant distances, posing risks of unauthorized surveillance. These intr usions can potentially breach individuals' reasona ble expectation of privacy, especially in residential or sensitive contexts.

DATA PROTECTION COMPLIANCE

Drone shots that identify individuals fall under the definition of personal data under the EU's General Data Protection Regulation (GDPR), which needs a valid basis to process it. India's Digital Personal Data Protection Act (DPDP Act) also places similar requirements on compliance, including minimisation

of data, secure storage and restricted access. Recurring drone monitoring could have a chilling effect on free expression and public assembly. This privacy concern with a psychological aspect is attracting more interest from civil liberties groups.

Regulatory Frameworks Across Jurisdictions

- **India-** The Directorate General of Civil Aviation (DGCA) regulates drones pursuant to the Drone Rules, 2021, requiring registration, operation permission and "No Permission, No Takeoff" (NPNT) adherence. Shooting pictures without permission might attract provisions of the Information Technology Act, 2000 and the DPDP Act.

- **United States-** The Federal Aviation Administration (FAA) oversees drone safety under Part 107 regulations, with privacy regulation being left mostly up to the individual states. A number of states have enacted legislation mandating warrants for law enforcement drone surveillance.

- **European Union-** The European Union Aviation Safety Agency (EASA) oversees regulation of drones, with GDPR compliance required when personal information is exchanged. Some member states have more stringent regulations in place for flights over residential neighbourhoods.

- **China-** China requires drone registration and geofencing in restricted airspace in accordance with the Civil Aviation Administration regulations. Data privacy is regulated by the Personal Information Protection Law (PIPL), which has severe penalties for violation.

Balancing Innovation, Privacy, and Enforcement

For drones to remain an ethical and legal means of gathering evidence, policymakers must prioritize three pillars:

- **Clear Legal Criteria:** Specific admissibility requirements, warrant proc edures and privacy protections.
- **Technical Integrity Measures:** Encryption, tamper-proof metadata and watermarking to uphold evidentiary reliability.
- **Public Awareness:** Open practices and consent-based data collection to foster trust in drone activity.

References:

Al-Dhaqm, A., et al. (2022). A comprehensive collection and analysis model for the drone forensics field (CCAFM). *ResearchGate*.https://www.researchgate.net/publication/363098113

Alotaibi, F. M., et al. (2022). Drone forensics readiness framework (DRFRF). *PubMed Central*.https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8901304/

Baig, Z., et al. (2022). Drone forensics and machine learning: Sustaining the investigation process. ResearchGate. https://www.researchgate.net/publication/360072198

Adel, A. (2024). Watch the skies: A study on drone attack vectors. MDPI. https://www.mdpi.com/1999-5903/16/7/250

Taylor, A. (2023). Forensics case study of DJI Mini 3 Pro. arXiv. https://arxiv.org/abs/2309.10487

Directorate General of Civil Aviation. (2021). Drone Rules, 2021. DGCA. https://dgca.gov.in

Ministry of Civil Aviation. (2021). Digital Sky Platform. https://digitalsky.dgca.gov.in

Indian Computer Emergency Response Team. (2023). Advisory on secure UAV operations. CERT-In. https://www.cert-in.org.in

Harshita Sonkar

Master's Student in Cyber Law and Information Security, NLIU Bhopal

About the Author:

Harshita holds a Bachelor of Commerce (B.Com.) in Applied Economics from Barkatullah University, Bhopal. She is currently pursuing a Master's in Cyber Law and Information Security (2024–2026) at the National Law Institute University, Bhopal. Her academic path combines economics, law, and cybersecurity, reflecting a multidisciplinary approach to emerging challenges in the digital era.

Conclusion

Evidence captured by drones is a potential game-changer in contemporary legal systems, but its worth hinges on lawful acquisition, protection of privacy and regulatory compliance. Balancing these factors across jurisdictions will be the key to realising the capabilities of drones without compromising essential rights. Global best practices from GDPR-compliant privacy standards to community engagement models show that good governance is possible. As technology evolves, how legal protection and ethical principles are blended will decide whether drones become an asset of trust or a cause of public anxiety.

