Unmanned Aerial Systems and the Threat of Non-State Actors

Challenges and Prospects for India

Mukesh Kumar*

The decade 2010–20 witnessed an upsurge of unmanned aerial systems. Alternatively known as drones, they are generating employment in different sectors including both civilian and defence. Goldman Sachs reported about a US$ 100 billion drone market between 2016 and 2020. In addition to its growing demand in commercial and government sectors, drones provide a cheaper and safer option for the armed forces as an alternative to manned aircraft. Applications of the drone in the Nagorno–Karabakh conflict and the ongoing Russia–Ukraine war have unleashed its growing importance on the battlefield. This trend shows that defence will remain its largest market, providing an opportunity to invest and manufacture the technology. The global competition for manufacturing drones is heating up and many countries are coming out with improved technology. The growing market has not only attracted the government but also non-state actors. Drones are becoming a viable option for terrorist groups and many non-state actors with their cheaper, less detectable and limited capabilities. For example, in 2018, Venezuelan President Nicolas Maduro was attacked by two drones while addressing the Bolivarian National Guards in Caracas. Drones are being used in regular armed conflicts between rebel groups

* Mr Mukesh Kumar is a Doctoral Scholar at the Centre for International Politics, Organisations, and Disarmament, School of International Studies, Jawaharlal Nehru University, New Delhi.

ISSN 0976-1004 (print); 2583-7567 (online)

Journal of Defence Studies, Vol. 17, No. 4, October–December 2023, pp. 154–176

and national armies in West Asian countries. The surge in drone attacks by terror outfits has posed a serious challenge to national governments. The objective of the article is to analyse the growing threat of drone attacks by non-state actors. The article will also draw lessons for India keeping in mind its vulnerabilities and developments in terms of national response to such attacks.

Keywords: *Unmanned Aerial Systems, UAS, Drones, Unmanned Aerial Vehicles, Non-state actors or rogue drones*

Introduction

Unmanned Aerial Vehicles (UAVs), as the name suggests, are flying vehicles with no pilot or crew member on board. It can also be understood as a flying robot that is controlled autonomously or by operators on the ground. Drones are defined by different terms. According to India's national counter-rogue drone guidelines, drones is the umbrella term for Remotely Piloted Aircraft (RPA), Remotely Piloted Vehicles (RPV), Unmanned Aerial Systems (UAS) and Unmanned Aerial Vehicles (UAV).

The outset of drones marked a technology transition from vulnerable heavy-weight aeroplanes to less detectable smaller aircraft. Unlike big aircraft, UAVs were easily adopted by countries due to their small size and varied applications. The evolution of drone technology can be divided into technological phases on the basis of its applicability, which was enhanced over time by different sectors. The early stage is marked by radio-controlled aircraft used for training and target practice. In the second phase, drones were used for surveillance and reconnaissance. The third and current phase has applications in offensive military operations. With every phase, drone manufacturers have launched superior technology that helped the drone industry flourish in different regions of the world.[1]

It was during the inter-war period when the term 'drone' was coined for the first time, inspired by DH82B Queen Bee, a pilot-less target aircraft designed for anti-aircraft gun training.[2] The development and demonstration continued with limited success till World War II. Subsequently, drones evolved as a means of intelligence gathering during the Korean War. Drones were deployed in actual battlefields by the US during the Vietnam War for reconnaissance, dropping leaflets and as decoys to trap communist guerrilla fighters. After the Vietnam War, countries other than US and Britain took a keen interest in investing in drone manufacturing with enhanced capabilities in terms of weight, endurance and ceiling height.[3] Soon, drones became

dual-use technology and were adopted by trade and commercial sectors. The adoption of UAVs by the civilian sector lead to increased demand and the proliferation of the technology. Among its many users, non-state actors and terrorist organisations quickly switched to the technology and exploited UAVs successfully for various purposes.

United States-led coalition forces have effectively used drones in its Global War on Terrorism (GWOT) in Afghanistan. The war was a significant event and since then the drone has proliferated and reached the non-state actors operating in the Golden Crescent (Afghanistan–Pakistan–Iran), Latin American Region and West Asia and Northern Africa (WANA) region. Easy availability and controlled functions make drones an affordable and preferred choice for non-state actors and states backing these notorious outfits for their purposes. In West Asia, Iran has been a significant player, providing drones of varied capabilities (in terms of sizes, range and endurance) to its regional proxies such as Hamas, Hezbollah and Houthis, who have been very active in recent years.[4] In Latin America, drones have become a popular mode for smuggling drugs and narcotics, a trend that reached India in 2019. Due to the evolution in the drone industry, drones are now easily accessible and can be easily manufactured, such as DIY and hobbyist drones.

