INTERNATIONAL JOURNAL OF SPACE LAW AND POLICY

VOLUME 3 AND ISSUE 1 OF 2025

APIS – 3920 - 0014 *(and)* ISSN - 2584-1955 [IF SCORE – 7.58]

Published by

Institute of Legal Education

https://iledu.in

UNMANNED THREATS: THE INTERNATIONAL LEGAL RESPONSE TO DRONE-ENABLED TERRORISM

AUTHOR - MS. ANNIE WILSON* & PROF. DR. V. R. DINKAR**

* RESEARCH SCHOLAR, (2022-2025 BATCH), SCHOOL OF LAW, HINDUSTAN UNIVERSITY, CHENNAI.

** DEAN, SCHOOL OF LAW, HINDUSTAN UNIVERSITY, CHENNAI.

BEST CITATION - MS. ANNIE WILSON & PROF. DR. V. R. DINKAR, UNMANNED THREATS: THE INTERNATIONAL LEGAL RESPONSE TO DRONE-ENABLED TERRORISM, *INTERNATIONAL JOURNAL OF SPACE LAW AND POLICY (IJSLP)*, 3 (1) OF 2025, PG. 84-88, APIS – 3920 - 0014 & ISSN - 2584-1955

Abstract

Drone-enabled terrorism forms one of the most complex technological and legal threats of the twenty-first century. Low-cost, easily modifiable, and increasingly available, UAVs blur the boundary between the regulation of airspace and armed conflict when transformed from their original civilian use to instruments of terror. Despite the growing security threat, the international legal framework, anchored within the Chicago Convention (1944) and Montreal Convention (1971), drafted originally for manned aviation, leaves the misuse of drones by non-state actors largely unregulated. This article examines the international regime governing drone terrorism through three analytical axes: (i) the inadequacy of existing legal instruments, (ii) the doctrinal and evidentiary challenges of attributing responsibility under the Articles on State Responsibility (2001), and (iii) a comparative assessment of Indian, United States, and ICAO regulatory models. Through doctrinal analysis and emerging state practice, this paper argues for an International Counter-Drone Protocol under ICAO and the United Nations that would institutionalize traceability, accountability, and cooperation while safeguarding human rights and civil liberties.

Keywords - Drone terrorism, international law, state responsibility, attribution, ICAO, sovereignty, drone, counter-drone governance, human rights, aviation security.

I. Introduction

The emergence of drone-enabled terrorism is a new phase of asymmetric conflict. Whereas early terrorism relied on conventional explosives or hijacked aircraft, contemporary non-state actors increasingly make use of commercially available small drones for reconnaissance, targeted assassinations, and delivery of improvised explosives. Incidents such as the 2019 Abqaiq–Khurais strikes on Saudi oil infrastructure and repeated UAV incursions across the India–Pakistan border provide examples of the disruptive capacity of these technologies (Singh 2022). Because drones can be operated remotely across frontiers, they erode the traditional notion of territorial control enshrined in Article 1 of the Chicago Convention (1944) that recognises each state's "complete and exclusive sovereignty" over its airspace.

Despite the scale of the threat, the international community is yet to devise a binding framework for unmanned aerial violence. Most of the existing aviation and counter-terrorism conventions were negotiated in an age predating miniaturized robotics and algorithmic navigation. States therefore currently rely on a patchwork of national rules, soft-law instruments, and ad hoc cooperative mechanisms. This research interrogates those legal lacunae through doctrinal, comparative,

INTERNATIONAL JOURNAL OF SPACE LAW AND POLICY
VOLUME 3 AND ISSUE 1 OF 2025
APIS – 3920 - 0014 *(and)* ISSN - 2584-1955 [IF SCORE – 7.58]
Published by
Institute of Legal Education
https://iledu.in

and policy analysis with a view to elucidating how international law stands-and where it must evolve-to confront the menace of unmanned terrorism.

