International Civil Aviation Organization

WORKING PAPER

A41-WP/271
EX/118
2/8/22

ASSEMBLY — 41ST SESSION

EXECUTIVE COMMITTEE

Agenda Item 14: Aviation Security — Policy

ENVISION OF PROPOSED REGULATORY FRAMEWORK FOR COUNTER ROGUE DRONE

(Presented by India)

EXECUTIVE SUMMARY

India is progressing in the development of provisions for the integration of remotely piloted aircraft systems (RPAS) into the aviation system, with the notification of liberalised "Drone Rules 2021". With the continuously evolving technology scenario, the drones have improved significantly in terms of their mode of communication with the base station, capability to fly autonomously, duration and payload capacity. The need is felt to identify, regulate and mitigate rogue- drone related activities in a manner that they do not pose any risk to safety and security of the nation, people and assets.

This working paper presents updates on India's work towards preparing a regulatory framework for establishing a graded response mechanism and counter rogue drone policy, to address the contemporary challenges posed by RPAS/drones, amid the growing proliferation of commercial drone activities in India.

Action: The Assembly is invited to:

a) note the information contained in this paper;
b) to consider whether it would be timely to do an experience sharing about how India is developing, establishing and maintaining a safe and secure civil aviation security eco-system, with counter rogue-drone policy and guidelines, which is being envisaged; and
c) encourage member state to avail the benefits arising out of implementation of this framework, as a best practice model.

Strategic Objectives:	This working paper relates to the *Security and Facilitation* Strategic Objective
Financial implications:	
References:	

1. INTRODUCTION

1.1 Recently, Ministry of Civil Aviation, Government of India notified The Drone Rules 2021. It will help leverage India's strengths in innovation, technology and engineering to make India a drone hub.

1.2 The liberalised Drone Rules 2021 are built on a premise of trust, self-certification and non-intrusive monitoring. These rules are designed to usher in an era of supernormal growth while balancing safety and security considerations.

1.3 Operated recklessly or negligently, the drones can be a nuisance and risk to public safety. Operated by ill intent (by terrorist and criminals), drone can pose serious threat to national security and critical infrastructure. It is primarily the latter scenario, which obligated us to envisage, identify and to codify Counter-rogue drone policy and guidelines, to counter such security challenges, amid India's perceived potential to be a global drone hub.

2. DISCUSSION

2.1 Released on August 25, 2021, the Drone Rules, 2021, Ministry of Civil Aviation has relaxed approvals and other requirements for unmanned aircraft systems to make it easier for civilian drone operators to do business and to tap the potential of this unexplored market.

2.2 To further boost the proliferation of Drone Industry in India, several approvals have been abolished via: unique authorisation number, unique prototype identification number, certificate of manufacturing and airworthiness, certificate of conformance, certificate of maintenance, import clearance, etc.

2.3 As per the Drone Rules 2021, The Indian airspace for drones is divided into three zones: Green, Yellow, and Red. "**Green zone**" is the airspace from the ground up to a vertical distance of 400 feet (120 meters) that has not been designated as a red zone or yellow zone in the airspace map. No permission is required for operating drones in green zones.

2.4 The airspace above 400 feet or 120 metre in the designated green zone and the airspace above 200 feet or 60 metre in the area located between the lateral distance of 8 kilometre and 12 kilometre from the perimeter of an operational airport, has been designated as "**Yellow zone**". Unmanned aircraft system operations are restricted in Yellow zone and requires permission from the concerned air traffic control authority. "**Red zone**" means the airspace within which unmanned aircraft system operations shall be permitted only by the Central Government of India.

2.5 The unmanned aircraft system has been classified as Nano, Micro, Small, Medium and Large unmanned aircraft system, based on the maximum all-up weight including payload, in India. It is provisioned that no remote pilot licence is required for Micro drones (for non-commercial use) and Nano drones.

2.6 Director General of Civil Aviation (DGCA) of India shall prescribe drone training requirements, oversee drone schools and provide pilot licences online.

2.7 Though India has guidelines in place since 2019, to counter threat from sub-conventional aerial platforms, civilian use of drones, but first-of-its-kind attack by purported drones at Jammu airport prompted to deliberate the framing of a policy response to check against security threats posed by the use

of unmanned aerial vehicles (UAVs). The incident has shown the need to recodify rules and response strategies to provide a clear deterrence against any such attacks.

2.8 As it became increasingly apparent that drones can pose a considerable security threat, the Govt. of India has envisaged to put together a graded response mechanism and proposes to have a counter rogue drone policy for countering rogue drones.

2.9 The graded response mechanism, which is under evolution, would propose to provide a policy framework and guidance to Law Enforcement Agencies (LEAs) to assist them in mitigating the dangers of malicious use of drones.

2.10 The Counter Rogue Drone Policy framework proposes to cover the envisioned objectives, which inter-alia includes, define malicious usage of drones; develop a proper understanding of the growing threat to national security, and institutional mechanism to deal with rogue drones. It also proposes to delineate the role of different authorities that would respond to this challenge and their role in different threat scenarios; as well as proportionate response to this evolving threat based on legal, regulatory, commercial aspects and deterrence thereof.

2.11 The Counter Rogue Drone Policy framework proposes to identify various types of drones on the basis of the threat profile, which primarily includes: **autonomous drones**, which are controlled by on-board computers and don't need to be manually operated; **drone swarms**, which can be used in attacks by simultaneously launching and managing multiple drones using coordination software; and **stealth drones** that can be made to evade radar and other means of detection.

2.12 Based on a thorough security review of all the civil aviation facilities in the country in terms of criticality and vulnerability, all the airports have been categorised as vital installation. It is proposed that all the airports would be requiring appropriate counter rogue drone solutions as obligatory requirement.

2.13 The proposed rogue drones policy framework for airport security recommends a multi layered approach to guarding against drones. The obligatory solution model is the top priority level and covers all airports in India.

2.14 Considering criticality, safety and security of air operations and navigation, it envisages a protective cover for the airports that includes primary and passive detection systems like radar, radio frequency detectors, electro-optical and infrared cameras. For the task of neutralising drones these sites can have both **'soft kill'** systems, like radio frequency jammers, and **'hard kill'** mechanisms like high-powered electromagnetic and LASER weapons, drone-catching nets, etc.

2.15 As the anti-drone technologies, across the world, are still at a nascent stage and their effectiveness is yet to be established, accordingly it is understood that LEAs would need to train their personnel. Specific to the roles and responsibilities, they would be expected to play and discharge in countering the rogue drone menace. Accordingly, the proposed rogue drones policy framework have identified the role of some of the national institutions of repute, in terms of imparting training and capacity building.

2.16 The threat from Rogue Drone calls for a comprehensive and coordinated approach, including all stakeholders within the country and international community. To stay abreast with developments and best practices, the Guidelines have identified and laid down a coordination and review mechanism, from national level to regional level. The Coordination and Review mechanism would analyse,

discuss and compare experienced threats across different theatres/sectors to improve collective understanding.

2.17 Accordingly, the purpose of the Working Paper is to draw the attention of Assembly towards the progress being made by India in establishing a resilient, robust, and inclusive proposed rogue drones policy framework to combat the growing menace on rogue drone activities in India; and request to note the contents of this working paper.

— END —