The proliferation of drones as a means of threat or weapon has necessitated state governments to analyse the threat pattern and form specific policies as a countermeasure. In 2021, US Military General Kenneth McKenzie Jr., while warning the US Central Command (CENTCOM) regarding Iranian drones said, 'For the first time since the Korean War, we are operating without complete air superiority.'[5] The same year, India acknowledged the potential of rogue drones when the Jammu-based Indian Air Force (IAF) station was attacked with explosives-laden drones. Drone menace in India can be attributed to its proliferation in regional countries such as Pakistan. In 2015, Pakistan possessed the capability of indigenously manufacturing armed drones with advanced technology; ironically it had criticised the US against their operation in Afghanistan. Pakistan's drone capability, which they acquired from China, has serious regional implications in the entire South Asian region, which can further drone proliferation. Considering the economic crunch and its anti-India stance, it could offer drones and its technology to non-state actors or terrorist groups to carry out operations in India.[6] India has been acting seriously to counter such incidents by assessing the rogue drone incidents that are happening worldwide and in its territory.

Rogue Drones and Potential Threat Scenarios

Drones used by non-state actors are not confined to offensive operations but are also used for various other motives. Earlier, these drones were mainly confined for use by the government and armed forces for security purposes. Now, such drones are easily available in the market and could be manufactured by hobbyist drone users. What's more, drone DIY kits are also available online; these can be self-assembled and are easily accessible by terror outfits.

Rogue drones can be utilised in three ways: as autonomous drones, drone swarms and stealth drones. Autonomous drones are controlled autonomously by computers or chips installed on board. They navigate towards their fixed targets automatically and do not require the operator's instruction for decision making and execution of tasks. Swarming of drones is another serious challenge where multiple intelligent drones navigate towards their target while coordinating amongst themselves simultaneously. They are well-networked and are controlled by a GPS system for smooth functioning. Stealth drones are designed and modified to elude radars and operate in a manner that makes them difficult to detect. By employing these means, drones can be used for various purposes by notorious outfits. The following section will throw light on some of the vulnerabilities or purposes behind rogue drone operations.

Surveillance and Reconnaissance

Drones installed with high-resolution cameras are used for stealing data by taking photographs and videos from a sizeable distance. With enhancement in technology and easy availability, such sophisticated drones are now being used by non-state actors and terrorist groups for intelligence gathering of government institutions and buildings, security installations, places of strategic and national importance, business firms, crowded places and other critical infrastructure to exploit a nation's vulnerabilities. Reconnaissance against fixed installations and military bases is usually conducted before conducting a ground assault. In 2012, Israel shot down an Iranian Ayub drone sent by Hezbollah over Dimona, a city where the Negev Nuclear Research Centre is established. Reportedly, the drone was capturing the nuclear reactor, ballistic missile sites, airfields and preparations for a US–Israel joint military exercise.[7] Moreover, real-time surveillance can also be conducted for online propaganda and imagery of surveillance drones can be used to expose the opponent's vulnerabilities and classified installations.

Smuggling and Transportation

Drones are used as delivery systems for the transportation of goods for business and commercial purposes. Its commercial use was mainly exploited during the COVID-19 pandemic. However, such drones have been exploited by terrorist groups to carry and equip their armed base camps at difficult locations with weapons and other necessary items relevant to operations bypassing traditional security mechanisms.[8] Besides transportation, drones are also exploited for smuggling arms and equipment, drugs, fake currency and other illegal items for economic gains. Such platforms can also emerge as opportunities for non-state actors to create proxies by equipping the ethnic, minorities, marginalised and unsatisfied sections of society with Small Arms and Light Weapons (SALW).

Runway and Airspace Interference

Drones can pose a serious threat to civilian and military aircraft. During flight, a mere collision with a drone (intentionally or unintentionally) could create collateral damage. The presence of drones near runways or airports, even at sizeable distances, could create disturbance, distraction and panic among the aircraft crew. Although drones are prohibited from operating near airports, autonomous and swarm drones could cause intervention at runways and airspace. Moreover, rainy and foggy weather impacts visibility and detection systems, which further makes drones a serious challenge for smooth flight operations.

