CENTRE FOR LAND WARFARE STUDIES

ISSUE BRIEF

No. 265 January 2021

Countering Malicious Drones: Analysing Regulatory Measures and Anti-Drone Solutions from an Indian Perspective

Soumya Nair is a Research Assistant at the Centre for Land Warfare Studies. She has earlier worked as a journalist with Asian News International (ANI), The Asian Age, and The Free Press Journal. Her research focusses on India's strategic neighbourhood in the East and South, Strategic Studies and Military Technology.

Key Points

- Proliferation of drones and multiple instances of their misuse has heightened the need to develop and field effective counter measures to deal with malicious drones.
- Demand for drones has shot up globally, so has the anti-drone market which is currently estimated to be at $0.6 billion and is expected to increase fourfold by 2025.
- Civil Aviation Regulations (CAR) 2018 has laid down comprehensive regulatory framework for operating drones. However, a diverse country like India with varied challenges needs effective counter-drone systems as well to mitigate and manage risks from rogue drones.
- Counter-drone systems have immense challenges in terms of performance, research and development cost, legality and policy. The innovations clause of DAP 2020 can be explored through iDEX to encourage various start-ups and MSMEs in this field.

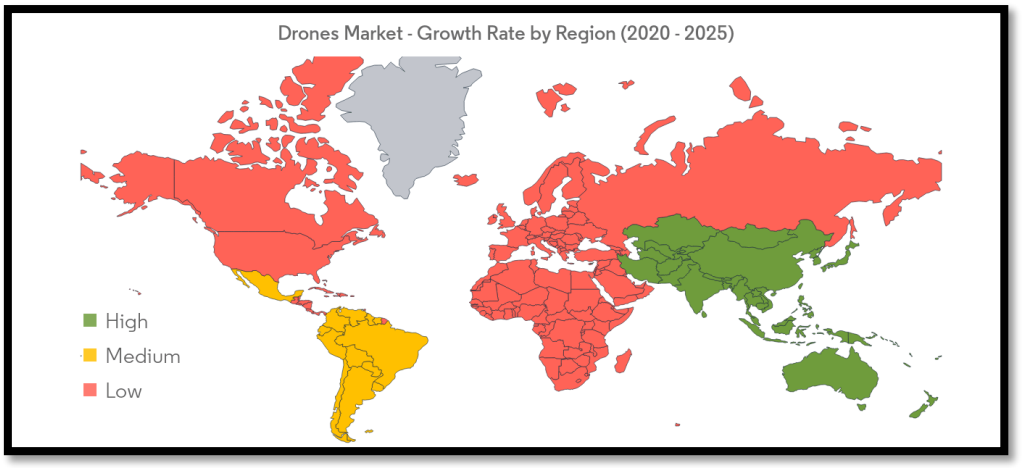
Introduction

Over the past 10 years, drones or Unmanned Aircraft Systems (UAS) or Remotely Piloted Aircraft (RPA) have evolved significantly from their military origins, proliferating into the commercial and civilian space as they find application across industries. Since the inception of the first commercial drone in 2010, they are being steadily adopted by businesses, individuals and government agencies for applications as varied as agriculture to healthcare owing to their easy availability, affordability and effectiveness for diverse purposes. As a result, the global drone market is booming and is expected to accelerate from USD 22.5 billion in 2020 to over USD 42.8 billion in 2025 at a compound annual growth rate (CAGR) of 13.8 per cent.[1] Every technology, however, has the potential for misuse and drones are no different. The proliferation of drones has thrown up new societal challenges to security and privacy of both individuals as well as organisations. The world has lately seen spectacular and innovative methods of utilisation of

drones by nations at war - as seen in the recent Armenia-Azerbaijan conflict[2], and by non-state actors and other suspicious entities – as witnessed in Syria or the ingenuous strategies being employed by Taliban to target Afghan government forces of late[3]. This has heightened the need for effective counter-drone systems to detect and neutralise rogue drones. So, even as drones proliferate, a new market for anti-drone systems is also growing rapidly as countries across the globe invest in developing and fielding counter UAS systems. Besides adoption of counter-drone technologies, there is a need to have a strong regulatory framework to mitigate the security, privacy and penetration risks posed by un-regulated drones. This paper examines the need for counter-drone systems, the UAS regulatory framework put forth by Directorate General of Civil Aviation (DGCA), and the pros and cons of available counter-drone technologies. It further discusses the challenges of developing effective anti-drone systems and way-forward from an Indian perspective.

