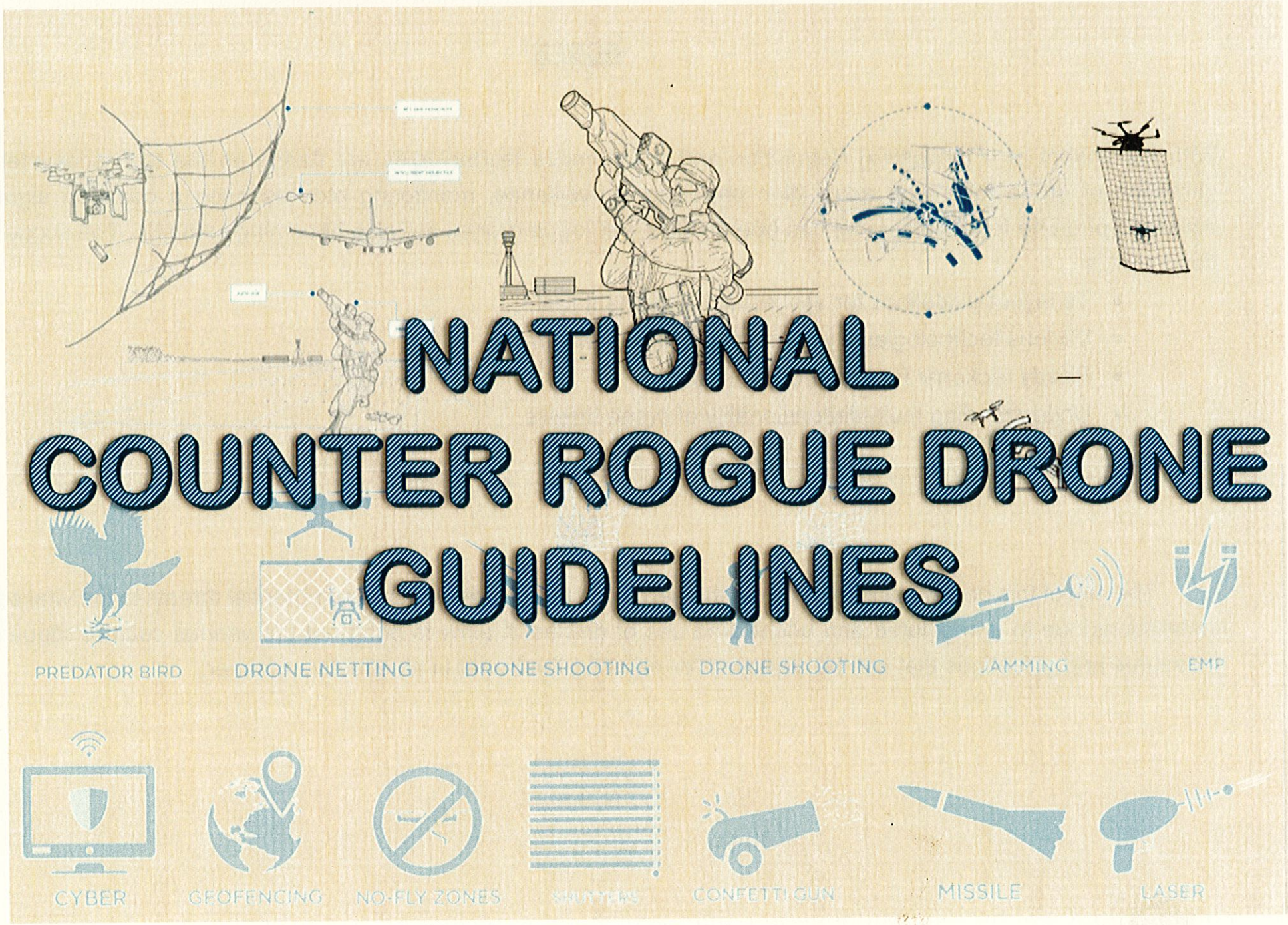
NATIONAL
COUNTER ROGUE DRONE
GUIDELINES
PREDATOR BIRD
DRONE NETTING
DRONE SHOOTING
DRONE SHOOTING
JAMMING
EMP
CYBER
GEOFENCING
NO-FLY ZONES
CONFETTI GUN
MISSILE
LASER

SCOPE

With the advent of 4th Industrial Revolution and autonomous technologies are flaring up the tech ecosystem and utilization of drone for image acquisition patrolling, surveillance, monitoring etc has been a common sight. The utilisation of drone for development has been a bliss, yet rogue drones are also becoming common. The scope of the document is:

- To layout guidelines for assessing the drone threat.
- Various technologies involved in handling drone threat.
- Ready reckoner for anti-drone measures.
- Understanding multi-dimensionality of drone threats.

AIM

The aim of this document is to bring out the perceived law & order outcry and potential threats to the vital security installations due to unregulated and unchecked use of drones. It aims to bring out the various counter rogue drone measures and guidelines that can be deployed for handling the threat in an effective manner.

CONTENTS

CHAPTER 1

EMERGENCE OF DRONES: SECURITY IMPERATIVES

1. Until the last decade, the utilisation of Remotely Piloted Aircraft (RPA) or Unmanned Aircraft Vehicle (UAV) technology was mainly controlled by governments across the globe to meet the emerging Civil and Military requirements. RPAs commonly known as Drones are frequently utilised by militaries for variety of applications, such as surveillance and reconnaissance of enemy or hostile terrain, to track enemy land or sea movements, for border patrols, search and rescue missions, and emergency services. Countries like USA have widely utilised armed versions of drones to target and kill enemy forces including terrorists in combat zones like Afghanistan.

2. However, with the technological advancements RPAs can now be effectively utilized in diversified Civil sectors including Infrastructure Development, Agriculture surveys, Industrial applications, Ground Mapping, Aerial photography, Payload delivery, urban Air Mobility solutions, Forestry services, Fish and Wildlife observation, Emergency medical response, Maintenance of Law and Order, Disaster relief etc. In India also, RPAs have found enormous potential for operations in Civil and Commercial fields. The possibility of utilization of RPAs towards swift transportation of blood, human organs and lifesaving drugs has opened new avenues for utilization of these platforms in the remotest part of the country for extending Medicare facilities.

3. As the global drone market has grown manifold, the debates on legal, regulatory, and even moral issues around their use have also gained momentum. The miniature Unmanned aircraft, Consumer drones and Do It Yourself (DIY) drones are readily available over the Internet and they don't require much of expertise for operating. However, the global mechanisms towards regulating and countering rogue drones, both procedurally and technologically, have remained inadequate till now. Hence, security of vital Civil and Military installations due to unauthorised usage of drones remains an inevitable flip side across the globe and in India too.

4. There are also issues pertaining to air collision and aerospace safety aspects due to growing infringement of UAS platforms which are of major concern for aerospace sector. In recent years, incidents of 'near misses' and air collision involving unmanned drones and manned aircraft, reported worldwide have come to light. In India also, multiple incidents of sightings of drones in near vicinity to commercial airliners and major airports like New Delhi and Mumbai have been reported in recent past, raising flight safety concerns. Further, the upsurge in drone use has also increased the threat quotient for VVIPs who can be targeted through the rogue drones. Recent incidents of utilisation of drones to target VVIPs in Venezuela and operations of such platforms dangerously close to dignitaries in Germany, Japan and USA are stark reminder of the threat level from errant and rogue drones.

5. Among industrial spectrum also, extensive and costly disruption to vital nuclear installations, Transportation networks, Power lines or Oil refineries from rogue drones, remains a potential threat area. The incidents of multiple sightings of Drones over sensitive facilities worldwide have adequately highlighted the feasibility of state and non-state-sponsored espionage. In addition, the possibility of utilization of drones to target crowded places like sports arenas and mass gatherings, utilising cheap commercially available drones for creating damage and generating public outcry cannot be ruled out.

6. In the military domain too, small drones have been proliferating at a rate that has alarmed battlefield commanders and planners alike. The utilisation of armed drones by extremist groups to carry out reconnaissance and targeting strategic Israeli installations during Israel-Lebanon war is an example of escalation of terrorist and insurgent drone capabilities. In certain incidents, the small drones were also armed with explosive ordnance, to convert them into potentially lethal guided missiles, thus demonstrating the growing sophistication with which these potent warriors have found relevance in combat zones.

