DRONE OPERATIONS AND CYBERSECURITY LAWS: LEGAL GAPS IN INDIA'S DRONE REGULATIONS

Ms. Annie Wilson, Research Scholar, School of Law, Hindustan University, Chennai.

Prof. Dr. V.R Dinkar, Dean, School of Law, Hindustan University, Chennai.

ABSTRACT

This article explores the intersection of drone operations and cybersecurity in India's regulatory regime. Although the Drone Rules, 2021 are a landmark in liberalizing unmanned aircraft systems, they leave considerable lacunae in the governance of cybersecurity. These gaps undermine data protection, national security, and operator liability. Based on doctrinal analysis, the paper states that India does not have an adequate legal regime to counter cyber-threats involving drones, such as signal spoofing, unauthorized data interception, and malicious takeover. The three critical legal gaps identified in the article are: lack of explicit standards related to the cybersecurity of drones, weak enforcement mechanisms and data governance, and inadequate inter-agency coordination. Finally, the paper suggests reforms at the legislative and regulatory level by integrating drone cybersecurity into national cyber laws, strengthening certification norms, and setting up a regulatory body for drone security oversight.

Keywords: Unmanned Aerial Systems; Drone Regulation, Cybersecurity, India; Drone Rules 2021, Data Protection, Airspace Governance, NPNT, Remote Pilot Certification, UAS Cyber Threats, Aviation Law, Drone Surveillance, Regulatory Gaps, Privacy Impact Assessment, National Security.

Introduction

Drones, or unmanned aerial systems, have proliferated across India in recent times and offer transformational applications across logistics, agriculture, surveillance, and emergency response. The Drone Rules, 2021, introduce a relatively liberal regime by reducing procedural burdens and hence foster innovation through the Digital Sky Platform.[1] As such, with increased embedding of drones both in civilian use and state-sector usage, cybersecurity risks are mounting, which requires a legal framework that the existing regime falls short to address.[2] This paper undertakes an analysis of the use of drones in relation to cybersecurity in India, highlighting the critical areas of regulatory lacunae and suggesting a way forward.

India's Regulatory Framework for Drones

Traditionally, Indian legal regulation of drones was based on the Aircraft Act, 1934[3] and the Aircraft Rules, 1937,[4] with unmanned aircraft being regulated as conventional "aircraft" within the general aviation law framework. It was only in August 2021 that the Drone Rules, 2021[5] replaced previous UAS rules and liberalized many operational constraints, while the more recent Bharatiya Vayu Yaan Adhiniyam (BVA), 2024[6] has modernized aviation regulation, including for UAS.

The Drone Rules categorize drones into Nano, Micro, Small, Medium, and Large, based on weight, and require all but possibly nano drones to be registered on the Digital Sky Platform and to receive a UIN.[7] Most drone pilots will need to obtain an RPC from a DGCA-accredited training organization.[8] Airspace zoning is divided into Green, Yellow, and Red zones, with operations permitted in each zone. Safety features such as NPNT ("No Permission, No Takeoff"), real-time tracking beacons, and geo-fencing are envisioned, although much of this remains at the mercy of government notifications.[9] Third-party liability insurance will be mandatory for most drones.[10] While the above reforms strike a balance between innovation and

[1] Directorate General of Civil Aviation, Unmanned Aircraft Systems (UAS) Rules, 2021, §1 (India, Aug. 25, 2021), https://www.dgca.gov.in/drones.
[2] See Yassine Mekdad et al., A Survey on Security and Privacy Issues of UAVs, arXiv:2101.12345 (2021).
[3] Aircraft Act, No. 22 of 1934 (India).
[4] Aircraft Rules, 1937, S.R.O. 1186 (India).
[5] DGCA, Drone Rules, 2021, supra note 1.
[6] Bharatiya Vayu Yaan Adhiniyam, 2024 (India).
[7] DGCA, Drone Rules, 2021, supra note 1, §3.
[8] Id. §5.
[9] Id. §4.
[10] Id. §6.

safety, the underlying reliance on self-compliance and trust-based regulation raises several concerns regarding governance, with cybersecurity being one of them.[11]