Proliferation of Drones

Map 1: Drones Market – Growth Rate by Region (2020-2025)



Source: Mordor Intelligence [4]

As per a study by Mordor Intelligence (base year 2019), in the coming years, the fastest drone market growth will be seen in the Asia-Pacific (APAC) region [5] because of the burgeoning demand for drones, legalisation of UAS in these countries and global market players expanding their operations in this region.

In India, owing to growing awareness on the benefits and implementation of the technology, the commercial drone market has witnessed a steady growth in the last few years as varied sectors such as construction, railways, agriculture, oil and health industry, etc. have started making use of drones. The outbreak of COVID-19 has further augmented the need for drones in the country as they are being used for enforcing social distancing measures,

disinfection purposes and for contact-less delivery of medicines. Furthermore, the government's Make in India initiative encourages domestic manufacturing of drones which will provide further fillip to the commercial drone market which is projected to grow at a CAGR of 12.4 per cent during the 2020-2026 period. [6]

Why the Need to Counter Drones

One of the first high-profile drone misuse was reported in 2013 when a small quad-copter flew close to German Chancellor Angela Merkel at a rally before crashing on stage.[7] Similarly, in January 2015, a drone crashed into the lawns of the White House, official residence of the US President, after its operator lost control raising major security concerns.[8] In July 2018, terrorists claimed to have used armed drone to attack the international airport in Abu Dhabi.[9] In August the same year there was a failed assassination attempt against Venezuelan President Nicolas Maduro which left a few in the audience injured.[10] Closer home, in September 2019 it was reported that drones flew in from Pakistan a few times to airdrop a cache of arms, ammunition and fake currency which was seized in Punjab's Tarn Taran district.[11] A drone swarm attack was reported the same month on a Saudi Arabian oil facility.[12] As mentioned earlier, the October 2020 Armenia-Azerbaijan conflict saw armed and unarmed drones and loiter munitions wreaking havoc in the Nagorno-Karabakh region.[13] These incidents accentuate the potential disruptions and destruction that drones can cause.

Given their small size and speed – some can attain a speed of 65 km per hour with payload carrying capacity of 6 kg[14] - it is difficult to detect current generation drones, sometimes even by the most sophisticated systems as in the White House lawn case. They can be flown manually as well as automatically to areas up to 8 km from the operator's location.[15] The threats posed by drones can be categorised as given below[16]:

- ***Spying and tracking.*** When drones are used for spying and tracking activities that can compromise others' privacy, or to carry out reconnaissance and 3D spatial reconstruction of sensitive installations.
- ***Physical attacks.*** When drones are used to carry out physical attacks by collision or by dropping explosive payload or for smuggling.
- ***Cyber attacks.*** Using drones with requisite payload as cyber weapon to steal data, to wirelessly compromise access points, or to spoof any unsecured networks or devices.

To keep a check on drones from being used for any hostile activity, the first step is to have an effective regulatory framework to avoid its misuse. However, despite a sound framework,

the possibility of any malicious drone making an attempt to intrude into sensitive areas cannot be ruled out - hence the need for an effective counter drone system.

Regulatory Framework

In 2018 the Directorate General of Civil Aviation (DGCA) came up with the first set of norms for drones that operate in visual line-of-sight (VLOS) only during daytime and can fly at a maximum altitude of 400 ft. The set of norms, called Civil Aviation Regulations (CAR or CAR 1.0) 2018[17], regulates the use of drones in the Indian airspace and lays out details of safety and operational accountability measures like obtaining a Unique Identification Number (UIN), Unmanned Aircraft Operator Permit (UAOP) and other such operational requirements. As per the CAR, UAS are classified based on its maximum all-up-weight (including its payload) and also based on its threat and damage potential as Nano (up to 250 grams), Micro (250 grams to 2 kg), Small (2 to 25 kg), Medium (25 to 150 kg) and Large (over 150 kg).[18]