7. The sub-conventional threat from rogue unmanned aerial platforms has emerged as a new threat spectrum with expanded list of target systems and vulnerability levels from the "bad actors". India, too is not immune to such threats. Hence, the risk to aerospace safety and threat to vital installations from rogue drones require the security establishment to devise regulatory mechanisms and protective security apparatus to inhibit the extremist groups from using these platforms for their ulterior purposes.

CHAPTER 2

DRONE CLASSIFICATIONS AND ROGUE APPLICATIONS

1. The terms like Drone, Remotely Piloted Vehicle (RPV), Remotely Piloted Aircraft (RPA), Unmanned Aerial vehicle (UAV) and Unmanned Aerial System (UAS) are the different nomenclature for the unmanned aircraft and have been used in different times but, all these terms mean the same. A classification system for drones is needed to stratify the required levels of air worthiness, equipage and aircrew training standards. There are numerous classifications systems within the RPA field, most commonly based on All Up Weight (AUW), Endurance and range, maximum Ceiling, Wing loading, Engine type, Power and thrust load etc. However, in India Civil RPAs are categorized in accordance with Maximum All-Up-Weight (including payload) as indicated below: -

(a) Nano RPAs (Less than or equal to 250 gm)
(b) Micro RPAs (Greater than 250 grams and less than or equal to 2 kg)
(c) Small RPAs (Greater than 2 kg and less than or equal to 25 kg)
(d) Medium RPAs (Greater than 25 kg and less than or equal to 150 kg)
(e) Large RPAs (Greater than 150 kg)

2. The classification of drones based on size is as mentioned below: -

(a) **Nano RPAs**. Nano RPAs weigh upto 250 gm with rotor diameter upto three to five inches and size that can accommodate on the palm. Due to technological advancements, Nano RPAs like Sky viper can be fitted with variety of sensors for better stability. Nano RPAs generally fly up to 500 feet from remote pilot. These platforms are widely utilised for recreational purposes, however, they can also be used for photography.

(b) **Micro & Small RPAs**. The RPAs in Micro and Small category weigh from 250 gm to 25 kg and are widely employed for recreational and commercial purposes. These platforms are also capable of carrying high resolution cameras for surveillance and

reconnaissance tasks and be suitably modified to fit small explosives. Due to their ability to be operated from any open site and no requirement of expert piloting skills, illegal usages of Micro and Small RPAs pose major security concern for security agencies.

(c) **Medium and Large RPAs**. The Medium RPAs fall in weight category from 25 kg up to 150 kg. These RPAs have larger wingspans and can carry heavier payloads that can be utilised for reconnaissance and surveillance purposes along with weapon delivery by rogue operators. But these platforms require qualified pilot for operations. RPAs like Pioneer, Eagle eye, Hunter, Watch keeper RPAs fall in this category. The Large RPAs with AUW above 150 kg are used mainly for combat operations by the militaries and require large open areas/ semi prepared strips for operations. Examples of these large UAVs are Heron, Searcher, US General Atomics Predator A and B and US Northrop Grumman Global Hawk.

Image 3- Various types of Commercial Drones

3. Hence, while the illicit usages of drones up to Micro weight category is likely to be predominantly restricted to photography and surveillance purposes, drones from small to large category may also be utilised to carry explosive payloads along with advanced surveillance payloads depending upon their load carriage capabilities. However, with the growing technologies and low cost solutions, utilisation of much smaller platforms for delivering weapons in near future cannot be ruled out. Certain categories of drones which can be employed for targeting are as follows: -

(a) **Autonomous Drones**. These drones are controlled by onboard computers to navigate to a fixed target and don't require real time control by a human operator during flight. To avoid the jamming of drone-pilot data link and prevent detention of drone operator based on position fixing technology, these drones are likely to be widely utilised for targeting by ANEs.

(b) **Drone Swarms**. The swarm attack demonstrates a capability to simultaneously control and coordinate several intelligent drones, networked together, at one time using a GPS unit. These swarms can overwhelm any existing opposition by sheer numbers of intelligently-targeted warheads and smart weaponry.

Image 4- Drone Swarms aimed to saturate the Surveillance and Engagement System

(c) **Stealth Drones**. These drones are designed to reduce their radar signature and can be programmed to operate in patterns that make them difficult to detect. To evade acoustic detection, rotors of stealth drones might be modified to dampen a drone's engine noise.

4. There are numerous envisioned potential adversary goals, including smuggling, reconnaissance, electronic and kinetic attack, distraction etc for which drones can be utilised by state/ non state actors, few of which are as follows: -

(a) **Nuisance**. Such actions represent any interference with individual's privacy by silently monitoring and recording their surroundings or disturbing the public peace by resorting to irritating means. A more serious infraction caused by a drone is trespassing, or the illegal intrusion onto someone else's property.

(b) **Surveillance & Reconnaissance**. The relatively sophisticated drones with high resolution surveillance pods can be effectively utilized to collect intelligence data and for identification of exploitable vulnerabilities in critical infrastructure, government sites, businesses, and private citizens alike, from a sizable standoff distance, effectively preserving their anonymity from potential criminal investigation.

(c) **Airspace Interference**. UAS platforms present a genuine threat to safe airspace utilization. In addition to interfering with normal aviation operations, unmanned aerial vehicles may tend to disrupt law enforcement, or aircraft with the intended purpose of curtailing tracking, emergency response, or disaster mitigation capabilities.

(d) **Kinetic attacks**. Even without armaments, a drone is capable of causing damage or injury to people or property on the ground or in the air, thus exemplifying the lethal potential of UAS platforms. These platforms have the potential to deliver a lethal kinetic blow to soft targets, while having the cover of appearing as a result of accidental straying or negligent flying.

(e) **Payload Threat/Smuggling**. UAS platforms can also be exploited as a transportation mechanism for illegal contraband or cargo. Uses of these platforms allow terrorists or criminals to bypass traditional security barriers such as fences, walls, and detection measures.

(f) **Messaging**. Drones can be effectively utilised to convey signals and propaganda messages directed at both internal and external audiences. With deep penetration of social media, these propaganda means have been readily utilised by various terrorist organizations to generate disproportionate media and state attention.

(g) **Weaponised Threat**. UAS platforms can be deliberately constructed or modified by ANEs to carry and employ weapons and explosives due to the relative ease in which a UAS platform can be weaponised to produce devastating results. Armaments that can be added to UAS platforms vary widely from incendiary or explosive devices to carefully engineered projectile systems.

(h) **Weapons of Mass Destruction (WMD)**. Drones can be effectively utilised as a delivery system for Chemical, Biological, Radiological, and Nuclear (CBRN) substances. These platforms could easily bypass traditional security measures and can cause mass casualties without the need for precision flying.

(j) **Electronic Attack**. A rogue drone can potentially be utilised as platform to commit an electronic theft of personal/ classified information by digitally hijacking Smartphone's/ PCs wireless signal. In addition, these platforms can also be utilised to electronic attack friendly Electromagnetic emissions with an aim to interrupt operations.

CHAPTER- 3

POTENTIAL THREAT SCENARIOS: ROGUE DRONES

1. The usage of drones for creating nuisance, conducting reconnaissance mission, making propaganda videos and to target military forces in various countries have been observed since long back which has varied in magnitude and end results. With the advancements in platform structure, payload technology and miniaturization of various components, the threat spectrum seen today is likely to aggravate further in future. However, for better understanding of likely threat scenarios in Civil and Military parlance, a case study comprising of two levels of drone threats ie Tactical and Operational and policy responses in each one of them are being deliberated in succeeding paragraphs.

Single UAV- Human controlled

2. Utilisation of single UAV under control of a drone pilot to attack selected targets have already been carried out by terrorist outfits like Al Qaida and IS in recent past by utilizing COTS technologies. Three likely scenarios which may be expected during such an attack by extremist group are as follows: -

(a) **VIP Targeting**. In this scenario variant, a low and slow flying drone may be utilised for targeting a VIP or group of human targets. Extremist groups may resort to detail intelligence gathering and surveillance to ascertain the desired target and time frame for execution of such attack. The ANEs may be in position to retain real time situational awareness utilizing the video link which may be subsequently utilised as propaganda means.

(b) **Crowd Targeting**. A drone can be flown into crowded places like sports stadium, mass congregations, political rallies etc with an intention to detonate among them to generate panic and create a stampede and/or crowd crush-type situation. Terrorist may resort to follow-on drones, even if unarmed, to create the illusion of a coordinated attack for terror generation purposes.