II. International Legal Framework on Drone Terrorism

2.1 Foundational Treaties and Their Limits

The Chicago Convention of 1944 established the ICAO and codified principles of state sovereignty and safe civil aviation. However, most of its provisions regulate manned aircraft only. For instance, Article 3 bis prohibits the use of force against civil aircraft, with no reference to unmanned systems. In the same vein, the Montreal Convention (1971) criminalises acts of unlawful interference with civil aviation-sabotage, hijacking, or attacks on airports-but not unmanned aircraft used by non-state actors. According to Boucher (2016), "the definitional omission has created a grey zone between aviation law and counter-terrorism law".

2.2 Soft Law and ICAO Guidance

ICAO has tried to fill part of the above gap by means of Circular 328/AN/190 (2011) on UAS and continuing RPAS initiatives. The aforementioned documents harmonised safety standards and categories of operation but maintained their non-binding character. Furthermore, they do not entail any enforcement commitments nor attribute a system or provide for data sharing schemes between states. ICAO, 2011. According to scholars, such as Kaplow, 2018, non-binding standards nullify deterrent effects because terrorists can take advantage of inconsistent national rules.

2.3 Counter-Terrorism Law and Due Diligence

UN Security Council Resolution 1373 (2001) requires states to prevent financing and support of terrorism, while Resolution 1540 (2004) addresses weapons proliferation. Both instruments impose general duties of prevention but are technologically neutral. They do not establish special mechanisms for tracing or intercepting UAVs. The principle of due diligence, articulated in the Corfu Channel case (1949) and since reiterated in environmental and cyber jurisprudence, arguably extends to UAV threats: states must not knowingly allow their territory to be used in acts causing harm to other states. Yet, enforcement of that norm depends upon evidentiary cooperation which few jurisdictions have institutionalised.

2.4 General International Law

The Articles on State Responsibility of 2001 codify attribution and breach, but their application to drone terrorism is highly problematic. Article 8 requires that a state exercise "direction or control" over the actors. Because terrorist groups often operate autonomously or from ungoverned spaces, the requirement of effective control-as defined in Nicaragua v. United States (1986)-sets a nearly unattainable evidentiary bar. Recent scholarship suggests evolving the standard toward an overall control or due diligence threshold, holding states responsible where they fail to prevent known or foreseeable UAV misuse.

2.5 The Need for Lex Specialis

Legal commentors call for a new protocol under ICAO-or the UN Office of Counter-Terrorism-to include UAV identification, cross-border data exchange, and sanctions for negligent non-compliance (Boucher 2016; Singh 2022). The proposed treaty would have ample precedents: the Convention on Certain Conventional Weapons (1980) and the Budapest Cybercrime Convention (2001) are among the international agreements that adapted legal regimes to new technologies. In the absence of a similar regime, drone terrorism will continue to exploit jurisdictional seams between aviation safety and counter-terrorism law.

III. Challenges of State Responsibility and Attribution

3.1 Doctrinal Foundations

Attribution determines who bears the legal consequences of a UAV attack. Under Articles 2 and 8 of the Articles on State Responsibility

(2001), a wrongful act is attributable to a state if performed by its organs or by entities acting under its direction or control (ILC 2001). However, when UAVs are launched by non-state actors, the question becomes whether the sponsoring or harbouring state exercised sufficient control. The ICJ in Nicaragua (1986) demanded "effective control" over each operation, a standard reaffirmed in Bosnia Genocide (2007) but criticised as excessively restrictive (Byers 2004).

3.2 Evidentiary Complexities

For drones, attribution requires digital forensics and telemetry retrieval, serial number, and radio-frequency signature and intelligence correlation. However, UAVs are inexpensive, modifiable, and usually come from open markets. Moreover, forensic evidence can be deleted or fabricated, and states are unwilling to share classified information. According to Singh (2022), "the very architecture of UAV technology is built for deniability." Lacking international standards of evidence, national investigations are inconsistent and relatively few prosecutions are successful.