FORENSIC CHALLENGES IN DIY AND MODIFIED DRONES

Rahul Sahi

Cybersecurity and Web Development Professional with Expertise in ISO 27001 & NIST CSF

Abstract- The do-it-yourself (DIY) and modified drone phenomenon is an emerging industry in the context of unmanned aerial vehicle (UAV) operations, ranging from innovative recreational use to criminality. In contrast to standard commercial drones, with standardized hardware, firmware, and data architecture, DIY and modified UAVs pose distinctive forensic challenges through their non-standard hardware, customized firmware, encrypted data storage methods, and concealed flight logs. This study discusses the difficulties faced by investigators conducting forensic examination of such drones, such as hardware disassembly challenges, proprietary or unfamiliar communication protocols, volatile memory persistence, and anti-forensic techniques employed by offenders. The study also discusses legal and policy barriers, specifically the admissibility of non-standard forensic evidence in court, while emphasizing the institutional readiness gaps among law enforcement agencies and national security institutions. Recommendations are directed at the improvement of technical capabilities through the exploitation of open-source intelligence (OSINT), facilitation of international forensic exchange, and the development of adaptive forensic frameworks able to cope with the diversity in DIY and modified drones. By bridging these observed gaps, forensic specialists can improve the response to the evolving threat horizon while maintaining the integrity of evidence in legal proceedings.

Overview

Drone technology has developed rapidly from hobbyis t tinkering to sophisticated uses in security, agriculture, delivery, and surveillance markets. The advent of do-it-yourself (DIY) and hacked drones, however, presents forensic issues much larger than those of traditional consumer unmanned aerial vehicles (UAVs) manufactu red by firms like DJI or Parrot. Unlike commercially ma -nufactured drones, which come equipped with onboa -rd telemetry logging, standardized firmware, and simp le-to-use diagnostic interfaces, DIY drones tend to wor k with custom hardware and software setups, which re duce the effectiveness of traditional forensic tools. In national security contexts, modified drones have been employed for cross-border smuggling, contraband deli very into prisons, spying, and even explosive payload delivery. In criminal investigations, their versatility mak es them even more deadly: GPS modules can be remo -ved, serial numbers erased, and communication encry -pted. This paper discusses the forensic issues associa ted with such drones and offers directions for enhanci -ng investigative capabilities.

Types of DIY and Modified Drones

DIY drones are usually made up of purchased commer -cial parts, open-source flight controllers (such as Ardu -Pilot, Betaflight), and modular components. Altered dr -ones, on the other hand, are commercial UAVs that ar -e modified to circumvent manufacturer limitations, incr -ease range, or add payload capabilities. This customiz -ation renders forensic analysis difficult as known archi tectures are what forensic suites are founded on. Recu rring variations are:

- Firmware upgrade to eliminate no-fly zone (NFZ) restriction.
- Radio frequency (RF) module settings for longer control range.
- Payload modifications for smuggling contraband.
- Sensor upgrades for sophisticated reconnaissance or clandestine operations.

Forensic Challenges

- **Hardware Heterogeneity-** DIY drones incorpora te microcontrollers, storage modules, and telem etry systems from various suppliers. It is possible for investigators to find unknown hardware with no documentation, and identification of the com ponents is difficult. Without a reference design, disassembly risks erasing volatile memory comp -onents containing valuable evidence.

- **Data Retrieval and Volatile Memory-** Commerci al drones typically cache flight logs in onboard non-volatile memory or in synchronized mobile devices. DIY drones cache logs on removable mi croSD cards, or solely in volatile RAM on flight controllers. When powered off, volatile data can be deleted. Without prompt forensic imaging, vit al navigation data may be lost.

- **Proprietary or Uncommon Protocols-** Altered dr ones can employ proprietary telemetry protocols or encryption, which are more difficult to interce pt and decrypt. Examiners can need protocol an alysis equipment and occasionally hardware logi c analysers to emulate communication protocols between controller and drone.

- **Anti-forensic Techniques-** Criminals can install self-destruct firmware, which will erase memory in case of capture, or encrypt logs with unguess able passphrases. GPS modules can be disabled in certain circumstances to prevent geolocation data, leaving behind only inertial measurement data, which is harder to interpret.

