

Skies Under Watch: Ethical and Legal Challenges of AI-Based Counter-Drone Systems in India and South Asia

Harmeet Singh and Anurag Jaiswal

INTRODUCTION

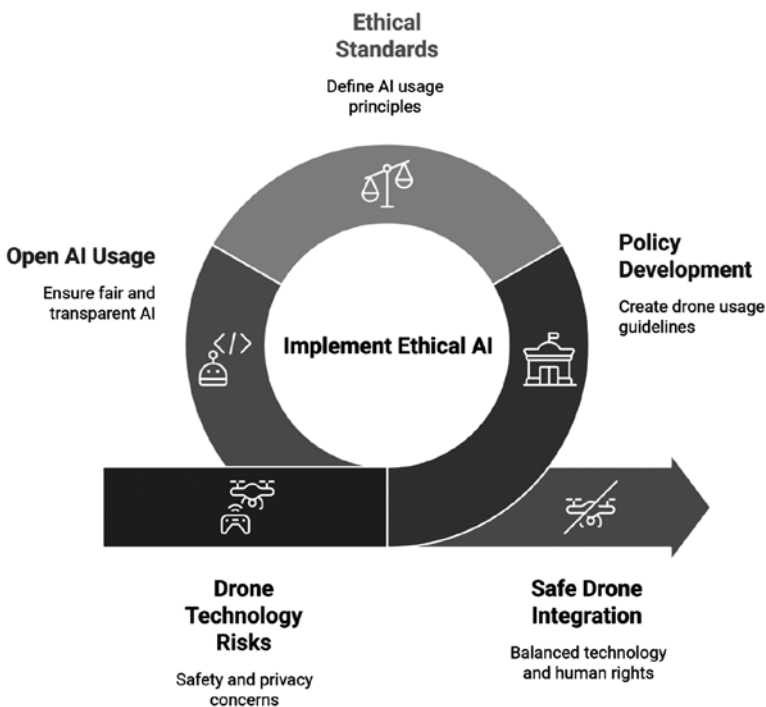
In recent times, the skies over South Asia have witnessed an exponential proliferation of drones. These Unmanned Aerial Vehicles (UAVs) are being routinely deployed for surveillance, disaster management, commercial activities like event management, infrastructure inspection, medical supply delivery and even for crop monitoring and wildlife protection. With the present relaxed norms in India, it has resulted in a booming industry projected to be over \$ 1.8 billion by 2026 and \$ 4.83 billion

Colonel **Harmeet Singh** is from the Regiment of Maratha Light Infantry with extensive experience in the counter-infiltration and counter-terrorism domains. He has a proven track record in international peacekeeping operations as well. The officer is currently pursuing Ph.D in Artificial Intelligence and Drone Warfare

Prof (Dr) **Anurag Jaiswal** is a distinguished professor with extensive expertise in the Department of Defence Studies at Meerut College. He has authored many books and more than 15 research papers have been credited to his name.

by 2030.^{1, 2} Though it is commendable from an economic viewpoint, it also presents certain concerns, especially over its misuse for smuggling contraband and weapons, espionage, privacy invasion and targeted attacks on critical assets. This makes one ponder over whether we have robust measures or policies to tackle these challenges.

Fig 1: Ethical AI for Counter-Drone Systems



As the Artificial Intelligence (AI) domain is witnessing an exponential growth, a probable answer to the challenge lies in AI-powered counter-drone systems. We know that these systems have the capacity for aerial threat detection and neutralising drones posing a danger. This capacity can be executed in real-

1. www.apeejay.news
2. www.techsciresearch.com

time because of the availability of technology like machine learning and data analytics, and that too with minimum human intervention. While this near autonomous capacity is an answer to the challenge faced, it also raises questions of legal ambiguities and ethical dilemmas. These issues become even more pertinent when seen from the prism of the South Asian geopolitical environment. Currently, there is very little literature available which addresses these concerns, addressing ethical governance and socio-legal aspects in the South Asian context. The existing literature generally centres on the Western context, thereby leaving a critical gap, especially for India and its neighbours, which have a distinct requirement. This paper is an endeavour to fill this void by analysing the pros and cons of AI-based counter-drone systems in South Asia and India, focussing on the need for a regulatory approach in the context of existing geopolitical dynamics.