An online registry platform called “Digital Sky Platform” has been provisioned for registration of manufacturers and operators of drones which is important for implementing effective regulation. The Digital Sky Platform regulates all drones in the micro and higher categories. This platform allows operators to apply for a Unique Identification Number, akin to the registration plate of a vehicle, that needs to be issued for all drones (with the exception of the smallest category), and Unmanned Aircraft Operator Permit online for approval by the civil aviation regulator. The pilot also needs a remote pilot licence and should be trained by registered Flight Training Organisations (FTO). India has a ‘No Permission - No Takeoff’ (NPNT) clause for aerial unmanned objects, which implies that a drone cannot be operated in Indian skies unless the regulatory permission is received through the Digital Sky Platform. NPNT requires all manufacturers to ensure any change in firmware and hardware that only allows flights as authorised by DGCA to physically take-off. That means no drone will be able to fly without initially specifying details like its intended flight path, time of flight and pilot credentials. To ensure that operating risks are not just limited to drone type but also the airspace, the latter has been classified into three zones - no-fly zones (Red), some operations permitted (Amber) and all operations permitted (Green). The Digital Sky Platform provides online convenience for all permission requests and automates issuing of permissions in Green zones, thus significantly speeding up the process.[19]

The table below summarises the important operational and safety aspects outlined in CAR:

Table 1: Operational and safety aspects outlined in CAR 1.0

Category	Weight	UIN	UAOP	NPNT	Allowed Height	Security Clearance	Night Operations	Pilot Training
Nano	up to 250 grams	No	No	No	50 ft (above 50 ft not exempted)	No	No	No
Micro	250 grams to 2 kg	Yes	No	Yes	200 ft (above 200 ft not exempted)	Yes	No	No
Small	2 to 25 kg	Yes	Yes	Yes	400 ft	Yes	No	Yes
Medium	25 to 150 kg	Yes	Yes	Yes	400 ft	Yes	No	Yes
Large	over 150 kg	Yes	Yes	Yes	400 ft	Yes	No	Yes

Source: Adapted from DGCA Requirements for Operation of Civil Remotely Piloted Aircraft System (RPAS).[20]

Further, in January 2019, a white paper on drone ecosystem policy roadmap was released that outlined the proposal for CAR 2.0 aiming for wider application of drones such as beyond visual line of sight (BVLOS) and operating above the current limit of 400 ft. It emphasises upon drone corridors (to keep commercial UAS operations out of non-segregated airspace in which manned aircraft operate), autonomous operations of drones (if adequate safety, security and privacy principles are demonstrated in the design of operations), drone ports (to facilitate the landing and take-off of drones), night-time drone flights, 100 per cent FDI under automatic route, etc.[21]

Counter Drone Technologies

The CAR framework as an initial measure outlines a policy to mitigate various types of risks from malicious drones. However, in a country as diverse as India, there is a need to have effective counter drone systems in place because of multiple vulnerabilities. CAR 2.0 as and when it comes into vogue will also lead to proliferation of UAS traffic. The latent population of unregistered drones prior to the regulations formed in 2018 is also a serious concern in India. This further necessitates implementation of counter-drone technologies that are sophisticated and efficient.

Given a volatile world scenario and enhanced use of drones by non-state actors and other hostile entities, many countries are investing in counter drone technologies as they strengthen their defence capabilities to tackle unconventional threats. The anti-drone market is currently estimated to be at USD 0.6 billion and is expected to touch USD 2.4 billion by 2025; the CAGR is expected to soar by 32.2 per cent by 2025.[22] Although COVID-19 has affected the anti-drone market, it is expected to shoot up in the post-pandemic period.

Counter Drone Technology refers to systems that are used to detect, identify and neutralize a hostile or rogue drone. It has already seen its extensive use in civil arena and combat zones. In India it has been routinely employed during Independence Day and Republic day celebrations. A complete counter drone system should have the capability to detect, track and interdict rogue drones.