3.3 Expanding Due-Diligence Obligations

In overcoming this impasse, many jurists suggest shifting from the traditional logic of strict attribution to one of preventive responsibility. Accordingly, a state would incur international liability when failing to exercise due diligence in preventing drone attacks from within its territory or its nationals. This falls under the interpretation in line with the preventive logic of UNSC 1373 (2001) and also with environmental precedents such as Trail Smelter (1938/41). This thus acknowledges the fact that under conditions of technological diffuseness, which is quite characteristic in this field, negligence may be as consequential as direct control.

3.4 Institutional and Political Barriers

Even where evidence exists, political calculation generally stands in the way of formal attribution. States will often favour diplomatic protest or covert counter-measures over legal proceedings that disclose intelligence methods. By contrast, the Tallinn Manual 2.0 on cyber operations suggests one alternative paradigm: a non-binding expert restatement to help clarify the threshold of responsibility without entailing adjudication. A similar Tallinn-style manual on drones would codify norms of conduct and investigative cooperation while leaving sovereignty intact.

3.5 Toward Attribution Mechanisms

A reformed attribution framework would rest on three pillars: a) technical standards-mandatory Remote ID and data-retention requirements to preserve evidence; b) legal harmonisation, adoption of an overall control plus due diligence test; c) institutional innovation, a joint ICAO-UNOCT Drone Threat Intelligence Network empowered to authenticate forensic data and coordinate investigations. Such mechanisms would strengthen accountability without overburdening states with unrealistic evidentiary expectations.

IV. Comparative Policy Analysis: India, United States and ICAO

4.1 India's Evolving Framework

India's Drone Rules of 2021 updated the domestic regulatory environment by categorizing drones based on weight, requiring registration through the Digital Sky platform, and introducing geofencing. The Draft Civil Drone Promotion and Regulation Bill 2025 further advances this course, integrating digital permissions and becoming more innovation-friendly. Still, both remain essentially internally oriented; neither tackles transnational attribution or international cooperation. Analyses by scholars underline this gap: India's counter-terrorism mechanisms are based on general penal provisions and not aviation-specific offenses. Besides, inter-agency overlap between the Ministry of Civil Aviation, Ministry of Home Affairs, and armed forces complicates operational coordination.

Nevertheless, India has pioneered technological counter-measures. The National Counter-Rogue Drone Guidelines (2019) establish detection and neutralisation protocols using radar, RF detectors, and soft-kill techniques. In June 2021, after the UAV attacks on an airbase in Jammu, India announced plans for a national counter-drone grid. Yet experts warn that domestic capacity cannot substitute for international cooperation when drones originate abroad.

4.2 The United States Model

The United States has adopted a layered system combining regulation, technology, and enforcement. The FAA's Remote Identification of Unmanned Aircraft Rule (2020) requires drones to broadcast identification and location data accessible to law enforcement (FAA 2020). Complementary legislation—the Preventing Emerging Threats Act (2018) and the National Defense Authorization Acts—empowers federal agencies to detect and neutralise rogue UAVs. Scholars praise the Remote ID framework for enhancing traceability and forensic readiness (Kaplan 2021). However, critics note privacy and federalism concerns, as pervasive tracking may infringe civil liberties (Wagner 2022). Furthermore, U.S. law remains territorially confined: absent bilateral arrangements, Remote ID data cannot easily be shared internationally.

4.3 ICAO and Multilateral Efforts

ICAO's ongoing RPAS Panel and UAS Advisory Group work to integrate unmanned traffic into civil airspace. Annex 6 Part IV and Annex 19 on safety management now reference RPAS operations, but none explicitly address counter-terrorism. ICAO's normative strength lies in its technical expertise and near-universal membership; its weakness is the consensual, slow nature of standard adoption. Boucher (2016) and Parameswaran (2020) argue that ICAO should adopt a dual-track strategy: (i) incorporate UAV-security annexes focusing on identification and interdiction; and (ii) coordinate with the UN Office of Counter-Terrorism to ensure that aviation safety norms are linked to security obligations.