Weapons of Mass Destruction

Rogue drones can be utilised to carry and drop weapons of mass destruction, mainly chemical, biological and radiological weapons. However, it is difficult for non-state actors to develop and access the weapons of mass destruction. In view of international regulations and norms regarding weapons of mass destruction, highly enriched uranium and low-yield tactical nuclear bombs could be made available via international black markets and illegal transfers. After the Soviet disintegration, a large quantity of Highly Enriched Uranium (HEU) was stolen or missing, which later surfaced in the black market. Dozens of cases have been reported by the International Atomic Energy Agency's (IAEA's) Illicit Trafficking Database regarding illicit transfers of HEUs.[9] In 2010, two Armenians were arrested for smuggling weapons-grade uranium enriched up to 90 per cent in a cigarette box in Georgian black market.[10] Aum Shinrikyo's plot to release sarin, a chemical agent, in

Japan in 1994 suggests that the application of UAVs for conducting a mass destruction attack has been explored by terrorists for long.[11]

Kamikaze Attacks and Launching Pads

Another potential threat associated with drones is their suicidal attack and kinetic attack capability. Drones, with and without weapons, are capable of hitting their targets with high speed and can cause serious damage, mainly in case of its collision with aircraft. Sacrificial drones carrying explosives, such as bombs and incendiary devices, can be programmed to collide with automated targets. Besides kamikaze attacks, weaponised drones can also be instructed to either drop or throw projectiles towards the target. Drones can be modified and fitted with automatic guns or firearms. These firearms can attack either premeditated targets installed in advance (autonomously) or on the command of drone operators. Such kind of an attack has not been registered yet, but the possibility cannot be denied. To increase the lethality of the attack, larger drones can be used as launching pads for missiles or rockets.

Nuisance and Messaging

This is the most common threat associated with the usage of rogue drones. Such attacks can be categorised into two forms. First, the attacks are linked with disturbing individual and public peace and stealing data (nuisance). Hovering drones enter private or public spaces and compromises individuals' security by intruding in their privacy. Modern drones are equipped with improved technology such as Wi-Fi Pineapple, which can steal personal or classified information by hacking smartphones and personal computers by spoofing Wi-Fi connections and other wireless networks.[12]After stealing sensitive information, drone operators can either demand payment or threaten their target with uploading the sensitive information on online platforms.

The second form of attack can take the form of messaging. Messaging as a threat can be directed for two major purposes—propaganda and seeking support. Drones can convey propaganda messages or videos on social media platforms to attract the attention of both internal and external audiences and disrupt normal public functioning. By connecting or sneaking into Wi-Fi or Bluetooth networks, drones can capture photographs and videos that can then be transferred to cell phones via video transmitters that converts them into Radio Frequency (RF) signals. In the ongoing Russia–Ukraine war, Russia's Leer-3 drone was used to bombard the cell phones of Ukrainian soldiers with sinful and diverting texts, something that is referred to as

pinpoint propaganda.[13] Drones with combat capability are used as a tactical means whereas drones that capture videos and photographs quietly without indulging in strikes are used for strategic purposes. These videos are used to earn money and trust from supporters and sympathisers, even seeking support for a separate territory as in the case of ISIS.[14] This propaganda messaging plays a vital role in mobilising the general public including the weaker sections, which can create distrust among the common masses against the national government.

Drones and Non-State Actors

There are numerous incidents of drones being used by non-state actors for various purposes worldwide. Amongst them, surveillance and collision were predominantly the main purpose behind the usage of drones by non-state actors; these were made by them and against the state's military forces and civilians. Abundant literature has been available on how terror outfits utilise drones in different regions of the world. One example dates back to the 1990s. In 1994, Aum Shinrikyo, a Japanese terror outfit attempted to exploit a remotely controlled helicopter to release sarin, a nerve agent, by an aerial spray mechanism. The helicopter failed while testing so a refrigerator truck was used as an alternative.[15] Since then, several such terror incidents have occurred in different regions of the world. With the rapid technological advancement in the drone market, the nature of drone usage has also enhanced from surveillance and collision to smuggling, airspace intervention and direct attack.