Types of Drone Detection and Tracking Technology

In a counter-drone system, its sensors must detect, identify, locate, and track incoming drones. Various types of detection and tracking technology of drones are as under: [23]

- ***Radar.*** Radar sends a radio signal to a target and based on the signal reflected, it gauges the direction and distance of the target. Radars are used to detect and track high-speed moving objects which also have a large surface area like an aircraft. It is difficult for radars to pick up small targets. Detecting objects of the size of a drone requires high frequency radar and it is highly susceptible to weather conditions. Also, low altitude, velocity and small radar cross section (RCS) of drones make it extremely difficult to distinguish a drone from a bird.
- ***Radio Frequency (RF) Analysers.*** RF analysers consist of multiple antennas to receive radio waves and a processor to analyse the RF spectrum. The system detects radio channel between the drone and its controller. It scans the frequencies on which most drones operate and based on the RF signatures matching with its library of drone frequencies, the algorithm detects RF-emitting devices in the area that are likely to be drones. Since it can only detect certain frequency bands in the library, the library needs to be updated periodically. RF scanners are limited in their capability to locate drones accurately in space but some integrated systems can locate the drone through triangulation, using multiple radio receivers deployed at a distance.
- ***Electro-Optical (EO)/Infrared (IR) Sensors.*** The commercial system combines visual and thermal sensors. Visual cameras are used for detection and tracking of drones during daytime. During night-time, infrared (IR) or thermal cameras are used to capture the heat signature of drones. Another optical mode detection technology is LiDAR (Light Detection and Ranging) that shoots a Laser beam at the drone and measures the time it takes for the light to return. It is difficult to use all these sensors for detection in silos because of high false-alarm rates (of distinguishing between a bird from a drone), requirement of good focusing capabilities, need of multiple cameras to give 360-degree detection and also being prone to inclement weather conditions.

- ***Acoustic Sensors.*** These systems use a microphone array that detects the noise of drone rotors and compare it with the library of sounds produced by known drones. These sensors are a good complementary approach to traditional techniques like Radar or RF or EO/IR sensors. They are vulnerable to noisy environments and have a very short range.
- ***Combined Sensors.*** No individual detection system is foolproof; hence commercially available counter drone systems use an integrated architecture with different types of above mentioned sensors. This arrangement increases the probability of a successful detection.

The effectiveness of the various sensors mentioned above to different environmental conditions are given in the table below:

Table 2: Sensors and their effectiveness

Factor	Sensors and its Effectiveness					
	RADAR	RF	Visual	IR	LiDAR	Acoustics
Light	Yes	Yes	Yes	No	Yes	Yes
Darkness	Yes	Yes	No	Yes	Yes	Yes
Noise	Yes	Yes	Yes	Yes	Yes	No
Distinguish a Bird & Drone	No	Yes	No	No	No	Yes
Adverse Weather Condition	No	No	No	No	No	No
Identification	No	Yes	Yes	Limited	No	Yes
Tracking	Yes	Need multiple sensors	Yes	Yes	Yes	Need multiple sensors
Long Range Detection	Yes	Yes	With focus lens	No	Yes	No
Multiple Drone Detection	Yes	Only if drones are operating on different channels	Yes	Yes	Yes	Only if drone are of different types

Source: arxiv.org on Security and Privacy in the Age of Drones.[24]

Based on the information received from these sensors, the users of counter-drone systems must decide how to respond to an incoming drone. Detection and tracking of hostile drones is an important part of counter drone system, but it is half the solution. It has to be augmented with an interdiction system as well. There may not be a requirement of activating an interdiction system (a hard kill measure) always. Soft kill measure would be a good option initially, like if the user detects and locates a drone, particularly in a civil area, the drone operator can be asked to cease flying in the area. Using an interdiction technology should be the last resort. Once a hard kill interdiction system is activated, the drone is intercepted based on the technique used. This would entail the drone landing on the ground or activating a “return to home” (RTH) mode (in the case of jamming or spoofing), or capture of the drone

(using nets), or the destruction of the drone (using Lasers, projectiles, collision drones, high powered microwaves) etc. Although the interdiction technology to neutralise drones is available, current regulations in most countries forbid these technologies to be used for neutralising drones (Exceptions are sometimes made for military or law enforcement agencies). The interdiction technologies are explained below:[25]