(c) **Aircraft Targeting**. In this possible scenario a single human operated UAV could be utilized to target commercial airliners or military aircraft during most vulnerable takeoff or landing stage to simulate a "bird strike" on an aircraft engine. As no explosive or form of armament would be required for such an attack, the pre-existing COTS capability can be employed by the ANEs without any modification.

3. **Response Mechanism**. All the scenarios mentioned above may be part of terror act undertaken by an individual or group. Hence, the impact of such attacks may be generally viewed as an immediate domestic security issue, based on the likely intent, requiring enhanced force protection and counterterrorism operations by security agencies and defence forces. To prevent such incidents from taking place, all concerned law enforcement and security agencies will be required to develop drone detection and neutralization capabilities along with strict enforcement of regulations pertaining to operations of civil drones to dry out all logistics support required for operations of such drones. Stringing up wires to stop access into open venues or in flight choke points may prove to be other hasty anti-drone protocols that may need to be considered if hostile UAV use becomes evident in an area of operations.

Group of UAVs— Human Controlled or Autonomous

4. This level of impact is insurgency environment focused and pertains to the use of groups of human controlled and semi-autonomous UAVs on combat forces. Due to existing technological and operational limitations in execution of such a co-ordinated attack by miscreants, the scenarios mentioned below are much more likely a near futures issue: -

(a) **Human Controlled UAV Squad**. In this scenario, a UAV squad composed of armed drone swarms, synchronized through single/ multiple controllers can be utilised to attack soldiers and security personnel by detonating the IEDs once they come into the proximity of their targets. The drones can be further modified to carry shaped charges or Explosively Formed Projectiles (EFP) for the precision targeting of military armored vehicles. The armed drone squad can be utilized to target adversary forces in a stand-alone mode or in co-ordination with human insurgent fighters/ regular army.

(b) **Autonomous Drone Squadron**. Such a squadron represents a small group of autonomous armed drones launched together in an assault wave. The drones can be sent against security forces and military personnel located within a designated area. The drones

could be provided with GPS fencing instructions to patrol within certain physical boundaries and target humans and/or moving objects that they come across using human form or motion sensors.

5. **Response Mechanism**. The direct implications of this scenario are at the military operational level in which groups of drones serve as potent weapons being controlled by humans, or machine soldiers controlled by onboard autonomous systems. In view of the magnitude of the effort required to co-ordinate and execute such attacks, this task is unlikely to be executed by a small group of terrorists. Hence, this scenario focuses on generation of combat power in force-on-force engagements, predominantly in combat zones. Defence services will be required to undertake measures like capability enhancement and conduct of regular exercises to cope up with this kind of threats.

6. In both the scenarios mentioned above, modeling of the technical capabilities of possible category of rogue drones, which are likely to be used against a particular target system and the likely human factors, becomes necessary in addressing new threats posed by drones. Ideally, it's based on observed data from known threats, which can be accomplished by studying similar incidents and filling in the gaps with estimates as to how a drone can be used by adversary for malicious acts before a threat actor figures it out. So, engaging a red team assists in being better prepared for what the real rogue elements might bring to the fight.

CHAPTER 4

DRONE REGULATION MEASURES IN INDIA

1. The UAS market in India is projected to touch US$ 886 million by 2021, while the global market is likely to touch US$ 21.47 billion. In order to accelerate growth in the sector, India is required to support its domestic drone industry and lay out comprehensive plans for safe integration of UAS into the national airspace. Further, there is need to formulate regulations for channelising of drones in our environment to prevent exploitation of our vulnerabilities by our adversaries. Towards formalising the operations of Civil Drones in India, Directorate General of Civil Aviation (DGCA) promulgated the Civil Aviation Requirements (CAR) on 'Operation of Civil Remotely Piloted Aircraft System' (also referred as Drone CAR 1.0) under the provisions of Rule 15A and Rule 133A of the Aircraft Rules, 1937 that took effect from 01 Dec 18. As per the existing guidelines, all civil drones in India are required to be registered with DGCA through "Digital Sky (Digisky) Platform". However, the registration of drones imported or locally procured prior to implementation of the CAR remains an issue to be addressed.

2. The Digisky platform is aimed to create a seamless and secure technology and regulatory framework to integrate the civil drones into the Indian airspace through complete digital and paperless registration and approval process. The platform ensures that every RPA has an identified operator allowing end to end traceability, accountability, traffic management which forms the foundation for issuance of Unique Identification Number (UIN) and Unmanned Aircraft Operator Permit (UAOP). Digisky enables a proactive approach to enforcement of safety and security guidelines by ensuring that every RPA must obtain a valid digital permission in the form of 'No Permit, No Takeoff (NPNT)' for undertaking operations. NPNT requires all manufacturers to implement firmware & hardware changes that only allow flights as authorized by DGCA to physically take-off.

3. Based on the weight category and altitude of operations as specified in the CAR, Civil RPA operators or remote pilots are required to file a flight plan through Digisky web portal/ Mobile application. Under the present Digisky framework Indian airspace has been segregated under three categories for grant of permission for operations of civil drones. Operations of civil drones in the 'Green zones' require only intimation of the time and area of operation of the flights via the Digisky web portal or the mobile app. However, permissions from concerned airspace

regulator shall be required for operations of Civil drones in 'Yellow zones'. Certain vital installations under various Ministries and Central/ State governments have been earmarked as 'Red zones' which are synonymous to 'No Drone Zones'. The operations of civil drones in these areas are not permitted without specific authority from concerned agencies, on case to case basis. The Dynamic Zoning facility in Digisky portal allows regulators to respond quickly to security and safety needs by being able to limit permissions in areas where they may be sudden security, safety or privacy challenges.

4. Thus, CAR 1.0 provides a basic framework for regulating the operations of civil drones through enforcement of mainly procedural measures. Presently, Civil RPAs presently can be operated within Visual Line of Sight (VLOS) only, up to the height of 400 ft during the daytime (between sunrise and sunset). The interim period of limited operations of civil drones under Drone CAR 1.0 provides an opportunity to the Law enforcement and security agencies to identify our vulnerabilities and be prepared to handle larger threat spectrum with increase in civil drone traffic in India.

5. In accordance with the provisions of CAR, Ministry of Home Affairs (MHA) has also issued the Standard Operating Procedures for 'Handling threats from Sub-Conventional Aerial Threats' in Delhi area and Countrywide. The SOP lays down the procedures for detection, recognition, reporting and interception of unauthorized drones by concerned Security agencies, in co-ordination with the Indian Air Force. The Security agencies designated for protection of strategic installations have also been assigned with the responsibility for protection against sub-conventional aerial threats, utilising the available conventional weapons. The decision to fire on the rogue drone rests with the IAF/ Police / Specialized unit / Security agency deployed at the VAs/VPs based on the threat posed by the rogue platform. Both CAR and MHA SOP impose penal provisions against rogue drone operators under Indian Penal Code for any violations in the usage of drones.

Limitations of Response Mechanism

6. The air defence systems that have traditionally been used to protect airspace from manned aircraft are generally ineffective against drones. Military anti-aircraft radars are mostly designed to detect large, fast moving objects. As a result, they cannot always pick up small, slow, low-flying drones. Furthermore, since unmanned aircraft are cheap, it is impractical to use traditional anti-aircraft weapons, which can cost millions of Rupees per unit, to shoot them down. Furthermore, countering the evolving drone threats is a difficult challenge as different drone groups have different sizes, flight characteristics, capabilities along with performance parameters, mission, and vulnerabilities making the

characterisation of all types of threats difficult, in presence of sheer number UAS platforms. Hence, an effective Counter Unmanned Aircraft System (C-UAS) needs to address following challenges posed by drones: -

(a) **Detect and Track**. The C-UAS should be capable to detect and continuously track the small, slow, low drone which has following peculiarities: -

(i) Small Size/ Radar Cross Section
(ii) Minimal Infrared Signatures
(iii) Limited Radio Frequency and Electromagnetic Footprint
(iv) Low Altitude and limited Line of Sight operations
(v) Low Acoustic Emissions

(b) **Identify and Classify**. The Engagement planning requires quick and accurate identification and classification of targets which has inherent challenges due to;

(i) Difficulties in segregation between Friendly or rogue drones
(ii) Limited Database of Drone Signatures and Features
(iii) Discrimination between True vs False Targets
(iv) Less reaction time

(c) **Engage and Defeat**. Defeating rogue drones in timely, cost effective manner prior to completion of its mission remains a challenge for security operator due to;

(i) Possibility of utilisation of Standoff weapons from drones
(ii) Collateral Damage to friendly elements during neutralisation

CHAPTER 5

CHALLENGES WITH GROWTH IN CIVIL DRONE SECTOR

1. After the promulgation of Drone CAR 1.0, integration of drones into manned aircraft environment, Beyond Visual Line of Sight (BVLOS) and Autonomous Operations etc are logical steps forward. However, with the expected increase in drone operations for Civil and Commercial purposes in India, a Drone Ecosystem is required to be put in place to regulate the traffic, integrated these unmanned aircraft in manned aircraft environment while ensuring flight safety and security of our strategic installations. Therefore, increase in drone traffic will necessitate commensurate efforts from our airspace regulators like DGCA and IAF to acquire realtime detection and tracking capabilities.