- **Chain of Custody and Admissibility-** The absen ce of standardized tools for extraction would hin der the admissibility of ad-hoc forensic techniqu es in court. The integrity of evidence is lost whe n procedures change from one case to another, particularly in jurisdictions that demand verifiabl e and reproducible forensic techniques.

Institutional and Policy Gaps

Existing forensic training courses for drone examinations are typically focused on mass-market commercial devices, leaving a vast skills gap for DIY and highly modified drones. Such bespoke platforms tend to be linked with hardware-level reverse engineering and advanced firmware analysis skills that are not yet common in most police technical units. The lack of specialist training has investigators struggling to even start the acquisition process, especially when encountering bespoke circuitry or non-standard storage arrangements.

The cross-border nature of most incidents related to drones, especially in smuggling or intelligence gathering cases, enhances this problem. Most of these operations cut across multiple jurisdictions, and different legal standards for the handling of evidence impede interagency cooperation. In some cases, critical telemetry information or equipment seized in one country may be rendered inadmissible in another because of incompatible forensic techniques or lack of mutual legal recognition. This problem is compounded by the fact that most countries lack well-defined policies on accepting evidence gathered using non-certified or improvised forensic equipment. Therefore, even if investigators successfully manage to extract vital information from a homemade drone, they end up wondering whether it will be admissible in court.

Technical Recommendations

CREATION OF UNIVERSAL DRONE FORENSIC FRAMEWORKS

A modular forensic examination with every module such as flight controller, RF module, storage with flexible extraction workflows.

MESHING OSINT WITH DRONE FORENSICS

Hobby websites, GitHub repositories, and social media can reveal firmware versions or build techniques, which can help in forensic reconstruction.

BUYING PROTOCOL ANALYSIS TOOLS

Purchasing hardware sniffers and signal analyzing software that can decode unknown communication protocols.

References:

Almusayli, A., Zia, T., & Qazi, E.-u.-H. (2024). Drone forensics: An innovative approach to the forensic investigation of drone accidents based on digital twin technology. *Technologies, 12*(1), 11. https://doi.org/10.3390/technologies12010011

Sabri, N. E. M., Singh, M. K. C., Mahmood, M. S., Khoo, L. S., Yusof, M. Y. P. M., Heo, C. C., Nasir, M. D. M., & Nawawi, H. (2023). A scoping review on drone technology applications in forensic science. *SN Applied Sciences, 5*(9). https://doi.org/10.1007/s42452-023-05450-4

Mantas, E., & Patsakis, C. (2022). Who watches the new watchmen? The challenges for drone digital forensics investigations. *Array, 14*, 100135. https://doi.org/10.1016/j.array.2022.100135

Klier, S., & Baier, H. (2025). Beware of the rabbit hole – A digital forensic case study of DIY drones. In *Lecture Notes in Computer Science* (pp. 325–344). https://doi.org/10.1007/978-3-031-79007-2_17

Baig, Z., Khan, M. A., Mohammad, N., & Brahim, G. B. (2022). Drone forensics and machine learning: Sustaining the investigation process. *Sustainability, 14*(8), 4861. https://doi.org/10.3390/su14084861