- ***RF Jammer.*** RF Jammers effectively neutralise drones by transmitting high RF energy that jams the controller signal of the drone. This may result in either a controlled landing of the drone from its current position or it returns to the user set home location (Return to Home (RTH) mode) or it could fall uncontrolled to the ground or it may fly off in a random uncontrolled direction. RF jammer has a drawback that it can jam other radio communications, or can result in drone taking an unpredictable path or may land near the target.
- ***GPS Spoofing.*** Using this technology, the equipment sends a new signal to the drone, thus interfering with its communication link channel with GPS satellites (used for its navigation) and forces the drone to get confused by making it forget its waypoints. In this way, the drone is spoofed by making it feel that its location is elsewhere. The system can keep altering the GPS coordinates in real-time and the drone remains in the control of the agency using the spoofing device. The drone can be directed to a safe zone once it is in total control of the spoofing agency. The system has a short range and also can jam other radio network.
- ***High Power Microwave Devices.*** High Power Microwave (HPM) system emits an Electromagnetic Pulse (EMP) that can disrupt the electronic circuitry of the drone and also interfere with its radio channels. The EMP injects a severe damaging voltage and current in the electronic components in the drone to neutralize it. Since its strike can instantaneously neutralize the system, there is a high probability of the destroyed drone falling uncontrolled on the ground. Also, in spite the equipment trying to focus the EMP in a particular direction, can cause some collateral damage through unintentional disruption of electronics of other communication systems in its vicinity.
- ***Kinetic Measure.*** This measure entails shooting down a UAS using a sniper rifle or an anti-aircraft gun or a missile based on the situation. This is certainly not a cost effective method and the shooter needs high level of skill and expertise.
- ***Nets and Net Guns.*** A net can be fired at or brought in contact with a malicious drone to impede the rotor blades of the drone and cease its flight. A Net gun can be used in hand held, shoulder launched or turret-mounted mode to fire at a drone, which is effective at a range of 20 to 300 m. These can be used with or without a

parachute for controlled descent of the captured drone. Even net cannon can be fired from another drone to capture a rogue drone.

- ***High Energy Lasers.*** A focused Laser beam towards the drone also can neutralize the drone by destroying its structure and/or the electronics. These systems are expensive and also can cause collateral damage affecting other electronic circuitry of systems in its vicinity.
- ***Birds of Prey.*** Given their natural hunting instincts, eagles can be trained to capture drones. Since there is no technology involved in this solution, it is cost effective, but requires immense efforts to train the bird and for its maintenance.

Counter-drone systems have immense challenges at the level of its performance, research and development cost, legality and policy. It faces challenges of detection effectiveness, false positives and false negatives, distinguishing legitimate and illegitimate use of drone, effectiveness and risk of interdiction technologies. Also, a scenario of drone swarm poses a very complex challenge from the counter-drone perspective. The drone technology is also changing at a fast pace that any counter measure also becomes rapidly obsolete.

Anti-Drone Systems from Indian Perspective

As per media reports, it is estimated that there are 6 lakh rogue drones or UAS in India.[26] The DGCA indicates there are approximately half a million drones either imported or manufactured before promulgation of CAR 1.0. To bring them under legal framework an option for disclosure has been given to such drone users subject to adhering to all conditions given in CAR 1.0.[27] While discussions have been on by security agencies on drones and anti-drone systems since some time, incidents like arms dropping in Punjab using a UAS in September 2019 at the India – Pakistan border has raised urgent concern with Law Enforcement Agencies, making it a necessity to expedite the process of implementing anti drone systems. In September 2019, Bureau of Police Research & Development (BPR&D), under the Ministry of Home Affairs, organised a National Level Seminar cum Exhibition on Anti-Drone Technology at BPR&D HQ, New Delhi, followed by a demonstration at BSF Campus in Haryana which was attended by all stake holders.[28] An Expression of Interest with draft Qualitative Requirement (QR) was initiated in October the same year by BSF.[29]

In October 2019, the DGCA also came up with a National Counter Rogue Drone Guidelines 2019 that laid down measures to be deployed in response to threats to vital installations from unmanned aircraft systems.[30] Apart from the anti-drone technologies, the exhaustive document also gives out the suggested deployment plan based on the vulnerability of different vital installations like a full scaled model, mid segment model or basic model. It emphasizes upon the apex nodal body (with members from MoD, MHA, Ministry of Civil

Aviation, DRDO, etc.) like the steering committee and the implementation committee for evolving counter drone framework and implementation mechanism at the national level. The document also outlines the legal procedure to handle rogue drones so as to ensure that all the legal provisions are consistent with public safety, law enforcement and internal security.