2. Towards this, an automated UAS Traffic Management (UTM) system for low-altitude airspace may be devised to provide hyper-local and real-time information for managing UAS induced traffic. This approach would ensure that only authenticated UAS could operate in the airspace. The UTM architecture needs to have Surveillance, Navigation, Communication, Traffic de-confliction and Emergency assistance aids to regulate the drone traffic on real time basis. The implementation and regulatory framework for counter drone tech capability would be undertaken by MoCA. For the purpose of managing an efficient UTM system and to address the variable issues that may arise in UAS operations, the following capabilities need to be embedded in the UTM system: -

(a) **Detect and Avoid**. To avoid any inadvertent collision with manned aircraft and ensure separation between various platforms in time and space, the UTM system should assist in de-confliction with another aircraft, obstacle or danger, without the need for human intervention. Towards this, Detect and Avoid equipment needs to be integrated in all drones, except Nano category.

(b) **Dynamic Re-routing**. Artificial Intelligence (AI) may be integrated in the UTM system to perform tasks of dynamic re-routing and de-confliction, in an automated manner to enable the utilization of all available airspace capacity on real-time basis. For positive identification of all drones feasibility of fitting miniaturized SSR transponder (Mode 'C' or 'S') or ADS-B OUT equipment on all drones, except Nano, may be explored.

(c) **Geo-fencing**. To prevent any inadvertent or intentional straying towards notified vital installations, dynamic Geo-fencing may be implemented in two ways viz. Trajectory based where the UAS may operate only along permitted trajectory in the airspace and Area based where UAS can operate in a permitted area in the airspace. The Geo-fencing equipment presently required for drones (except Nano) for operations in only Controlled airspace in CAR 1.0, needs to be extended to all type of airspace to prevent entry into vital installations.

3. Further, to ensure effective integration with the UTM system, all UAS manufactured, imported or operating in India, must be equipped with appropriate navigation and communication software and hardware to allow for live telemetry and other data exchange with UTM service provider. The UAS must allow for operational command to be transferred to UTM service provider, at any time during and be capable of executing manoeuvres as instructed by the UTM service provider, in real time, including adjusting attitude, velocity and performing emergency landings or return to home procedures.

4. The capability building measures and associated infrastructure shall act as deterrent for any drone operator willing to undertake illegal activities. However, the willful offenders and extremist groups, willing to target vital installation/ personnel/ aircraft, can only be deterred by deploying Counter UAS infrastructure at vital target systems. Towards this, the airspace regulators and security agencies shall be required to enhance capabilities to track, detect, identify and engage hostile drones in real time.

CHAPTER 6

DEFENCE MECHANISM AGAINST ROGUE DRONE THREATS

1. To counter the misuse of drones, the security agencies will be required to execute "an integrated system of detection, delay and response" to achieve 'Defence in Depth'. The Counter Drone infrastructure needs to adopt diversified defensive strategies so that if one layer of defence turns out to be inadequate, another layer of defence takes over to prevent a full breach. Universally, five concentric circles of Prevention, Deterrence, Denial, Detection, Interruption and Destruction are followed as broad defence strategies.

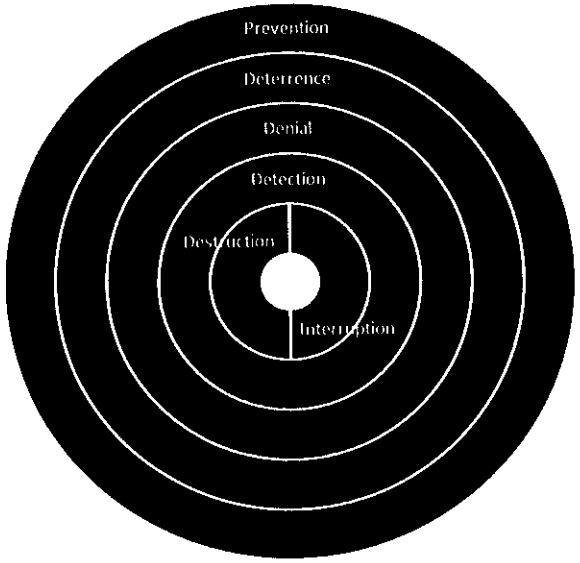

Image 5: UAS Defence in Depth Model

2. The terms Prevention, Deterrence and Denial are mostly enforceable through procedural means, notification of guidelines or promulgation of regulations. However, Detection, Interruption and Destruction are active measures as part of Counter Drone capabilities with the security agencies. The actions required to be undertaken for executing each layer is as mentioned in succeeding paragraphs.

Procedural Means

3. **Prevention**. Being the outermost layer of the defence bubble, prevention is the first activity to counter any rogue drone threat. Existing air defence radars have limitations against terrorist mini UAVs, this is where the challenge exists for the state. Hence, the most important layer of Counter drone defence lies in preventing a UAS attack. Pre-emptive investigation by law enforcement agencies and intelligence collection efforts remain the effective mechanism for dealing with the threat of terrorist UAVs. Under such circumstances, the role of actionable intelligence becomes very important. Supplementing intelligence and pre-emptive investigative activities, to curtail adversary access to heavy payload or long-range UAS platforms is also a key element of prevention activities.

4. **Deterrence.** The second layer of UAS threat defence lies in the deterrence of UAS attacks. Towards this, there is a need to equip security agencies to develop and deploy a concerted C-UAS defence. There will also be a need for establishment of robust legal framework for delivering prompt civil and criminal penalties to offenders to deter illegal UAS usages. In addition to legislative deterrence, promulgation of 'No Drone Zones' shall also act as deterrent against illegal access by rogue UAS platforms in sensitive areas.

5. **Denial.** The third layer of UAS threat defence encompasses all passive security measures to thwart the use or effectiveness of drones in conducting illegal activities or terrorism. Passive security measures like Camouflage, Concealment and Deception provide an ideal security mechanism for averting UAS threats, since many such measures are inexpensive and relatively easy to implement with advanced planning. In addition, the physical environment of protected asset along with unpredictability and randomness in employment of security measures also act as effective tools to deceive planned terrorist attacks. Geo-fencing can be considered as one of such methods to deny entry to the craft within the confines of pre-established virtual boundaries.

Active Means

6. **Detection.** In the event of failure of passive defence mechanisms to prevent, deter, or deny a UAS threat, active defence mechanisms are required to be employed. Rapid detection or early warning of the UAS, identification of the threat, and subsequent telemetry tracking assists in employment of weapons or other active defence means. Mix of technologies are being utilised as part of the Counter Drone Systems which include active means like Primary radars. Passive detection systems use sensors that sample the electromagnetic spectrum within certain wavelengths to determine the presence of UAS-characteristic signals including visual, acoustic, thermal/infrared, and UAS communications/control frequencies.

7. **Interruption.** Also termed as the Soft Kill measures, Interruption is a component of defence mechanism designed to avert a rogue UAS from carrying out an adverse action. Interruption can be carried out in one of three ways: operator interruption, jamming, and spoofing. The most obvious method of UAS interruption is to locate and identify the UAS operator and either forcibly compel the operator's compliance in removing the UAS threat or assuming direct control of the UAS.

8. **Destruction.** Destructive defence measures are employed with the sole purpose of eradicating a threat UAS platform and are also referred as Hard Kill measures. This defence mechanism can be implemented using a wide variety of means including projectile weapons, directed energy weapons, guided munitions, and interception. Destructive weapons should be used as a last resort, as the airborne destruction of a UAS threat can potentially cause collateral damage by falling debris, falling weapon projectiles, field of fire obstructions, scattered Nuclear Biological Chemical (NBC) elements (if part of the payload) etc.