Rahul Sahi,,

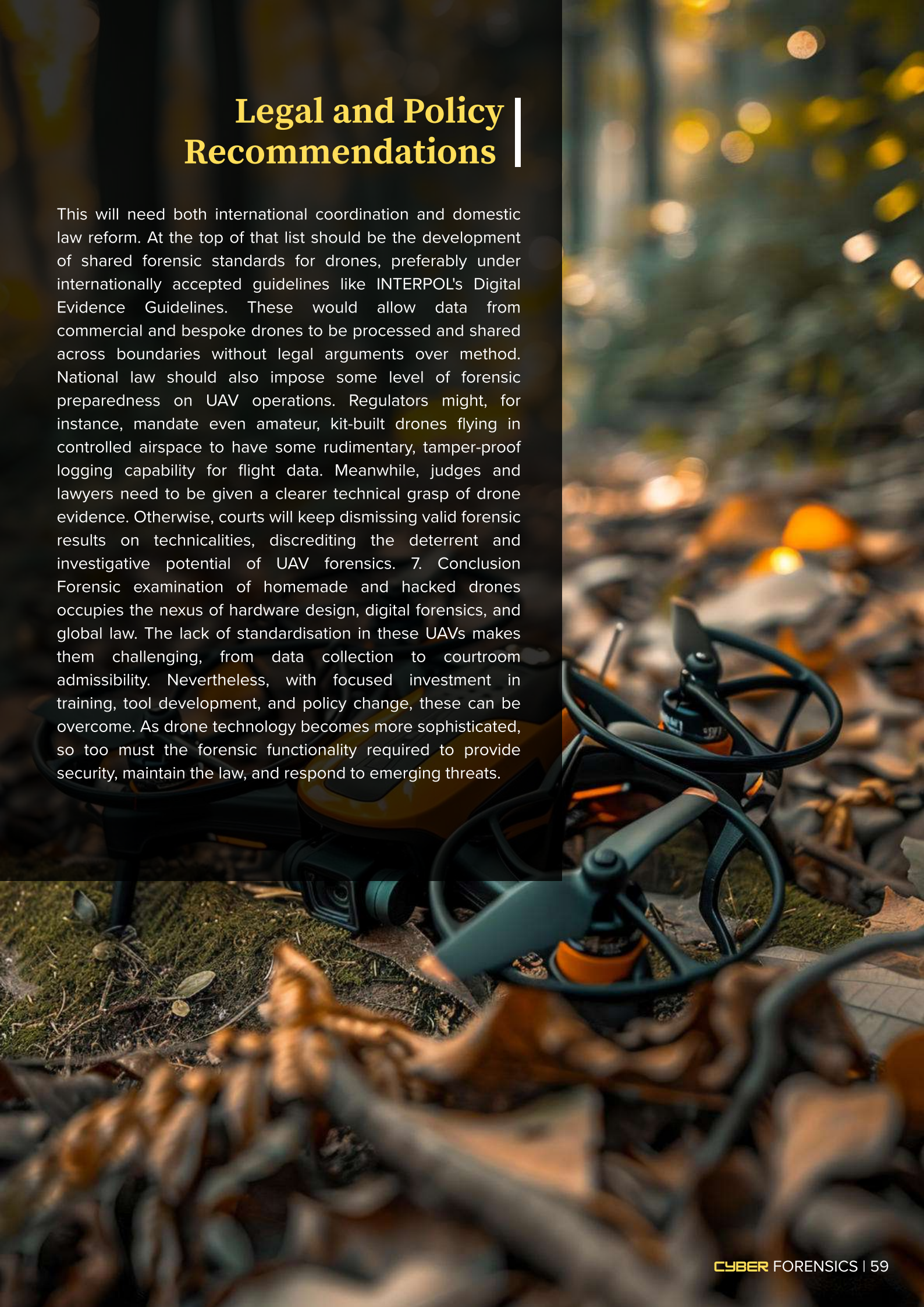
Cybersecurity and Web Development Professional with Expertise in ISO 27001 & NIST CSF

About the Author:

Rahul Sahi is a cybersecurity and web development professional with expertise in ISO 27001, NIST CSF, compliance audits, and full-stack development. He brings a blend of technical and regulatory knowledge to his work, bridging secure practices with innovative digital solutions. Connect with him on LinkedIn or reach him at **sahirahul07@gmail.com**

Legal and Policy Recommendations

This will need both international coordination and domestic law reform. At the top of that list should be the development of shared forensic standards for drones, preferably under internationally accepted guidelines like INTERPOL's Digital Evidence Guidelines. These would allow data from commercial and bespoke drones to be processed and shared across boundaries without legal arguments over method. National law should also impose some level of forensic preparedness on UAV operations. Regulators might, for instance, mandate even amateur, kit-built drones flying in controlled airspace to have some rudimentary, tamper-proof logging capability for flight data. Meanwhile, judges and lawyers need to be given a clearer technical grasp of drone evidence. Otherwise, courts will keep dismissing valid forensic results on technicalities, discrediting the deterrent and investigative potential of UAV forensics. 7. Conclusion Forensic examination of homemade and hacked drones occupies the nexus of hardware design, digital forensics, and global law. The lack of standardisation in these UAVs makes them challenging, from data collection to courtroom admissibility. Nevertheless, with focused investment in training, tool development, and policy change, these can be overcome. As drone technology becomes more sophisticated, so too must the forensic functionality required to provide security, maintain the law, and respond to emerging threats.