The website of BPR&D indicates that QR for the handheld, vehicle mounted and static version of anti-drone system are in place.[31] As per media reports[32], the anti-drone system developed by DRDO (through BEL as its designated lead agency), and deployed during 2020 Republic and Independence Day, uses Radar for detection/tracking and RF Jamming as the interdiction technology. They have also developed a mitigation technology based on Laser beam to target the drone and neutralise it. Apart from DRDO, some private sector companies along with security agencies have also been able to develop anti-drone systems.

The drone technology is evolving at a rapid pace and the existing counter-drone systems have their own limitations, which necessitates rapid development of new counter-drone systems. As the technology industry is harnessing the power of Artificial intelligence (AI) and machine learning, this technology can be utilised in drones to operate it in automatic and collaborative modes. Countering a swarm of such drones poses a serious threat to security forces. Even the drone manufacturers are focusing on counter measures so that their devices are not detectable. Under these conditions, research and development activities in counter-drone systems merit consideration. As the newly formulated Defence Acquisition Procedure (DAP 2020), lays down a new category of innovations through Innovation in Defence Excellence (iDEX), the same needs to be exploited to align various startups, MSMEs or individual innovators who can contribute in counter-drone technologies.

From the defence perspective, there lies a bigger challenge in intercepting hostile drones that enter Indian airspace from either Pakistan or China. China is a global leader in manufacturing armed drones which has benefitted Pakistan too in having a good supply to the country's state and non-state actors. Globally, China has seized the initiative in exploiting technology (particularly AI and machine learning) and producing Unmanned Aerial Vehicles (UAV). They are heavily into manufacturing of various types of aerial platforms for their ascendancy in the new battle space. The aerial platforms like Medium Altitude Long Endurance (MALE) UAV, High Altitude Long Endurance (HALE) UAV and loitering munitions (that can be piloted or pre-programmed to strike specific targets) are actively marketed for exports too. [33]

India's preparedness for conventional operations has enhanced along the LoC and LAC, with sound infrastructure in terms of ground deployment of troops, arms, ammunition, aircraft, EW systems etc. for a visible threat. This makes adversaries think of newer ways of

waging war using aerial platforms like UAVs or drones. In such a scenario, the ground formations are vulnerable without adequate early warning sensors, air defence systems, EW cover and counter drone systems. This necessitates counter drone systems to be made integral to the EW systems at various formation levels particularly along the borders. Also, investments in this comprehensive EW systems (integrating the counter drone technologies with technological advancements in the field of AI and machine learning) will have to be made to effectively interdict and destroy drones, drone swarms or cluster munition fire assaults. The scenario of a drone based threat and its mitigation measures needs to be brainstormed during war games as well.

Conclusion

The defence sector is expected to account for a major share of the anti-drone market in the years to come. The use of drones for cross border terrorism, smuggling, and spying are on the rise. Drone technology and its demand is increasing at a rapid pace, so the anti-drone systems have to evolve at a similar pace. Though there are drone detection, tracking and interdiction technologies in the market, but these systems are not foolproof and have got their own performance limitations, risks and legal implications. In Indian context, the process started with regulatory framework for drones (CAR 1.0) in 2018 which is under the process of evolving as CAR 2.0. The same was followed by seminars/demo on various counter drone systems and technologies in 2019, framing of the QRs by MHA and also the framing of counter-drone guidelines by DGCA. Currently DRDO and few private players have evolved counter-drone system, but the challenges ahead are enormous. The advent of AI and machine learning and its use in drone technology mandates the counter-drone industry to focus on research and development activities to support law enforcement agencies. Anti-drone technology is relatively new in the market, it needs immense R&D and it also has high cost implications, so this is one sector wherein the innovations clause of DAP 2020 can be explored through iDEX to encourage various start-ups and MSMEs in this field.

End Notes

[1] "The Drone Market Report 2020-2025", GlobeNewswire, 22 July 2020. Available on https://www.globenewswire.com/news-release/2020/07/22/2066029/0/en/The-Drone-Market-Report-2020-2025.html ,accessed on 11 December 2020.

[2] Mike Eckel (2020), "Drone Wars: In Nagorno-Karabakh, The Future of Warfare Is Now", Radio Free Europe Radio Liberty, 09 October 2020. Available at https://www.rferl.org/a/drone-wars-in-nagorno-karabakh-the-future-of-warfare-is-now/30885007.html accessed on 02 December 2020.