CHAPTER 7

COUNTER DRONE TECHNOLOGIES

1. Counter-drone technology, also known as Counter-UAS (C-UAS) or Counter Drone technology, refers to systems that are used to detect and/or intercept unmanned aircraft. Counter-drone technology has already seen extensive use in civil arena and combat zones including base protection, airspace protection at airports, security during large events and major sports gatherings, VIP protection etc. In India C-UAS systems have been routinely employed during Independence Day and Republic Day celebrations in Delhi. Various components of C-UAS systems are explained in succeeding paragraphs.

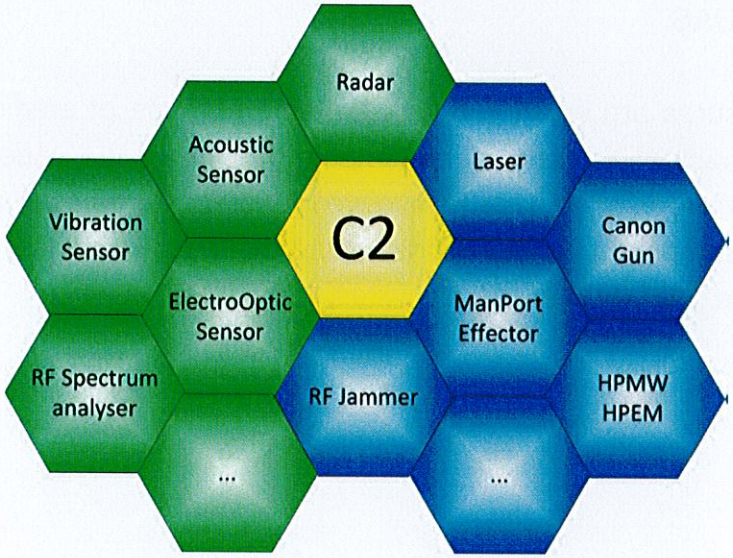

Image 6: General components of C-UAS Systems

2. **Detection**. Early detection and identification is the key to effective neutralization of the UAV threat which can be undertaken by a combination of sensors. However, during various trials it has emerged that utilisation of sensors in complementary manner can improve the UAV detection and identification abilities. Some of the detection and identification systems being employed in modern C-UAS systems are as mentioned below: -

(a) **Radar**. Unlike conventional Air Defence (AD) sensors, Radar detection algorithms in C-UAS systems are specifically tuned to detect small targets in the presence of false returns like clutter. These systems are known to pick up drones of the size of small birds using very low transmitted power. The detection ranges varies with the size of RPA platform.

(b) **Electro-optical/ Infra Red**. EO/IR sensors monitor for drones in the visible light and infrared (thermal) spectrum, either with an operator watching the video feed or specially designed automated algorithms. While the visible imaging includes possibility to distinguish between a UAV, birds, or any other object in the sky the Passive thermal imaging results in reduction of background signal noise, enhanced night time detection and less susceptibility to weather degradations.

(c) **Radio Frequency**. Most drones employ radio link between the drone and operator on the ground. External properties of the data link's signal can be used for position approximation of the drone and operator. With access to the data link's internals, more detailed information like drone's exact position and possibly where it's going can also be ascertained.

(d) **Acoustic Sensor**. These set of sensors detect specific noise signatures created by UAV motors and propellers. However, these sensors have limited range, they rely on matching registered acoustic sensors to a database of known UAV signatures and suffer from high nuisance alarm rates (especially in urban environments).

(e) **Passive Coherent Locator (PCL) System**. Passive Coherent Location (PCL) is a passive radar system, which utilises third-party transmitters in the environment like Television terrestrial broadcasts, FM Radio or Mobile Telephony to detect a target and provide location, heading and speed information of the object. A PCL system is capable of detecting extremely small signal changes scattered by micro drones, which are produced by an interaction of the transmitted signal of opportunity and the target.

3. **Interception**. The broad definition for response and neutralization is denial of mission, including destruction of the UAV target. The options for response range from diverting the UAV in a different direction, capturing it, or to destroying it broadly categorized into two main groups of "nondestructive" and "destructive". The neutralization measures being utilized by C-UAS systems is as mentioned below: -

(a) **Kinetic Kill**. ***Kinetic Kill*** is currently the most relied and preferable option for neutralising rogue drones. The response options can range from shooting down with sniper rifles, to anti-aircraft guns and missiles and even deploying fighter aircraft, depending on the situation. However, this mode of engagement of rogue aircraft demands a high level of skill and expertise on the part of the shooter.

(b) **High Power Electromagnetic Weapons (HPEM)/ Lasers**. HPEMs/ Lasers can be used in both detection by way of scanning and neutralisation, with high energy beams focused on the drone to physically burn the drone or a part of it. However, lasers are affected by adverse weather conditions, such as clouds, rain, fog and can pose a hazard to humans and the surrounding infrastructure; and difficulty of keeping the laser focused on a fixed location on the UAV.

(c) **Radio Jamming**. ***Jamming*** is a much safer option than kinetic kill but is a tricky one as modern UAVs are specifically encrypted to withstand these very attempts. To accomplish this, the target UAV should be identified and then targeted with an electromagnetic signal strong enough to overwhelm the system's controls. Depending on the drone and flight conditions, this may force the drone to land itself immediately or return to its home point.

(d) **Spoofing**. ***GPS Spoofing*** is an effective option for neutralising a hostile drone as it not only removes the threat but also gives access to the adversary's technology intact for analyses. In this, the drone is essentially confused to forget its waypoints and go into auto-pilot mode and in this stage using power transmission; it is directed to obey new commands.

(e) **Drone Capture Nets**. Capture nets can be used from the ground as well as a hunter-killer drone. The net encompasses the drone and causes it to cease flying by disrupting the propulsion system. The net-drone bundle then falls to the ground. However, ranges of these capture nets are limited, so the ability to engage the hostile drone at standoff distances from the target is very important. Variants of this system like Drone-on-Drone and Bird-on-Drone are also used to bring the rogue drone down.

4. A suggestive summary of technological needs to improve the detection, delay and response functions of security systems to vital installations against threats from rogue drones is as enumerated below :-

Potential UAV Threat	Detection	Delay	Response
Reconnaissance	- Early detection and identification is needed - Detection capability for small UAVs is needed	-Effective Geofencing needed as the primary delay mode	- 'Non Destructive' response is preferred for further analysis of the UAV and identifying its operator
Smuggling	-Detection means for the presence of payload are needed	-Effective Geofencing needed as the primary delay mode	- 'Non Destructive' response is preferred for further analysis of the UAV, its payload and for identifying its operator
Kinetic Attack	-Detection of larger UAVs required -Detection of gliding UAVs required	- Physical means of delay are needed	- 'Destructive' response is preferable to disable the threat at the safe distance from facility
Electronic Attack	-Additional means for detection of EM payload needed	-Effective Geofencing needed as the primary delay mode	- Both 'Destructive' and 'Non Destructive' response options are needed, choice depends on the severity of attack
Distraction	-Early detection and identification is needed -Detection capability for small UAVs is needed	-Effective Geofencing needed as the primary delay mode	- 'Non Destructive' response is preferred to further analysis of the UAV and identifying its operator

5. **Challenges to C-UAS Systems**. As the unmanned aircraft systems market expands, counter-drone systems will be required to be capable enough to detect and neutralize a growing variety of targets, ranging from large unmanned aircraft to low-flying micro surveillance drones. Further, with the increase in legitimate civil drone operations, differentiating between legitimate and potentially threatening drones is

likely to be a big challenge for C-UAS operators. An effective C-UAS system must be able to tell the difference between those drones and a single rogue drone that is operating with malicious intent to avoid fratricide.

6. Further, the advancements in Drone technology will try to outperform the C-UAS technology. In future, Drones might be programmed to operate in patterns that make them difficult to detect. Counter-laser systems could protect drones from directed energy attacks. Finally, forces might seek to deploy drone swarms, which present a range of vexing technical challenges from a C-UAS perspective. Hence, the C-UAS technologies will therefore have to constantly respond to new advances in unmanned aircraft technology to provide better solutions.

CHAPTER- 8

COUNTER ROGUE DRONE DEPLOYMENT PLAN

1. The level of security cover required against drones is expected to be at variance with conventional aerial threats like fighter aircraft due to disparity in weapon carriage capabilities of both platforms and quantum of air effort required to achieve comparable results. Further, the impact of attack by Small/ Medium class of drones on permanent concrete target system is expected to be lesser than any conventional attack and hence, such actions may be attempted for drawing public attention and generating sense of insecurity. However, the impact of drones with manned aircraft and armed attack at places of mass gatherings are likely to generate disproportionate results. Hence the deployment of C-UAS systems for protection of vital assets is considered necessary.