AI AND COUNTER-DRONE SYSTEMS

Use of AI for counter-drone operations provides a huge advantage, especially enabling management of complex and large-scale scenarios. Thus, as a way forward, it is prudent to employ AI-based systems. We are aware that traditional systems of drone detection have the disadvantage of not being foolproof since they rely on vigilance and observational capability, further dependent on the efficiency of the human operator. By leveraging the potential of AI-based systems, the response to threats would not only be fast but also almost foolproof since it utilises vast datasets and algorithms to identify drone behaviours.

Any counter-drone system integrates four key functional aspects:

- Detection – Using radar, radio frequency scanners, and acoustic sensors.
- Identification – Classifying the drone type using AI.

- Tracking – Tracking the path and likely target area.
- Neutralisation – Using jamming, spoofing or kinetic measures.

When these systems are based on AI, it will lead to shortening of the Observe, Orient, Detect, Attack (OODA) loop, thereby ensuring faster and more efficient decision-making.

In the Indian context, the government has given an impetus to counter-drone capability through the *Atmanirbhar Bharat* schemes. Both the Ministry of Defence and the Ministry of Civil Aviation, through the Defence Research and Development Organisation (DRDO) and Bharat Electronics (BEL), have undertaken projects to develop counter-drone capacity.³ Moreover, many private firms are also working on integrating AI into both drone and counter-drone projects. This clearly reflects the changing environment of South Asia, where reliance on AI is growing manifold. However, what is important to note is that this advancement is outpacing the ethical and legal guidelines required to govern these systems, thus, creating a void.

LEGAL CHALLENGES

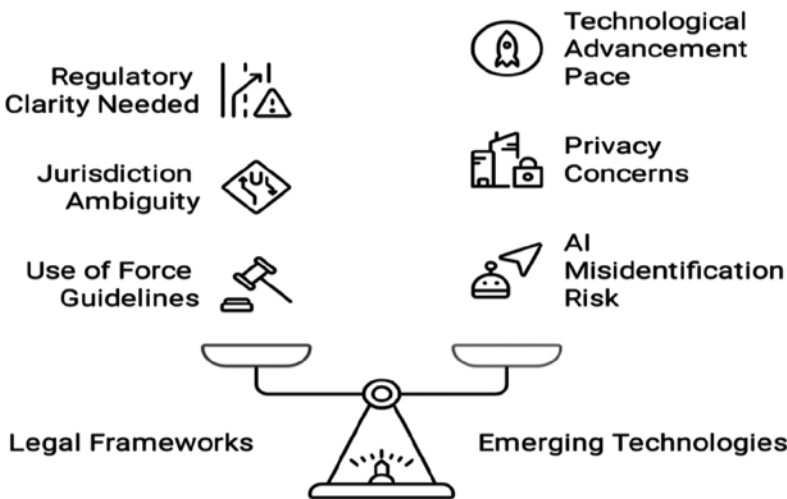
In India, the Directorate General of Civil Aviation (DGCA) has been entrusted with the responsibility to regulate drone usage, but the ambiguity emerges when it comes to signal jamming or the use of kinetic means against suspicious drones, thereby raising questions of legality. Similarly, the legal frameworks regarding governing the emerging technologies for use in the airspace are at a nascent stage across South Asia. A core concern remains as to who holds the authority to act. For instance, in India, the central government is mandated to manage airspace, but state governments and private players remain uncertain when it comes to responding to any unauthorised drone incursion. The

3. Ministry of Defence, “DRDO Develops Anti-Drone Technology”, Press Information Bureau, August 14, 2021.

existing Drone Rules of 2021, categorise drones based on weight, along with use, but provide less clarity when it comes to legally tackling/intercepting suspicious drones.⁴

Another key aspect which merits attention is that of ‘use of force’. As per both Indian law and International Human Rights Standards, any use of force should follow the principle of ‘*necessity and proportionality*’. Hence, if any AI-based system misidentifies a target, leading to intended/unintended damage to property or persons, the difficulty of assigning responsibility and liability is a reality. The question to ponder over is: who would be accountable? Would it be the operator or software developer, or agency entrusted with the responsibility of managing the system?