Empowering Digital Guardians CyberPeace Corps

CyberPeace Corps (CPC) is a global initiative that unites individuals, cybersecurity professionals, and tech enthusiasts on a mission to fortify our digital defenses. With the ethos of peace, protection, and prosperity, they actively engage in activities that promote cybersecurity awareness. The volunteers come from diverse backgrounds professions and demographics. What unites them is their unwavering dedication to this noble cause and making a meaningful impact in society by.

How to join CPC?

Join as Volunteers by registering at https://cyberpeace.global and grow as an Ambassador through different Levels of Certifications. Our unique point-based system tracks volunteer activities, enabling them to progress through different levels and earn stars with distinctive titles from Cadet, Sentinel, Defender, Champion Ambassador.

TOGETHER, LET'S BUILD A SAFER, MORE SECURE AND RESILIENT CYBERSPACE

Be a **Volunteer**, Be a **First Responder**

Join the CyberPeace Volunteers

Be the frontline defense against cyber threats

CyberPeace Helpline
+919570000066
www.cyberpeace.global

SCAN the QR code or follow the link to visit

EXPERT INTERVIEW:

Drone Policy and the Case for Military-Civil Technology Fusion in India

Unmanned aerial systems are rapidly transforming both civil and military domains all across the globe. From surveillance and logistics to counter counter-drone defense, drones are at the heart of modern warfare and national security. Yet, India's drone ecosystem faces persistent challenges around indigenisation, testing infrastructure, certification, and integration between civilian and defense stakeholders. To understand these issues, *Cyber4N6* spoke with Gp Capt Rajiv Kumar Narang (Retd), Senior Fellow at the Manohar Parrikar Institute for Defence Studies and Analyses. A noted expert on drone policy and the author of a monograph, *The Necessity of Military – Civil Fusion (MCF) for Making India a Global Drone Hub@2030*, Gp Capt Narang shares his insights on lessons from recent operations, the future of indigenous drone development, and the reforms required to position India as a global drone hub by 2030.

Q 1: Welcome, sir, and thank you for being here today. To begin, what are some lessons India has learned from the use of drone technology during Operation Sindoor?

A: The first lesson is the critical role of indigenous technologies. Both our drones and counter-drone systems were pivotal to the success of India's operations. While drones created havoc in many conflicts globally, India successfully used them for armed strikes, surveillance, and neutralizing adversaries' systems.

Several indigenous technologies developed by Indian industry were validated in real operations, which not only strengthens our defense capability but also builds export potential—because proven products are always valued.

That said, there are areas requiring attention:

- **Unmanned Traffic Management (UTM):** We need a civil UTM system to differentiate between friendly and adversary drones, even in peacetime.
- **Integration:** Better coordination between the Army, Navy, Air Force, and also with paramilitary forces like the BSF is essential.
- **Upgradation:** Critical components must be indigenized to avoid vulnerabilities. In counter-drone technologies, indigenous versions of anti-aircraft systems like L70s, Zu-23s, and Shilkas must be developed with AI integration. Future systems must also rely on smart and specialized munitions to deal with drone swarms.

Q 2: For our readers, could you explain how counter-drone systems work?

A: Broadly, counter-drone systems work in three steps:

- **Detection:** Using radar, radio-frequency detectors, electro-optical, or infrared sensors.
- **Identification & Tracking:** Distinguishing friendly drones from hostile ones and following their trajectory.
- **Neutralization:** This can be *soft kill* (jamming) or *hard kill* (destroying with guns, lasers, or high-power microwaves).

India has made progress. DRDO and IDEX innovators have developed indigenous counter-drone systems, and DRDO's "D4" system has been transferred to six companies. But more work is needed, particularly in radar, detection, networking, and swarm-drone countermeasures.

Q3: Stepping back, what does the drone ecosystem in India look like today?