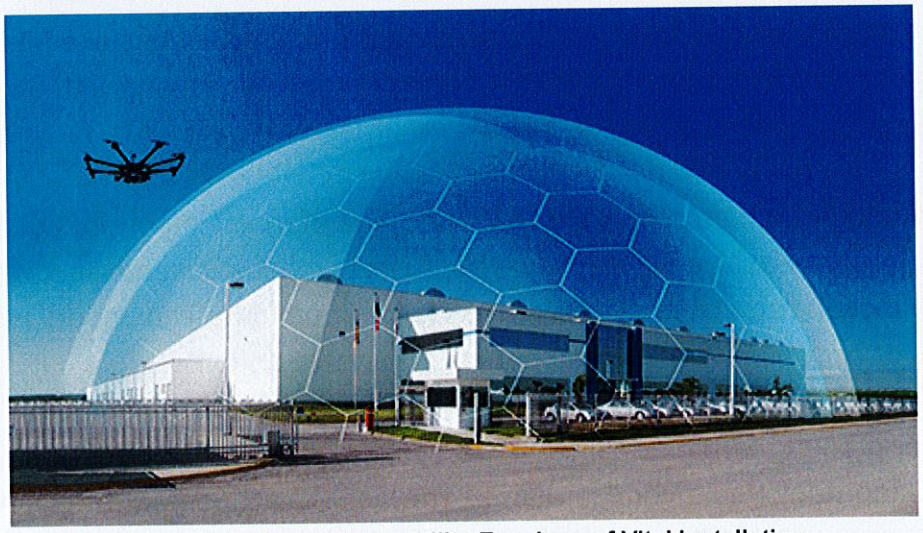

Image 7: Notional Vulnerability Envelope of Vital Installation

2. The strategic installations differ from state to state and place to place based on their geographical condition, criticality and construction type. In view of the requirement of numerous C-UAS systems for protection of strategic installations in the country, a realistic vulnerability analysis of identified VAs/ VPs by specialist security agencies based on Impact assessment from different category of drones, natural camouflage and local security scenario etc needs to be conducted by MHA and State Home Departments to finalise the requirement of C-UAS protection. However, collateral damage to own assets due to employment of C-UAS measures needs to be adequately deliberated. A suggested C-UAS deployment model is as mentioned below: -

(a) **Full Scale Model.** This model is considered necessary for protection of VAs/VPs of critical national importance like Rashtrapati Bhawan, Parliament House, Nuclear Installations, Major airports etc. This C-UAS model could consist of Primary and Passive detection means like Radar, Radio Frequeny (RF) detectors, Electro Optical (EO)/ Infrared (IR) cameras etc. In addition, Soft Kill (RF Jammers/ GPS Spoofers) and Hard Kill measures (High Power Electromagnetic weapons, LASERs, Drone Catching nets etc) may also be considered.

(b) **Mid Segment Model.** The Mid Segment Model can be considered for installations like Metro Airports, Oil Refineries, Ports and Power plants etc. This model could consist of Primary and Passive means for detection along with Soft kill measures. The Kinetic weapons of forces protecting the VA/VP along with Drone catching nets could be utilised for hard kill.

(c) **Basic Model.** The Basic models could be considered for State Secretariats/ important official premises, Monuments of National Importance etc. This model could consist of Passive RF detectors as primary means of surveillance along with Soft kill measures. Kinetic weapons of the force protecting the installation could be utilised as Hard kill options. This model would not have detection capability of autonomous drones, in the absence of control link but would be most affordable option.

3. Security Agencies may also consider procurement of Mobile C-UAS systems to cater for Event based deployments. The Mobile system could consist of Vehicle mounted and Rooftop deployable configurations. The actual requirement of C-UAS systems would be required to be worked out by concerned Security agencies in consultation with the System OEMs depending upon the dimension of the VA/VP, terrain specifications and other security considerations.

CHAPTER- 9

INSTITUTIONAL SETUP FOR COUNTER DRONE MEASURES

1. Multiple departments and agencies have responsibility for the safety or security of installations, facilities and operations that may be vulnerable to threats posed by rogue drones, including the Ministry of Defence, Ministry of Home Affairs, Ministry of Civil Aviation, Ministry of Law and Justice, Department of Atomic Energy etc. In addition many departments and agencies also perform important operations that may be vulnerable to threats posed by UAS which includes tasks varying from Search and Rescue operations, Medical evacuations, Law and Order maintenance, Surveillance during National Events, emergency response etc. Hence, a coordinated approach is critical to ensure that development and use of technical countermeasures for detecting and mitigating rogue drones is consistent with the safety and efficiency of Indian airspace, security of VIPs and vital installations and protection of privacy/ data etc.

2. Indian Air Force is responsible for Air Defence of entire Indian air space. However, in view of involvement of multiple agencies for protection against sub-conventional aerial threats, an apex multi-agency Sub-Con regulatory body, with IAF as lead service shall be constituted at national level.

3. **Steering Committee**. This Committee shall act as the apex Nodal body to evolve Counter rogue drone framework and implementation mechanism at national level. The role of steering committee shall be as follows: -

(a) Formulate guiding principles for Vulnerability analysis and security classification of vital installations from Sub-con aerial platforms.

(b) Recommend concerned Ministries for deployment of suitable C-UAS measures at vital installations based on security considerations.

(c) Regulation of commercial civil drone applications in accordance with security scenario in the Country.

(d) Co-ordinate with DGCA/ AAI for capability building towards real time monitoring of drones along with enforcement of airworthiness and safety norms, pilot certification mechanism and maintenance practices for Civil drones.

(e) Monitor and track the developments in the fields of drones and C-UAS technology and co-ordinate with R&D organisations for indigenous development.

4. The composition of the Steering Committee shall be as follows:-

(a) Indian Air Force

(b) Ministry of Home Affairs (comprising of nominated reps from NSG, CAPFs/ State Police)

(c) Ministry of Civil Aviation (comprising of reps from DGCA/AAI)

(d) Intelligence Agencies (comprising of NTRO, IB)

(e) Reps from DRDO/ R&D organizations.

5. **Implementation Committee**. The Steering Committee will be assisted by an Implementation Committee for regular monitoring of sub-conventional threat environment and implementation of Counter-drone measures at VAs/VPs at National and State level. The role of the Implementation Committee shall be as follows: -

(a) Co-ordinate for implementation of Counter Drone framework at national and state level.

(b) To oversee procurement and deployment of C-UAS at vital assets.

(c) Updation of central C-UAS threat/ signature library.

(d) Management of shared catalogue of approved C-UAS systems.

(e) Implementation of best practices in a unified and co-ordinated manner.

(f) Training of Security agencies on Air Defence procedures for handling drone threats and optimum employment of Counter drone systems.

(g) Co-opt members from reputed R&D organisations, academia, drone industry etc in evolving new tactics and technologies.

6. The composition of the Implementation Committee shall be as follows:-

(a) Ministry of Defence (comprising of reps from IAF, IA and IN)

(b) Ministry of Home Affairs (comprising of reps from CAPFs & State Police)

(c) Ministry of Civil Aviation (comprising of reps from DGCA/AAI and BCAS)

(d) Invitees from Academia, Drone industry on as required basis.

7. For regulating civil drone traffic in India and effective handling of threats from rogue drones the following steps may be undertaken:-

(a) A multi-agency Drone regulatory body with two committees - Steering Committee & Implementation Committee. The committees would be responsible for formulation of Counter rogue drone framework and implementation mechanism along with co-ordination for deployment of Counter-drone measures at VAs/ VPs, based on their vulnerability.

(b) Infrastructure development by airspace regulators for real time monitoring of drone flight utilizing Cloud based server/ UTM system. The architecture should enable real time sharing of necessary information/ details with the law enforcement agencies for effective implementation of law and order in the place of operation of the drones.

(c) Implementation of stringent airworthiness criteria and Drone Pilot training along with certification mechanism by DGCA for ensuring safe operations in BVLOS and dense air traffic scenario.

(d) Registration of drones as well as the vendors that are selling the imported/locally manufactured drones within country. Prior to implementation of Drone CAR, a provision for one time voluntary disclosure would be permitted. However, the registration of drones shall be subject to compliance with all existing safety provisions laid down by DGCA.