Fig 2: Balancing Legal Clarity with Technological Advancement



To address these concerns, the respective agencies are working on policies and laws which are evolving. Though the Digital Personal Data Protection Act was promulgated in 2023, certain inadequacies persist, especially related to the surveillance

4. Government of India, “Drone Rules, 2021”, Ministry of Civil Aviation, August 25, 2021.

capabilities of counter-drone systems.⁵ Since these systems gather extrinsic data related to the move patterns of unconcerned civilians and even capture imagery, they can lead to privacy concerns if robust data governance provisions/policies are not put in place.

A similar scenario exists at the international level where the legal picture remains unclear. Even though the Chicago Convention and guidelines from the International Civil Aviation Organisation (ICAO) do address the civil aviation conventions, they do not address the counter-drone technology-related concerns.⁶ This, when seen from the perspective of the South Asian geopolitical domain, especially in sensitive regions like Jammu and Kashmir (J&K) or the Indo-Pak border, will require clear provisions to be implemented. The deployment of autonomous systems for countering suspicious/rogue drones in these areas must adhere to the principles of commensurateness, peculiarity and precautions, in conformity with International Humanitarian Law.

ETHICAL CHALLENGES

The ethical dilemma which we face today with the use of AI-based counter-drone system stems from the *concern for transparency, accountability and authority*. The current South Asian environs are a complex mix of mistrust, exploitation and opaque policies. In such a region, can we afford to grant autonomy to systems to neutralise a drone? This question goes beyond legality and becomes an ethical concern, especially when such a critical decision could be made without direct human involvement. Since these AI-based systems exercise significant control over monitoring and automated decision-making backed by pre-fed algorithms, issues of openness and liability, arise, especially in a region where mutual trust is fragile.

5. Digital Personal Data Protection Act (India, 2023).

6. International Civil Aviation Organisation, *Convention on International Civil Aviation* (Chicago Convention, 1944).

As one looks deeper into these issues, one also comes across another vulnerability of '*algorithmic biases*'. What happens if AI models are trained on datasets which have a prejudice or bias? For instance, if the training dataset for these AI-based counter-drone systems has been collected from conflict-prone border areas, then all low-altitude drones may be classified as hostile, though there may be legitimate agricultural drones being used by the civil diaspora for crop monitoring, spraying, etc. Thus, it may lead to disrupting livelihoods and repeated interventions to prevent any suspicion against communities. Similarly, in an urban scenario, if the past dataset has been prepared by over-representing surveillance from a certain area, the automated system could unreasonably target such areas, which will further compound the bias of the datasets. Since these systems are prepared in such a manner that they continue to learn on the job, at times even their creators cannot fully explain how a decision would have been arrived at. Addressing this 'black box' nature of AI systems, thus, becomes a big challenge, further eroding accountability and legal oversight.

Moreover, the widespread use of AI for surveillance to detect drone threats underlines the vulnerability of being constantly watched. This erodes privacy, weakens trust and impacts civil liberties. In countries like Pakistan, where the public already lacks trust in institutions due to opaque policies and military control, these technologies could be misused in Pakistan Occupied Kashmir (PoK) or Balochistan to carry out systemic surveillance and suppress dissent under the pretext of drone control. Additionally, due to its dual-use nature, such technology can be repurposed for extensive political surveillance and domestic monitoring, with ulterior motives. To obviate these challenges, there is a need for clear ethical boundaries and strict controls, alongwith a robust mechanism. Otherwise, these systems, designed for defensive purposes, could be misused as instruments of control.