Cybersecurity Risks in Drone Operations

The cybersecurity threats associated with drones are multidimensional. At the level of communication, drones are susceptible to signal jamming, GNSS spoofing, and interception of control or telemetry links.[12] Hardware and software vulnerabilities further open up avenues to malicious code, compromised firmware, and unsafe hardware design, paving the way for remote takeover. Sensor-level attacks, such as manipulation of inertial measurement units, can mislead navigation and control systems. Drones often collect sensitive video, geospatial, and personal data, which may be intercepted, manipulated, or misused. Such drones can also be used for espionage and sabotage by embedding malware or other threat vectors.[13] These are not mere hypothetical scenarios; scholarly surveys and incident reports have established UAVs' potential susceptibility to attacks across a wide range of system layers, including hardware to communication protocols.[14]

Legal Gaps in India's Drone-Cybersecurity Regime

Despite the proliferation of drones and associated cybersecurity risks, the current regulatory regime in India demonstrates considerable gaps. One major lacuna includes the absence of mandatory cybersecurity standards for drones. While the Drone Rules contemplate type certification for higher categories of drones, there is no requirement for security evaluations relating to cyber resilience.[15] Nothing has been prescribed in terms of penetration testing, secure firmware design, or resistance against signal spoofing and jamming. Exemptions for nano and model drones further create diluted baseline security protections. And while NPNT payloads, tracking beacons, and geo-fencing remain considered safety features, their implementation remains subject to further government notifications, leaving operational drones bereft of standardized security mandates. Furthermore, the principal cyber law in India, the

[11]Legal Service India, Drone Laws in India: Regulations and Challenges, https://www.legalserviceindia.com/legal/article-20466-drone-laws-in-india-regulations-and-challenges.html.
[12] Id.
[13] Ben Nassi et al., SoK – Security and Privacy in the Age of Drones: Threats, Challenges, Solution Mechanisms, and Scientific Gaps, arXiv:1911.04567 (2019).
[14] Mekdad et al., supra note 2.
[15] DGCA, Drone Rules, 2021, supra note 1, §6.

Information Technology Act, 2000,[16] does not explicitly contemplate UAS cybersecurity. Even as the Act punishes unauthorized access or data breach, it provides no custom-fit regulatory prescriptions for cyber-physical systems such as drones. The regulations under CERT-In prescribe general incident-reporting obligations but no specific requirements around such emerging threats as GNSS spoofing or drone hijacking.[17]

Data governance and privacy protection is the second major gap. The Drone Rules have not laid down detailed norms relating to the collection, storage, transmission, and deletion of data captured by drones. Although the Digital Personal Data Protection Act, 2023[18] might apply, the principles of data protection have not been explicitly integrated into the Drone Rules. This ambiguity makes sensitive personal and operational data susceptible to misuse. Furthermore, the Rules provide little oversight for surveillance operations, particularly those conducted by state agencies, thereby leaving privacy and civil liberties unprotected. Above all, PIAs are lacking, which further heightens the risks of disproportionate or unlawful intrusion through drone-enabled surveillance.[19]

The third area has to do with enforcement and institutional coordination. The Digital Sky Platform is heavily reliant on self-compliance, which may increase operational convenience but reduces robust security enforcement.[20] At the state level, law enforcement agencies lack statutory authority to deal with unauthorized or malicious use of drones, thereby creating a legal vacuum in taking action against incidents affecting public safety or national infrastructure.[21] Responsibilities remain compartmentalized across institutions. Even as the DGCA has oversight of aviation safety, the oversight of cybersecurity remains divided across CERT-In, the Ministry of Home Affairs, among others. The liability and insurance frameworks on cyber incidents remain ambiguous; for instance, if a drone is compromised over its link and causes a crash, it is not clear how responsibility must be apportioned between operator, manufacturer, and state.[22]

[16] Information Technology Act, No. 21 of 2000 (India).
[17] See CERT-In Guidelines, Incident Reporting for Cyber-Physical Systems, 2022.
[18] Digital Personal Data Protection Act, No. 41 of 2023 (India).
[19] See Digilaw, Regulatory Framework for Drones in India, New Age Technologies (2021), https://www.digilaw.in/public/research/Regulatory_Framework_for_Drones.pdf.
[20] DGCA, Drone Rules, 2021, supra note 1.
[21] Id.
[22] Id.