(e) Vulnerability analysis of identified VAs/ VPs by security agencies based on Drone Impact assessment by different category of drones, natural camouflage and local security scenario etc to be conducted by MHA and State Home Departments to finalise the requirement of C-UAS protection.

(f) Security agencies designated for protection of respective VAs/ VPs will continue to be responsible for protection of these assets from sub-conventional aerial threats, including drones. The security agencies may deploy suitable C-UAS models for protection of VAs/VPs, based on threat analysis.

(g) A central C-UAS threat/ signature library and management of a 'shared' catalogue of approved C-UAS systems in a unified and coordinated manner among all stake holders to adopt synergized procedures.

(h) Carrying out operational trails of C-UAS systems, prior to deployment at VAs/VPs, so as to rule out any possible interference with Communication, Surveillance, Navigational aids and collateral damage to friendly assets.

(i) Preparation of VA/VP specific Counter Drone SOPs by all Security agencies for neutralisation of rogue drones. This SOP would be vetted from concerned ministries for optimal utilisation of C-UAS systems and avoid fratricide.

(k) A legal framework for authorized use of C-UAS systems by Security agencies for protecting vital assets, safeguarding manned aviation, supporting law enforcement activities, protecting national borders and conducting operations.

(l) A well designed phase-wise training capsule for civil security personnel on detection, identification, reporting and engagement procedures of drones.

(m) Utilisation of IA and IN AD training establishments to broaden Sub-con training infrastructure. Engagement of retired IAF Air Defence Safety Operators for training personnel from all relevant agencies on handling sub-con aerial threats.

(n) Periodic interaction between security agencies, R&D Organizations and OEMs for upgrading operational requirements according to technological innovations so as to be at par with futuristic threats from Sub-Conventional aerial platforms, refining of security procedures and deriving best practices.

CHAPTER- 10

LEGAL PROCEDURES TO HANDLE ROGUE DRONES

1. With the increase in civil application of drones after promulgation of Drone CAR 1.0, the vulnerability of our vital assets from reckless or hostile drones has considerably increased requiring law enforcement and national security agencies to control access to sensitive airspace and interdict threatening drones. As a procedural measure, Drone CAR 1.0 provides for penal action against offenders for breach of compliance to any of the requirements and falsification of records/ documents including imposition of penalties as per applicable IPCs (such as 287, 336, 337, 338 or any relevant section of IPC). The MHA SOP on 'Handling of Threats from Sub-conventional Aerial Platforms' in Delhi and Countrywide also lay down penal provisions for prosecuting the offenders under relevant sections of IPC. In addition, the security personnel deployed for protection of strategic installations are only authorised to neutralise rogue drones utilising their kinetic weapons, if identified as targeting vital installations/ committing hostile acts.

2. In most countries, signal jamming devices for RF and GPS jamming and seizing control of aircraft, including the more advanced directed systems and other Kinetic and non-Kinetic means for interception of drones are either illegal or restricted. There are many legal issues surrounding this area which make the development, testing, marketing, and using of counter drone technology problematic. With the need felt for utilisation of C-UAS platforms for targeting rogue drones, the U.S. Congress in December 2016, passed the National Defence Authorization Act of 2017 (NDAA) which created brand new sections on counter UAS in Title 10 and Title 50 of the United States Code. In October 2018, the FAA Reauthorization Act of 2018 was passed which gave the Secretary of the Department of Homeland Security, Department of Justice, and the United States Coast Guard authority to counter rogue drones.

3. As the drone industry continues to expand in India, it is essential that necessary legal provisions are framed to authorize the designated law enforcement agencies to protect the public/vital assets from rogue drones. The legislation shall contain safeguards to ensure that the use of Counter-UAS authority will be risk-based and coordinated closely among relevant departments and agencies to mitigate adverse impacts to the safety, efficiency and accessibility to the Indian airspace to the maximum extent feasible. Further, the provisions need to be consistent with public

safety, law enforcement and internal security requirements. Legal authority to be extended to designated law enforcement agencies against rogue drones as mentioned below: -

(a) Without prior consent, carry out detection, identification, monitoring, and tracking the unmanned aircraft system or unmanned aircraft utilising all possible communication/ data links.

(b) Warn the operator of the unmanned aircraft system or unmanned aircraft, including by passive or active, and direct or indirect physical, electronic, radio, and electromagnetic means.

(c) Disrupt control of the unmanned aircraft system or unmanned aircraft, without prior consent, including by disabling the unmanned aircraft system or unmanned aircraft by intercepting, interfering, or causing interference with wire, oral, electronic, or radio communications used to control the unmanned aircraft system or unmanned aircraft.

(d) Seize or exercise control of the unmanned aircraft system or unmanned aircraft.

(e) Seize or otherwise confiscate the unmanned aircraft system or unmanned aircraft.

(f) Use reasonable force, if necessary, to disable, damage, or destroy the unmanned aircraft system or unmanned aircraft.

4. The legislation shall ensure that authorised members of the Armed Forces, Govt Departments, Security agencies and other appropriate persons designated by the heads of concerned department and agencies consistent with the requirements of the legislation will not face penalties for protecting these entities in a way that is consistent with other applicable laws in the country. In addition, officials should be given broader authority to engage in counter-drone operations to protect national security, safeguard manned aviation, support law enforcement activities, protect the border, and further other critical missions. The legislation shall also stipulate measures to ensure that detection and mitigation technologies are developed, tested, and deployed in a manner that minimizes adverse impacts on airspace access, as well as air navigation services, avionics, and other systems that ensure safe and efficient aviation operations.

5. **Insurance**. The legal framework shall also cater for adequate financial liability that might incur for any damage to third party resulting from the collateral accident/incident due to the employment of counter drone measures.

6. **Voluntary Disclosure of Drones**. As per available inputs, approx half million drones in India, imported to/ manufactured within India prior to promulgation of Drone CAR are still unregistered which pose a danger to the drone ecosystem. To induct these drones under legal framework, a provision for voluntary disclosure of such drones may be considered. However, registration of these drones by DGCA shall be subject to adherence to all safety provisions laid down in the existing CAR.

CHAPTER- 11

TRAINING REQUIREMENTS FOR SAFE DRONE OPERATIONS

Remote Pilot Training

1. A risk free environment for the commercial use of UAS and BVLOS operations would largely depend upon the operations of the UAS by the Remote Pilot. Therefore, to minimize the risks, it is important to ensure that all Remote Pilots have undertaken necessary certifications and practical training for operations of the UAS. Drone CAR 1.0 lays down the comprehensive training requirements for remote pilots, however, with the proposed expansion of commercial civil drone sector in India, formulation of commensurate training syllabus to enable BVLOS and night UAS operations along with setting up of adequate training infrastructure for remote pilots is considered necessary.

2. The training program for Remote Pilots should include teaching theoretical subjects intended to equip them with the similar knowledge as that of an aircrew of a manned aircraft or a private pilot license holder to enable the Remote Pilot to control the operation of a UAS under any and all circumstances. This would enable the Remote Pilots to control the UAS throughout its operating conditions, including safe recovery during emergencies and critical system malfunction as soon as practicable. All records in relation to the history of each Remote Pilot (such as number of flights, flight logs, occurrences - if any, training records, compliance records etc.) should be maintained and the same should be factored in while granting necessary clearances.

3. Remote Pilots having knowledge of any physical or mental condition that would interfere with the safe operation of an UAS should be prohibited from operating an UAS. To assess the fitness of a Remote Pilot for undertaking UAS operations, they should also be subject to similar conditions as applicable to the pilots of manned aircraft under the Aircraft Rules, 1934. Foreign nationals with remote pilot license from the relevant authority outside India must be required to obtain necessary certifications in India to operate UAS in the Corridor.

Training on Handling Drone threats

4. The Road Map for training of personnel from various Civil Security agencies has been finalized and included in the MHA SOP on 'Handling of Threat from Sub-Conventional Aerial Platforms in Country'. The personnel from security agencies including various Central Armed Police Forces, National security Guards, State Police, Coast Guard, Indian Army etc are being trained on aspects of Detection, Identification, Reporting and Engagement of sub-conventional aerial platforms including Drones, Para hang gliders, Micro light etc at IAF Regional Training Centres across India. To broaden the sub-con training infrastructure, training of Civil security personnel at IA and IN training establishments imparting Air Defence training (Army AD College Gopalpur & INS Dronacharya Kochi) within their respective states, under the IAF Roadmap of training may be incorporated.