A COMPARATIVE GLANCE: EU AND US REGULATORY APPROACHES

The concern posed by AI systems underlines the global nature of this challenge. There is a need for the South Asian region to study the developments being undertaken by the European Union (EU) and the United States (US). Though every region has its own peculiarities, the best practices, with certain modifications may give us the way forward for a holistic solution. For instance, the proposed AI Act by the EU has its basic framework based on the fundamental rights of its people. It aims at classifying autonomous AI systems or applications on the basis of risk. Systems identified as 'high risk' based on assessment will be subjected to strict controls and obligations related to quality of data, transparency, strength of systems and clear practices.⁷

As regards US policies, they follow a system which adopts the sector-specific approach and is rather more fragmented, unlike the rights-based approach of the EU. Both these systems are in stark contrast with the South Asian environment, which is less restrictive and gives more freedom. The Federal Aviation Administration (FAA) and the Department of War (DoW) of the US are in the process of developing their own protocols. The DoW's approach is to emphasise ethical principles for AI to focus on traceability, reliable and governable systems, alongwith responsible behavior.⁸ These principles are not codified in a single law, unlike the EU's AI Act, but guide future developments and, more significantly, the deployment of AI-based counter-drone systems. It is pertinent to mention that the US system also faces a serious challenge to strike a balance between security requirements and ensuring civil liabilities.

7. European Parliament, "Artificial Intelligence Act: Amendments Adopted by the European Parliament", 2023.

8. US Department of Defence, *Directive 3000.09: Autonomy in Weapon Systems*, 2023.

The above comparison underscores that even the developed nations are struggling to regulate this space. Though the EU's rights-based and regulations-centric model is in contrast to the US' principles-guided approach, which is decentralised in nature, these two templates do provide options for South Asia. The primary endeavour in the South Asian environment should be to chart its own path, creating a tailored model that balances the EU's emphasis on fundamental rights, along with the practical operational approach adopted by the US, in line with the felt need and catering to the specific security needs of the region.

REGULATORY RESPONSE

In India, the regulatory landscape is primarily based on two legal provisions, i.e. Drone Rules, 2021, and the Digital Personal Data Protection Act (DPDPA), 2023. These two form the legal pillars on which the agencies base their activities. In addition, the agencies responsible for ensuring security during key or sporting events develop *ad hoc* protocols. However, these *ad hoc* protocols lack legal standing, and even their application is not standardised across the spectrum. Another big hurdle observed is the lack of inter-agency coordination with different protocols applied by different states and regions. The primary challenge faced today is that these *ad hoc* protocols or Drone Rules and DPDPA provide very little guidance on the critical aspects of accountability for automated decisions: operations of automated systems; and management of surveillance data.

When we look at the neighbouring countries, the situation is even more grim. For instance, in Pakistan, the counter-drone operations are managed by its army, clouded with a lack of transparency. This limited oversight for public scrutiny raises concerns in the civil populace regarding unaccountable surveillance and the use of force. At the regional level, the

biggest hurdle remains a lack of consensus due to geopolitical compulsions, especially with regard to standards for counter-drone systems. The South Asian nation-states need to appreciate that in the absence of collaboration, the security of the region may be adversely impacted, especially with the increased risk of miscalculation and subsequent escalation. To prevent such a situation, there is a need for India to commence collaboration efforts wherein international standards for AI transparency laid down by the International Organisation for Standardisation (ISO)/International Electrotechnical Commission (IEC) or the *Ethically Aligned Design* of the Institute of Electrical and Electronics Engineers (IEEE) could be adopted in the region.^{9, 10} The way ahead will have to be a consultative and collaborative process, else these theoretical guidelines would remain ineffective on the ground.