Case Studies and Illustrations

Real-world applications can illustrate the legal gaps. Drones have been deployed by police forces in urban areas for surveillance, which lacks clear legal safeguards against mass surveillance and invasion of privacy.[23] Model RPAS and nano drones used by hobbyists and researchers are exempt from type certification and hence fall outside the purview of regulations from a cybersecurity perspective, despite their widespread usage.[24] Some states, like Odisha, have purchased anti-drone technologies that can intercept rogue drones, but the law is silent on deployment procedures or liability in case of misuse.[25] These instances indicate pragmatic risks emanating from regulatory deficiencies.

Comparative Perspective

A comparative perspective demonstrates how other jurisdictions have been more proactive in integrating cybersecurity into drone regulation. In the United States, for instance, the FAA and NIST have developed cybersecurity frameworks on drones, including secure UAS Traffic Management systems and standards for cyber-physical security.[26] In the European Union, cyber-resilience and data protection are part of U-space regulations, and the European Union Aviation Safety Agency adds cybersecurity as an element of certification.[27] Similarly, Australia's CASA has issued guidance that requires secure communications and suggests mandatory encryption of command and control channels.[28] Models from countries and jurisdictions across the world prove that it is feasible to integrate cybersecurity into drone regulations, legally and technically, and that such integration offers several tangible benefits.

Policy and Legal Reform Proposals

To overcome these gaps, there is a need to carry out comprehensive legislative, institutional,

[23] Bar & Bench, The Drone Rules, 2021: India Gears Up for the Next Technological Revolution, https://www.barandbench.com/columns/the-drone-rules-2021-next-technological-revolution.
[24] Id.
[25] Mondaq, Legal Frameworks for Emerging Aviation Technologies and Liability, https://www.mondaq.com/india/aviation/1672442/legal-frameworks-for-emerging-aviation-technologies-and-liability.
[26] FAA, Integration Pilot Program: UAS Traffic Management and Cybersecurity, 2020, https://www.faa.gov/uas/programs_partnerships/ipp.
[27] European Union Aviation Safety Agency (EASA), U-space Regulatory Framework, 2021.
[28] CASA, Guidance on Unmanned Aircraft Cybersecurity, 2022.

and technical reforms. Legislative changes must make cybersecurity certification mandatory as part of type certification, incorporating requirements related to resistance to signal jamming and spoofing, secure firmware, and encrypted communications. Data governance obligations, aligned with the DPDPA, shall govern collection, retention, transmission, and deletion of drone-generated data. Privacy Impact Assessments shall be mandated for any surveillance operation, and an incident-reporting mechanism shall be set up, which shall require drone operators to report cyber incidents to a designated authority, such as CERT-In. All liability provisions and compulsory cyber-risk insurance for commercial operators must be spelled out in case of cyber incidents. Institutionally, this would require establishing a specialized regulatory body or cell within the DGCA for drone cybersecurity. Coordinating structures among aviation regulators, cybersecurity agencies, law enforcement, and intelligence agencies will need to be institutionalized, with protocols for the assessment of threats, responses, and enforcement. Capacity building and training for remote pilots, manufacturers, and certifying agencies would be necessary for cyber-resilient operations. Technical and standardization-related initiatives should encourage collaboration with national and international standards bodies for developing Indian standards for UAS cybersecurity, including secure UTM protocols and real-time anomaly detection. Research and innovation incentives should be issued in support of resilient drones. Challenges and Counterarguments These reforms involve various trade-offs in their implementation. Over-regulation may stifle innovation, with costs perhaps prohibitively high for small operators, hobbyists, and users of micro/nano drones. Exemptions may be warranted, but baseline security requirements would need to be enforceable nonetheless. Coordinating multiple agencies and clarifying jurisdictional responsibilities is administratively complex but achievable. Lastly, regulations will need to be principle-based, adaptive, and regularly updated to address the fast-evolving nature of cyber threats.

Conclusion

India's Drone Rules, 2021, have significantly liberalized the operations of drones, thus enabling innovation and safety. However, the legal framework related to cybersecurity is still underdeveloped and does not address critical vulnerabilities. Such gaps need to be bridged through legislative amendments, institutional strengthening, technical standardization, and capacity building to protect privacy, safeguard national security, and ensure reliable and resilient drone operations. Essentially, embedding cybersecurity within the regulatory fabric of

the drone ecosystem in India will be very important for ensuring sustainable growth, public trust, and operational safety.