During the last few years, rogue drones have become popular with terror outfits for their operations. Rogue drone incidents have proliferated steadily, which has augmented the challenges and risks for nations. In 2017, the Islamic State of Iraq and Levant (ISIL) aka ISIS began creative modifications in drone manufacturing and announced the establishment of Unmanned Aircraft of the Mujahedeen (UAM) via its newsletter al-Naba.[16] ISIL's creative deception tactics included booby-trapped UAVs that exploded when taken for examination after being shot down. The deployment of UAVs and the establishment of an innovation unit made ISIL a frontline terrorist organisation in the usage of drones.[17]

In 2018, two Russian military bases were attacked by homemade drones. It was a swarm of 13 drones that attacked Russia's Hmeymim Airbase and Tartus Naval facility in Syria.[18] The year 2018 saw one of the most serious drone attacks when Venezuelan President Nicolas Maduro

survived an assassination attempt made allegedly by Columbia. While addressing the state military forces at the 81st National Army Day event in Caracas, two explosive-laden drones detonated near the Venezuelan leader, injuring several military and police personnel.[19] In the event, two DJI M-600 commercial drones delivered C-4 explosives to target the President.[20]

In recent years, Iran has been actively involved in providing drones to its proxies in different countries. In 2019, the Houthis conducted their first major attack using Qasef-1, a variant of the Ababil-T drone, on the Yemeni military parade at Al-Anad military base, killing six people.[21] Research highlighted that these UAVs originally belonged to Iran which had supplied them to the Houthis. London-based Conflict Armament Research (CAR) documented that the Houthis have their own domestic manufacturing facility and have developed two types of UAVs based on objectives—Reconnaissance UAVs (Hudhed-1 Raqib, Rashid and Sammad-1) and Combat UAVs (Qasef-1, Qasef-2K, Sammad-2 and Sammad-3).[22]

Hamas acquired drones from Iran and has been involved in drone attacks since 2012, mainly against Israel. In 2021, Hamas launched an 11-day conflict against Israel where it used Shehab, a new loitering suicide drone similar to the Iranian Ababil-T, which is considered its first precision guidance munition.[23] Popular Mobilisation Forces (PMF), an Iraqi militia backed by Iran, recently acquired drones and conducted six drone attacks in 2021 against various US targets in Iraq.[24] After PMF's attack, the US expressed concern regarding the proliferation and growing number of attacks by drones that are too small in size and flying at very low altitudes, making it difficult for the US's defence system to track. In 2022, a series of drone and rocket attacks were conducted by Yemen's Houthis rebels on Saudi Arabia's energy depots including the Aramco oil facilities at Jeddah. The attacks happened a few days before the final Formula One race, which is a worldwide sporting event. The drone attack was a retaliation against the Saudi-led coalition forces fighting against the Houthis rebels who have occupied Yemen's capital Sana'a since 2015.[25]

The growing cases of worldwide rogue drone incidents also have implications for other countries in the region. Additionally, the trend signifies that Iran has been backing its proxies in different countries by providing them with drones and other equipment to further their interests in the region. India has been facing proxies and cross-border terrorism mainly along the Indo-Pak border. In the growing drone menace, India is not resistant and has been facing intrusions by rogue drones in the past few years.

India and Rogue Drones

Unlike West Asia, drones as a means of terror tool came very late to India. In South Asia, however, Pakistan and Afghanistan have already addressed the legitimate and illegitimate drone incidents in previous years. Actors such as al-Qaeda, Taliban and Lashkar-e-Taiba have experimented with drones during the same time for reconnaissance and attack purposes. After the US's phased withdrawal from Afghanistan, the stock of arms including air and ground assault weapons in the region became a major issue. According to the US Department of Defence, around US$ 7.12 billion worth of US weapons were in Afghanistan's former government's possession when the Taliban took over in August 2021. Later it was reported that Tehreek-e-Taliban Pakistan (TPP) and the Baloch Liberation Army were using advanced weapons and gadgets left by the US.[26] However, it is not confirmed whether US drones were used, but reportedly terror groups in Kashmir got their hands on the US arms and equipment left in Afghanistan.[27] In the wake of the increasing drone incidents by non-state actors in West Asia and the Gulf region, it was a matter of time how long India could remain resistant. In India, rogue drone activities have increased manifold in the last few years.