RECOMMENDATIONS

To address the legal and ethical concerns which have come to the fore because of the advent of emerging technologies, there is a necessity to adopt a holistic approach from womb to tomb. Governments and agencies responsible for regulating and managing the airspace need to lay down clear guidelines for ensuring transparency, accountability and oversight. The following aspects merit attention:

- **Strengthen Regulations/Regulatory Reforms:** The government needs to enact clear laws which are unambiguous and give clarity when it comes to aspects of transparency and accountability. These laws must lay down strict limits when it

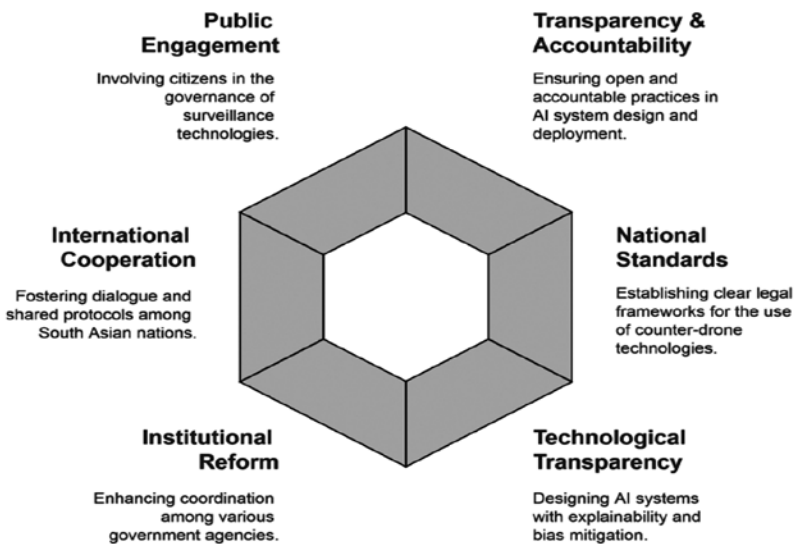
9. Institute of Electrical and Electronics Engineers (IEEE), *Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems*, 1st ed., 2019.

10. ISO/IEC JTC 1/SC 42, *Artificial Intelligence – Overview of Trustworthiness in AI* (ISO/IEC TR 24028: 2020).

comes to data collection, storage and even its access. To build on trust and visibility, there should be provisions for public scrutiny and a grievance redressal mechanism. One of the key concerns which emanates from autonomous decision-making by AI systems can be addressed by mandating the 'human in the loop' for any use of force by the system.

- **Ethical Design and Technological Transparency:** The key to addressing ethical concerns is by mandating and encouraging designers to incorporate *explainability and transparency* as core principles. It is imperative for designers to have algorithms that are open to audit and will mitigate any bias. All such systems should be subjected by law to rigorous testing and open to public review.

Fig 3: Strengthening AI Governance in South Asia



- **Promote Institutional Coordination:** For effective implementation of policies and addressing the concerns of everyone, there is an inescapable requirement for inter-agency

coordination. In India, coordination is required among various stakeholders like civil aviation, defence, law enforcement and authorities responsible for data protection. The mechanism for coordination between states and even with the central government stakeholders would also be a prerequisite to harmonise standards and practices, ensuring ethical use of AI.

- **Regional Cooperation:** As highlighted earlier, confidence-building measures will have to be adopted on the terms of cross-border discussions to come to a consensus and a common yardstick related to drone identification, threat assessment and conflict management. The formulation of these common protocols can only be done through a collaborative process. India, being a major stakeholder in South Asia, is recommended to take the lead.
- **Public Engagement:** The legal and ethical concerns affecting the civil populace would require a clear framework and laws which lend themselves to public scrutiny, audit and grievance redressal mechanisms, thereby making it a transparent system. It is prudent that civil society organisations and experts are engaged before the formulation of such policies. This will facilitate overcoming any concerns related to human rights.

CONCLUSION

AI-based counter-drone systems emerge as an effective and efficient defence apparatus to counter aerial threats, but this technology stands at a critical juncture as well. If these systems are left improperly governed, they can pose a serious risk to human rights and civil liberties. Ambiguous laws, weak policies related to regulatory oversight and unanswered ethical concerns will further depreciate the trust of the population. This paper has tried to highlight the pros and cons of the advancement of

AI technology for countering drones. The need of the hour is to adopt a holistic approach which focusses on the core principles of transparency, accountability and cooperation at all levels. The endeavour of technocrats and policy-makers has to be on ensuring that advancement of technology is in consonance with the fundamental freedoms of the civil population.