The lack of compulsory certification for cybersecurity makes drones highly susceptible to every possible cyber threat ranging from spoofing and jamming to malicious takeover and interception of sensitive data. Existing regulations are essentially centered around operational safety issues, with little being said about either cyber resilience or data protection. This regulatory gap is further exacerbated by the fragmented nature of enforcement machinery and reliance on self-compliance, as no clear guidelines or statutory authority has been delegated to the concerned agencies to monitor and enforce cybersecurity standards. Consequently, India risks leaving the drone ecosystem open both to opportunistic and state-sponsored cyber-attacks. Again, there is an absence of explicit integration with India's national cyber laws, particularly the Information Technology Act, 2000, and the Digital Personal Data Protection Act of 2023, which might give rise to confusion regarding data governance, privacy, and operator liability. Without incident reporting and liability apportionment frameworks, in the event of a cyber incident, the drone operators, manufacturers, and the state authorities may be in a legal gray area, characterized by delayed response, unmitigated damages, and increased vulnerability against public safety.

Countries such as the United States, members of the European Union, and Australia have taken note from a comparative perspective that the intersection of drones and cybersecurity requires regulatory integration. The FAA and NIST in the United States have started to develop cybersecurity standards within the UAS traffic management system, while EASA and U-space regulations in Europe embed cyber resilience and data protection directly into certification processes. Australia, through CASA, mandates secure communications with encryption protocols at command and control links. Though pioneering in ease of access and digital governance through the Digital Sky Platform, India's regulatory framework lags behind in codifying cybersecurity measures that make drone operations resilient against evolving cyber threats. Taking a similar proactive approach would go some way toward bolstering operational security and public confidence in the wide deployment of drones across civilian, commercial, and governmental sectors.

Policy reforms must, therefore, be undertaken on several fronts. Legislative amendments should make cybersecurity certification a mandatory requirement for type approval, provide

statutory duties for secure data handling, and mandate privacy impact assessments for drone-based surveillance. Institutional reforms include a separate regulatory body or dedicated cell within the DGCA for drone cybersecurity, ensuring the requisite oversight and coordination among aviation regulators, CERT-In, law enforcement, and intelligence agencies. Technical measures to develop secure Unmanned Traffic Management protocols, mandating encryption and anti-spoofing mechanisms, and fostering national standards along with international bodies, would further strengthen resilience. Incentivizing research and innovation in secure UAS technologies will ensure that regulatory requirements do not constrain growth but rather point the industry toward robust and secure solutions.

Of equal importance is recognizing that cyber threats are dynamic and constantly changing. Static rules are at risk of growing outdated and may even fail to respond to new emerging vulnerabilities. In this view, the regulatory framework for drones in India needs to be flexible, principle-based, and focused on risk management, continuous monitoring, and adaptive compliance. Therefore, incorporating mechanisms for periodic review, threat assessment, and updating of cybersecurity norms and standards will ensure a legal regime responsive to technological change. The capacity building through training of operators, manufacturers, and regulators will nurture a culture of cybersecurity awareness and preparedness at large and reduce the possibility of human error or negligence contributing to the vulnerabilities.

Finally, embedding cybersecurity into India's drone law is a regulatory necessity and a strategic imperative.

Drones are increasingly employed in the service of critical infrastructure monitoring, disaster management, border security, and state surveillance. Vulnerabilities in these could be exploited to disrupt operations, compromise sensitive information, or even threaten public safety. Addressing these legal gaps will position India to lead in the field of secure drone operations and provide a model for harmonizing innovation, safety, and cybersecurity. A comprehensive legal framework with the inclusion of robust cybersecurity measures, well-defined liability, data protection, and effective mechanisms for enforcement would help engender more trust in UAS technology, ensure sustainable growth, and reduce risks inherent in the cyber-physical operational environment. The convergence of innovation and security is thus at the heart of the long-term viability of India's drone ecosystem in ensuring that technological advancement is not at the expense of national security, civil liberties, and public confidence.