Drone sightings are very common near the Line of Control (LoC). The earliest signs of rogue drone intrusions were registered in mid-2019. The Punjab Police recovered four hexacopter drones from the Tarn Taran district of Punjab. These drones, each capable of carrying a 4 kg payload, were used several times to carry 80 kg of arms (including small arms and AK-47 rifles) and fake currency in Punjab. With this recovery, the Punjab Police busted a serious attempt by Khalistan Zindabad Forces, a Punjab-based separatist outfit, to infiltrate the international border.[28] In 2019, numerous sightings of drones from Pakistan were reported by security personnel. The Punjab Police seized a consignment of arms that was dropped by a drone that came from Pakistan. Chinese pistols and AK-47s were among the arms seized by the police. The number of such incidents reduced in 2020 due to the COVID-19 pandemic and other reasons analysed in Table 1.[29] In 2020, another arms consignment was recovered by the police near Gurdaspur. In a separate incident, the BSF destroyed an unspecified drone near Jammu's Hira Nagar sector. All the reported rogue drone activities in India from 2018–21 were mainly used for smuggling and transferring arms and drugs. In June 2021, India encountered its first major drone attack at the Jammu Air Force base near the border. Two drones laden with improvised explosive devices exploded over the roof of a building.[30]

Here the most striking factor is that the drone activities were started and augmented at a time when the Indian government was planning to abolish Article 370 from the Indian state of Jammu & Kashmir (J&K). The Border Security Force (BSF) and Polish Forces have since adopted the strategy of 'Sight and Blight' for any drones or unidentified flying objects in the sky.[31] From 2019 to 2022, 576 cases of unidentified drones were reported by the BSF and district police forces, followed by 57 cases by the end of May 2023.

Table 1. Drone Incidents during the period 2019–2023

Year/states	**2019**	**2020**	**2021**	**2022**	**2023 (till May)**
Punjab	142	47	64	186	50
J&K	25	19	31	20	5
Rajasthan	0	10	7	18	2
Gujarat	0	1	2	4	0

Source: South Asia Terrorism Portal (SATP, 2023)[32]

Analysis of the data shows that states adjacent to the India–Pakistan border are the most affected. Punjab, J&K, Rajasthan and Gujarat have registered rising incidents of unidentified drones, with Punjab leading with maximum cases. As per Table 1, the number of rogue drone cases initially dropped between 2019 and 2020 in both Punjab and J&K (overall dropped by 90 per cent). This drop could indicate the seriousness of the Indian government and security agencies to swiftly and forcefully respond to such attacks due to the worldwide increase in rogue drone incidents and the enhanced military arrangements in J&K after the revocation of Article 370. Since 2020, such incidents have increased steadily in all four states, which can be attributed to the limited options available with the security agencies to counter rogue drones. Security agencies have provided state-wise data of rogue drone incidents to the government decision makers responsible for the procurement of anti-drone systems.

In Figure 1, total drone sighting incidents from 2019–23 have been divided into state-wise records. Out of a total of 633 cases, Punjab registered the maximum 489 cases (77 per cent), followed by J&K 100 cases (16 per cent), Rajasthan 37 cases (6 per cent) and Gujrat 7 cases (1 per cent). In February 2023, Inspector General of Police (IGP) Sukhchain Singh Gill reported that the Punjab Police has arrested 10,576 people involved in drug smuggling since the launch of a special campaign in July 2022. Moreover,

the police have recovered 667 kg of heroin, 423 kg of opium and 51,49,882 kg of medical drugs (tablets and injections) from the Firozpur, Tarn Taran, Fazilka, Gurdaspur, Amritsar and Patiala districts of Punjab.[33] On account of the nature of drone threats, smuggling of contrabands, surveillance and collision-type attacks can be presumed as the prime motives of rogue drone operators. Application of rogue drones is still in its nascent phase in India; however, possibilities of drones being used for airspace intervention and as launching pads for rockets and projectiles cannot be denied.