A: I see five verticals in the ecosystem:

- **Research & Development (R&D):** Defense and civil R&D are complementary but uneven. Civil aviation must strengthen its R&D ecosystem to validate technologies like UTM and remote tracking.
- **Testing Infrastructure:** Defense testing sites are emerging, but civil testing sites are limited. We need dedicated corridors and facilities for advanced applications like urban air mobility.
- **Standards:** India lags behind global best practices in trial-based standards (common in the US, EU, and China). Standards must cover not just drones but also components.
- **Standardization:** Minimum interoperability standards are needed so drones can function on common frequencies and protocols.
- **Certification:** Both military and civil certification mechanisms must include *component-level certification* to ensure reliability and security.

Q 4: How can we differentiate between drones with indigenous components and those with imported ones, especially during procurement?

A: Traditionally, indigenous content was measured by cost share, which was ambiguous. Now, the Ministry of Defence has moved to a components, software, and materials approach. But we still lack:

- A technical body to set standards.
- A certification mechanism for indigenous content.
- Component-level certification for both civil and military use.
- Without these, imported sub-systems can easily slip into "assembled in India" drones, which poses security risks.

Q 5 : What are the major challenges faced by India's civil drone sector?

A: There are several:

- **Core Technologies:** Few companies are working on critical components like communication systems, data links, and storage. Many rely on imported sub-systems.
- **Procurement Policies:** Tenders and requirements (QRS) do not always prioritize indigenous

- **Market Pressures:** Global players can undercut Indian firms by flooding the market with cheaper products, even if only temporarily.

To strengthen the sector, government support is needed in the form of:

- Positive indigenization lists for civil drones.
- Dedicated "indigenous product" tags on procurement platforms like GeM.
- Affordable testing, certification, and handholding for smaller firms.

Q 6: You've argued for a formal Military-Civil Technology Fusion (MCTF) policy. What would such a framework look like?

A: Globally, both the US and China have benefited immensely from integr ating civil and military technology ecosystems. India needs a similar approach. This approach is essential if India wants to become a global drone hub by 2030.

A functional framework would include:

- **Joint R&D and Trials:** Civil aviation authorities, defense forces, and in dustry working together.
- **Shared Testing Infrastructure:** Facilities used collaboratively by civil and military players.
- **Real-Time Monitoring:** Integrated airspace management across civil, defense, and paramilitary operators.
- **Policy Synergy:** Guidelines co-created with industry, instead of waitin g for international models.

Q 7: With AI playing a bigger role in drone operations, how should India approach the ethical dimension?

A: India has consistently emphasized keeping a human in the loop. For ex ample, the Air Force refers to drones as "Remotely Piloted Aircraft" (RPA) to underline human oversight.