[3] Franz J. Marty (2020), "Fire from the Sky: The Afghan Taliban's Drones", The Diplomat, 22 December 2020. Available on https://thediplomat.com/2020/12/fire-from-the-sky-the-afghan-talibans-drones/, accessed on 23 December 2020.

[4] "Drones market - growth, trends, and forecasts (2020 - 2025)", Mordor Intelligence, 2020. Available on https://www.mordorintelligence.com/industry-reports/drones-market ,accessed on 11 December 2020.

[5] Ibid.

[6] "The Indian Commercial Drone Market is Projected to Grow at a CAGR of 12.4% during 2020-2026", GlobeNewswire, 31 August 2020. Available on https://www.globenewswire.com/news-release/2020/08/31/2085879/0/en/The-Indian-Commercial-Drone-Market-is-Projected-to-Grow-at-a-CAGR-of-12-4-during-2020-2026.html ,accessed on 11 December 2020.

[7] Sean Gallagher (2013), "German chancellor's drone "attack" shows the threat of weaponized UAVs", arstechnica.com, 19 September 2013. Available on https://arstechnica.com/information-technology/2013/09/german-chancellors-drone-attack-shows-the-threat-of-weaponized-uavs/ , accessed on 02 December 2020.

[8] Michael D. Shear and Michael S. Schmidt (2015), "White House Drone Crash Described as a U.S. Worker's Drunken Lark", *The New York Times*, 27 January 2015. Available at https://www.nytimes.com/2015/01/28/us/white-house-drone.html, accessed on 02 December 2020.

[9] Bernard Hudson (2018), "Drone attacks are essentially terrorism by joystick", *The Washington Post*, 06 August 2018. Available at https://www.washingtonpost.com/opinions/drone-attacks-are-essentially-terrorism-by-joystick/2018/08/05/f93ec18a-98d5-11e8-843b-36e177f3081c_story.html, accessed on 02 December 2020.

[10] Ibid.

[11] PTI (2019), "GPS-fitted drones from Pakistan airdropped weapons into Indian territory", *The Economic Times*, 25 September 2019. Available at https://economictimes.indiatimes.com/news/defence/gps-fitted-drones-from-pakistan-airdropped-weapons-into-indian-territory/articleshow/71291349.cms?from=mdr ,accessed on 02 December 2020.

[12] "Massive swarm drone strike on Saudi oil facility demonstrates destructive potential of autonomous weapons", DeZeen, 16 September 2019. Available at https://www.dezeen.com/2019/09/16/drone-strike-saudi-arabia-aramco-oil-supply/, accessed on 02 December 2020.

[13] Mike Eckel (2020), "Drone Wars: In Nagorno-Karabakh, The Future of Warfare Is Now", Radio Free Europe Radio Liberty, 09 October 2020. Available at https://www.rferl.org/a/drone-wars-in-nagorno-karabakh-the-future-of-warfare-is-now/30885007.html accessed on 02 December 2020.

[14] Ben Nassi, Asaf Shabtai et al (2019), "SoK - Security and Privacy in the Age of Drones: Threats, Challenges, Solution Mechanisms, and Scientific Gaps", arxiv.org, 12 March 2019. Available at https://arxiv.org/pdf/1903.05155.pdf , accessed on 02 December 2020.

[15] Ibid.

[16] Ibid.

[17] "Requirements for Operation of Civil Remotely Piloted Aircraft System (RPAS)", Director General of Civil Aviation, 27 August 2018. Available at https://dgca.gov.in/digigov-portal/jsp/dgca/homePage/viewPDF.jsp?page=InventoryList/headerblock/drones/D3X-X1.pdf , accessed on 11 December 2020.

[18] Ibid.

[19] Ibid.

[20] "Requirements for Operation of Civil Remotely Piloted Aircraft System (RPAS)", Director General of Civil Aviation, 27 August 2018. Available at https://dgca.gov.in/digigov-portal/jsp/dgca/homePage/viewPDF.jsp?page=InventoryList/headerblock/drones/D3X-X1.pdf , accessed on 11 December 2020.

[21] "Drone Ecosystem Policy Roadmap", Global Aviation Summit Report, 2019. Available at https://www.globalaviationsummit.in/documents/DRONE-ECOSYSTEM-POLICY-ROADMAP.pdf , accessed on 02 December 2020.