4.4 Comparative Insights

Comparatively, the U.S. model has the lead in traceability, India's in the speed of regulatory adaptation, and ICAO's in global coordination. An optimal framework would synthesize these strengths:

- Technical interoperability: universal Remote ID and telemetry standards to enable cross-border identification.
- Legal harmonisation: shared definitions of drone-related offences under the multilateral protocol.
- Information sharing: a centralized Drone Threat Intelligence Network under the auspices of ICAO-UNOCT, and
- Human rights safeguards: oversight and transparency in counter-drone operations consistent with ICCPR.

4.5 Literature Synthesis

The comparative scholarship converges on the notion of shared responsibility. Singh (2022) views drone terrorism through the prism of collective security, calling for "a mosaic of domestic, regional and international cooperation." Boucher (2016) frames it as a governance deficit demanding hybrid regulation that combines aviation safety with criminal accountability. Recent analyses by the European Parliament (2023) and Asian Policy Foundation (2024) call for a Drone Code of Conduct akin to the Hague Code of Conduct against Ballistic Missile Proliferation. This literature is together supportive of a model that preserves innovation while embedding accountability in international law.

V. Human Rights and Ethical Considerations

Counter-drone measures-signal jamming, directed-energy weapons, and AI-enabled surveillance-must be implemented within human-rights limits. Article 6 (ICCPR) ensures the right to life, while Article 17 protects privacy.

INTERNATIONAL JOURNAL OF SPACE LAW AND POLICY
VOLUME 3 AND ISSUE 1 OF 2025
APIS – 3920 - 0014 *(and)* ISSN - 2584-1955 [IF SCORE – 7.58]
Published by
Institute of Legal Education
https://iledu.in

Indiscriminate electronic counter-measures can disrupt civilian communications or put legitimate air traffic in danger. Hence, proportionality and necessity, being the principles derived from International Humanitarian Law, should guide deployment (Melzer 2021). Ethically, the increasing resort to autonomous defense systems creates questions of accountability: in case an AI algorithm wrongly identifies a civilian drone, leading to collateral damage, legal responsibility would remain unclear. Scholars recommend a "human-in-the-loop" requirement for any lethal or destructive counter-drone decisions (Crootof 2019). Transparency via public reporting and judicial review would enhance legitimacy and public trust.

VI. Recommendations and Way Forward

A sustainable international response rests on four pillars:

• Legal Codification: Establish an International Counter-Drone Protocol under ICAO/UN that requires UAV registration, Remote ID, and data-sharing obligations.

• Institutional coordination: The ICAO-UNOCT-INTERPOL Drone Threat Intelligence Network will allow real-time information exchange and joint investigations.

• Capacity Building: Technology-transfer partnerships with developing states can help them establish forensic, radar, and AI-based detection systems.

• Protection of Rights: Include oversight and accountability in counter-drone legislation to ensure compliance with IHRL and IHL.

These measures would take abstract principles of sovereignty and responsibility and turn them into operational cooperation, transforming fragmented national policies into a coherent global architecture. Conclusion Drone terrorism epitomises the intersection of technology, law, and global security. Existing aviation and counter-terrorism treaties, conceived in a pre-digital era, cannot by themselves address unmanned threats that are fast, anonymous, and transboundary.

The challenge is not merely legal but systemic: ensuring that sovereignty, accountability, and human rights evolve alongside technological capability. A treaty-based International Counter-Drone Protocol, grounded in due diligence and shared responsibility, would bridge doctrinal gaps and institutionalise cooperation. Through ICAO's normative reach and the UN's enforcement legitimacy, the international community can move toward secure, ethical, and rules-based skies.

References

1. Boucher, P. (2016) Unmanned Aerial Systems: Opportunities and Challenges for Civil Aviation, European Parliamentary Research Service.
2. Byers, M. (2004) War Law: Understanding International Law and Armed Conflict, Grove Press.
3. Crootof, R. (2019) 'The Legal and Ethical Implications of Autonomous Defense Systems', Yale Journal of International Law, 44(1).
4. Federal Aviation Administration (2020) Remote Identification of Unmanned Aircraft Rule, Washington D.C.
5. Government of India (2021) Drone Rules 2021, Ministry of Civil Aviation.