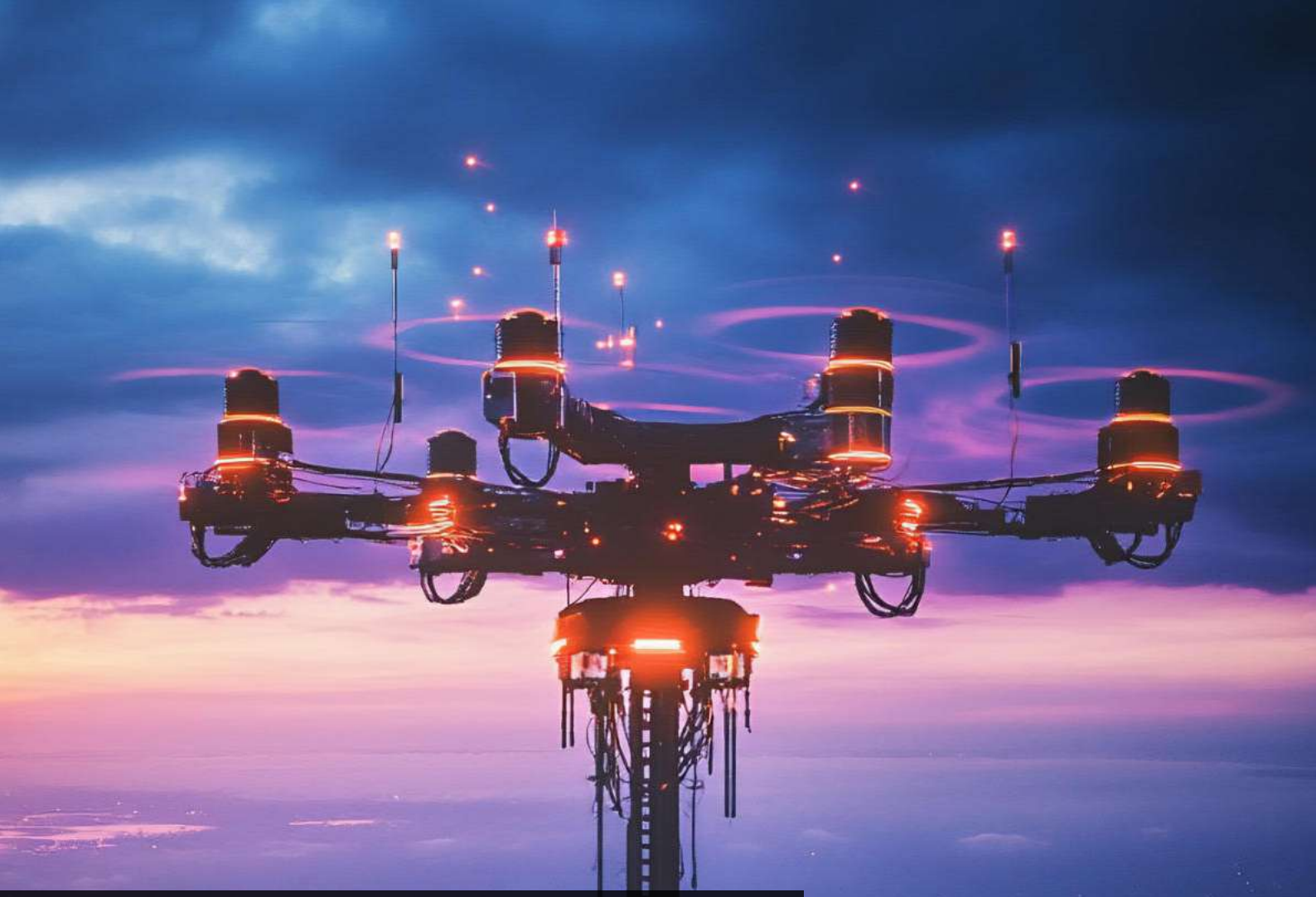
That said, AI is crucial for managing swarm attacks and coordinating multi ple counter-drone systems. The right balance is AI-assisted operations wit h human override authority, ensuring effectiveness without compromising accountability.

Gp Capt Rajiv Kumar Narang (Retd)

Senior Fellow Manohar Parrikar Institute of Defence Studies and Analyses

About

Group Captain (Dr.) Rajiv Kumar Narang, Vayu Sena Medal (Retd.), is Senior Fellow at MP-IDSA and a former Indian Air Force helicopter pilot. A qualified Flight Safety and Accident Investigator with a PhD in International Relations, he has authored *India's Quest for UAVs and Challenges* and numerous papers on drones, aviation, and self-reliance. He previously served at the Centre for Air Power Studies, the Drone Federation of India, and high-level committees under DPIIT and iDEX. He also authored the 2022 HQ IDS–SIDM report *A Roadmap for India Becoming Atmanirbhar in Counter-Drone Technologies/Systems*. He can be reached at https://in.linkedin.com/in/rk-narang



Q 8: To conclude, what reforms are needed in India's drone ecosystem?

A:

- **Civil Sector:** Create an R&D vertical within the Ministry of Civil Aviation, operationalize *Digital Sky*, enable manned-unmanned collaborative flying, and institute component-level certification.

- **Defense Sector:** Approve and operationalize projects like the *Ghatak* UCAV, *Archer-NG*, and short-range UAVs. Esta blish minimum standards for drones and counter-drone systems.

- **Cross-Sector:** Launch a Military-Civil Technology Fusion policy to ensure synergy.

If these steps are taken, India can not only secure its borders but also emerge as a leading global drone hub.

Volume 10 | Issue 3 | September 2025

CyberPeace

CYBER FORENSICS (4N6)

DRONE SECURITY