5. With the induction of C-UAS equipments, the personnel would also be required to be trained by the concerned Original Equipment Manufacturers (OEM) on operational utilisation of all sub-systems. Further, the technical maintenance crew also needs to be trained for regular upkeep and maintenance of the C-UAS system. The feasibility of employment of retired IAF Air Defence System Operators by Central and State Law enforcement agencies for imparting training to their personnel on Sub-con training aspects may be considered by MHA and other nodal ministries.

6. In view of the advancements in drone technology the Sub-Conventional threat spectrum is likely to broaden to include threats from Drone Swarms and miniature weaponised drones that will aim to saturate and target our Surveillance systems. Towards this, regular interaction with various R&D organisations and OEMs is likely to provide an insight into integration of C-UAS systems into the existing Air Defence network and facilitate in developing Security models commensurate to our threat perceptions.

CHAPTER- 12

CONCLUSION

1. Drones/UAS are the emerging threats not only for the military but, also for the civil society. This could attain threatening dimensions when these carry out unregulated indiscriminate flying in the air space while being used by the civil government, businesses and hobby enthusiasts. Today, their destructive capability and threatening potential has become a challenge for the security providers. There is a need to regulate their use and identify and neutralize/ground those which threaten the national security and safety security of the civil society.

2. In view of the promulgation of Drone CAR 1.0, the civil use of drones is expected to grow manifold as unmanned vehicles offer the government and business sector a better, cost effective and efficient mechanism to deliver public benefits in much shorter time frame. However, with the increase in commercial drone operations, there remains likelihood of misutilisation of these platforms for nefarious activities by ANEs. As a procedural measure, IAF is in process of training the civil security personnel on Detection, Identification, Reporting and Engagement of rogue sub-conventional aerial platforms including Drones, while MHA has issued SOP for handling threat from rogue drones. However, in absence of positive means for detection and engagement of drones, the existing mechanism remains highly inadequate.

3. The incidents of utilisation of drones to target vital assets and personnel worldwide, pose very serious challenge for our national security and the quantum of threat is feared to increase further with advancements in drone technology. Hence, there is a requirement to establish a unified Drone regulatory architecture for undertaking concerted and coordinated effort to handle the emerging menace. Formulation of operational guidelines in consonance with the emerging commercial usages of drones, setting up of UTM, strict enforcement of airworthiness aspects, training and maintenance are expected to facilitate constructive applications of the platform. Besides, induction of C-UAS systems at identified VAs/VPs is considered necessary for timely neutralisation of rogue drones. Awareness among personnel, effective enforcement of legal framework and interaction with R&D organisations and academia are likely to assist in handling of any such threat.

ACRONYM

AAI	-	Airports Authority of India
AD	-	Air Defence
ADC	-	Air Defence Clearance
ADS-B	-	Automatic Dependent Surveillance - Broadcast
AGL	-	Above Ground Level
AI	-	Artificial Intelligence
ANE	-	Anti National Elements
ANS	-	Air Navigation Service
AUW	-	All Up Weight
BCAS	-	Bureau of Civil Aviation Security
BVLOS	-	Beyond Visual Line-Of-Sight
CAR	-	Civil Aviation Requirements
C-UAS	-	Counter Unmanned Aircraft System
COTS	-	Commercial off the Shelf
DEW	-	Directed Energy Weapons
DGCA	-	Director General Civil Aviation
DIY	-	Do It Yourself
EO	-	Electro-Optical
FAA	-	Federal Aviation Agency
FM	-	Frequency Modulation
GPS	-	Global Positioning System
ICAO	-	International Civil Aviation Organization
IFR	-	Instrument Flight Rules
IED	-	Improvised Explosive Devices

IPC	-	Indian Penal Code
IR	-	Infra Red
MHA	-	Ministry of Home Affairs
MoCA	-	Ministry of Civil Aviation
MoD	-	Ministry of Defence
NOTAM	-	Notice to Airmen
NPNT	-	No Permission-No Takeoff
NTRO	-	National Technical Research Organization
OEM	-	Original Equipment Manufacturer
PCL	-	Passive Coherent Locator
POC	-	Proof of Concept
PSS	-	Passive Surveillance System
PPL	-	Private Pilot License
RCS	-	Radar Cross Section
RF	-	Radio Frequency
RPA	-	Remotely Piloted Aircraft
RTC	-	Regional Training Centre
SOP	-	Standard Operating Procedure
SSR	-	Secondary Surveillance Radar
UA	-	Unmanned Aircraft
UAOP	-	Unmanned Aircraft Operator Permit
UAS	-	Unmanned Aircraft System(s)
UAV	-	Unmanned Aircraft Vehicle
UIN	-	Unique Identification Number
UTM	-	Unmanned Aircraft System Traffic Management
VA/VP	-	Vital Area/ Vital Point
VLOS	-	Visual Line-Of-Sight

DEFINITIONS

All up Weight Total weight of an aircraft with passengers, cargo, fuel, payload etc

Artificial Intelligence The theory and development of computer systems able to perform tasks normally requiring human intelligence such as visual perception, speech recognition, decision making, and translation between languages.

Combat zone The forward part of a theater of military operations extending from the front line to the forward boundary of the communications zone

Radio Frequency Link The data link utilising Radio Frequency between the Unmanned Aircraft and the remote pilot station for the purpose of managing the flight.

Controlled Airspace Airspace of defined dimensions within which air traffic control service is provided in accordance with the airspace classification.

Counter Drone Also known as **Counter-UAS**, C-**UAS** or **Counter-UAV** refers to systems that are used to detect and/or intercept unmanned aircraft.

Drone Corridor A segregated airspace defined by the appropriate authorities in consultation with the airspace designers to keep commercial UAS operations out of the non-segregated airspace in which manned aircrafts operate.

Geo-fencing A feature programmed in the software that uses Global Positioning System or Radio Frequency identification to define geographical boundaries.

Hard Kill Measures that physically counterattack an incoming threat thereby destroying/altering its payload/warhead in such a way that the intended effect on the target is severely impeded

Prohibited Area Airspace of defined dimensions, above the land or territorial waters of India within which the flights are not permitted at any time under any circumstances.

Radar Cross Section Radar Cross Section is the measure of a target's ability to reflect radar signals in the direction of radar receiver. A larger RCS indicates that an object is more easily detected.

Remote Pilot A person charged by the operator with duties essential to the operation of a remotely piloted aircraft and who manipulates the flight controls, as appropriate, during flight time.

Remotely Piloted Aircraft (RPA) An unmanned aircraft, which is piloted from a remote pilot station.

Remotely Piloted Aircraft System (RPAS) A remotely piloted aircraft, its associated remote pilot station(s), the required command and control links and any other components, as specified in the type design.

Restricted Area Airspace of defined dimensions above the land areas or territorial waters of India within which the flight of aircraft is restricted.

Rogue Drone. A drone behaving in ways that are not expected or not normal, often in a way that causes damage

Segregated Airspace Airspace of specified dimensions allocated for exclusive use to a specific user(s).

Soft Kill Electronic countermeasures that alter the electromagnetic, acoustic or other signature(s) of a target thereby altering the tracking and sensing behavior of an incoming threat (e.g., guided missile)

Unmanned Aircraft System (UAS) An aircraft and its associated elements, which are operated with no pilot on board.

Unmanned Aircraft System Traffic Management It is an air traffic management ecosystem under development for autonomously controlled operations of unmanned aerial systems (UAS).

Visual line-of-sight operation Operation in which the remote pilot or RPA observer maintains direct unaided visual contact with the remotely piloted aircraft.

Vital Area/ Vital Point A designated area or installation to be defended by air defence units.

REFERENCES

1. DGCA Civil Aviation Requirements on 'Operation of Civil Remotely Piloted Aircraft System (RPAS)'

2. Ministry of Civil Aviation 'Drone Eco System Policy Roadmap' January 2019

3. Ministry of Home Affairs 'Standard Operating Procedures on Handling Sub-Conventional Aerial Platform Threats in Country' issued on 10 May 19

4. Examining Unmanned Aerial System Threats & Defences: A Conceptual Analysis, International Journal of Aviation, Aeronautics, and Aerospace- Volume 2/ Issue 4, Embry-Riddle Aeronautical University

5. Terrorist and Insurgent Unmanned Aerial Vehicles: Use, Potentials and Military Implications, Robert J Bunker, Strategic Studies Institute, US Army War College

6. 'Analyzing the Threat of Unmanned Aerial Vehicles (UAV) to Nuclear Facilities' by Alexander Solodov, Adam Williams, Sara Al Hanaei, Braden Goddard