[22]"Anti-Drone Market" report, marketsandmarkets.com, 2020. Available at https://www.marketsandmarkets.com/Market-Reports/anti-drone-market-177013645.html , accessed on 02 December 2020.

[23] Arthur Holland Michel (2019), "Counter Drone Systems", Center for the Study of the Drone, Bard College, December 2019. Available at https://dronecenter.bard.edu/files/2019/12/CSD-CUAS-2nd-Edition-Web.pdf , accessed on 11 December 2020. Also see, "9 Counter Drone Technologies to Detect and Stop Drones", Robin Radar Systems, 22 March 2020. Available at https://www.robinradar.com/press/blog/9-counter-drone-technologies-to-detect-and-stop-drones-today , accessed on 11 December 2020.

[24] Ben Nassi, Asaf Shabtai et al (2019), "SoK - Security and Privacy in the Age of Drones: Threats, Challenges, Solution Mechanisms, and Scientific Gaps", arxiv.org, 12 March 2019. Available at https://arxiv.org/pdf/1903.05155.pdf , accessed on 02 December 2020.

[25] "9 Counter Drone Technologies to Detect and Stop Drones", Robin Radar Systems, 22 March 2020. Available at https://www.robinradar.com/press/blog/9-counter-drone-technologies-to-detect-and-stop-drones-today , accessed on 11 December 2020. Also see, Arthur Holland Michel (2018), "Counter Drone Systems", Center for the Study of the Drone, Bard College, February 2018. Available at https://dronecenter.bard.edu/files/2018/02/CSD-Counter-Drone-Systems-Report.pdf , accessed on 11 December 2020.

[26] PTI (2019), "India has over 6 lakh rogue drones; agencies analysing sky fence, drone gun technology", *The Hindu*, 29 September 2019. Available at https://www.thehindu.com/sci-tech/technology/india-has-over-6-lakh-rogue-drones-agencies-analysing-sky-fence-drone-gun-technology/article29548347.ece accessed on 02 December 2020.

[27] Drone registration notice, Ministry of Civil Aviation, 13 January 2020. Available at https://www.civilaviation.gov.in/sites/default/files/Drone_Registration_Public_Notice_13012020.pdf , accessed on 11 December 2020.

[28] "PIB, BPR&D to organize a National Level Seminar cum Exhibition and Demonstration on Anti-Drone Technology", Ministry of Home Affairs, 25 September 2019. Available at https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1586189, accessed on 11 December 2020.

[29] Draft Qualitative Requirements (Qrs / Specifications) And Trial Directives For Anti-Drone System, DG BSF, Ministry of Home Affairs, DG BSF, 2019. Available at https://www.mha.gov.in/sites/default/files/QRs_AntiDroneSystem_11102019.PDF , accessed on 02 December 2020.

[30] "National counter rogue drones guidelines", Ministry of Civil Aviation, 2019. Available on https://www.civilaviation.gov.in/sites/default/files/Counter_rogue_drone_guidelnes_NSCS.pdf , accessed on 11 December 2020.

[31] Shishir Gupta (2020), "DRDO ready with anti-drone system for armed forces, PM Modi to have drone killer as part of his security detail", *Hindustan Times*, 29 November 2020. Available on https://www.hindustantimes.com/india-news/drdo-ready-with-anti-drone-system-for-armed-forces-pm-modi-to-have-drone-killer-as-part-of-his-security-detail/story-ZzSLytENkCubX9CuP0XV7N.html , accessed on 02 December 2020.

[32] Qualitative Requirements and Trial Directives, Bureau of Police Research and Development, Ministry of Home Affairs, 14 October 2020. Available on https://bprd.nic.in/content/40_1_QualitativeRequirementsandTrialDirectives.aspx , accessed on 02 December 2020.

[33] Norine MacDonald and George Howell (2020), "Competition in Artificial Intelligence and Unmanned Aerial Vehicles", National Defence University Press, 2020. Available on https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-3/prism_8-3_MacDonald-Howell_102-126.pdf , accessed on 11 December 2020.

CENTRE FOR LAND WARFARE STUDIES (CLAWS)
RPSO Complex, Parade Road, Delhi Cantt, New Delhi 110010
Tel.: +91-11-25691308, Fax: +91-11-25692347, CLAWS Army No. 33098; Email: landwarfare@gmail.com Website: www.claws.in