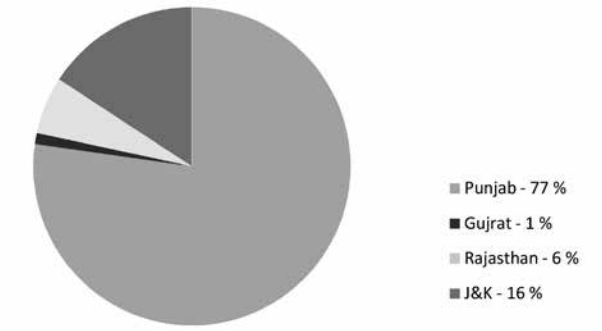

Figure 1 Drone incidents percentage between 2019 and 2023
Source: South Asia Terrorism Portal (SATP, 2023)[34]

On 11 April 2023, India's permanent representative to the United Nations (UN) Ambassador Ruchira Kamboj addressed the United Nations Security Council's (UNSC's) open debate on 'Threat to International Peace and Security: Risks Stemming from Violations of Agreements Regulating the Exports of Weapons and Military Equipment'. Speaking at the session, she said 'We are facing a serious challenge of cross-border supply of illicit weapons using drones, which cannot be possible without active support from the authorities in control of those territories', while condemning Pakistan and its link with the non-state actor for transferring arms across the border.[35] Inputs provided by the intelligence agencies, BSF and local police forces highlight the central role of Pakistan's intelligence network ISI, Khalistan separatists and other non-state actors in the transfer of Fake Indian Currency Notes (FICN), drugs and weapons by drones.[36]

On 1 August 2023, Minister of State in the Ministry of Home Affairs (MHA), Shri Nisith Pramanik informed the Lower House of the Parliament (Lok Sabha) that 'Anti-national elements or smugglers are using drones for

smuggling of arms/narcotics across India–Pakistan border in the State of Punjab. In the last three years till 30th June 2023, 53 incidents of recovery of drones involved in smuggling arms/narcotics have been detected.'[37]

In India, there can be two major reasons behind the usage of drones for rogue purposes and its sudden proliferation:

(a) Switching from a land-based to an air-based attack medium
(b) Risk assessment of cross-border infiltration

As already discussed in the previous sections, drones have become popular with terror outfits operating in various regions. Innovation in the field of military modernisation has served non-state actors with the same path and opportunity as provided to state militaries, thereby enhancing their capabilities to switch from ground-based to air-based operations. The role of Pakistan's Intelligence Agency (ISI) has been instrumental in assuring the accessibility/availability of drones to Pakistan-based terror outfits and separatist groups to violate the Indian air space and intrude into Indian territories.

The second reason is very important for analysing India's security arrangements at the international border between India and Pakistan. Due to the dense forest, hilly and difficult terrain, the LoC in J&K has proved a favourable ground for non-state actors to infiltrate and carry out their operations including the transfer of arms, drugs and FICN to other notorious groups in India. The terrain at the border in Gujarat, Rajasthan and Punjab does not provide a suitable environment for the infiltrators as in J&K. India's big investment and installation of smart fencing and seat sensors at the international border has denied room for large cross-border infiltrations. However, the advent of drones has provided non-state actors with a feasible option or an alternative to land-based infiltration.

Data in Table 2 presents that cross-border infiltration has decreased consistently since 2019, whereas for the same period drone incidents have increased significantly. The contrary pattern of cross-border infiltration and drone incidents at the Indo-Pak border indicates that drones have become a viable substitute for land-based infiltration. The dissolution of Article 370 and the subsequent enhancement of security in J&K have made it difficult for the non-state actors supported by the ISI to infiltrate India. The risks associated with cross-border infiltrations are high as compared to drone operations. Self-assembled drones, especially of autonomous nature, are difficult to detect and can easily locate the operator's identity and location. Cross-border infiltrations in India have often resulted in arrests and killings, which also tarnishes the infiltrators' nation's image. The pattern has also

created a dilemma in the minds of the Indian government and security agencies: while investment in smart fencing at the border and the deployment of night surveillance systems, heat sensing gadgets and night vision cameras among other security enforcements diminishes infiltration these measures have proven to be less effective against drones.[38]

Table 2. Cross-border infiltrations versus drone incidents at the India–Pakistan border

Year	Drone Incidents	Cross-Border Infiltration
2019	167	141
2020	77	51
2021	104	34
2022	228	14
2023 (till two quarters)	57	00

Source: SATP, 2023 and PIB, 2023[39]

India's Response and Challenges

In view of the on-going misuse of drones in local conflicts and against national assets, places of national, strategic and security importance, the Government of India in 2019 established a policy called 'National Counter Rogue Drone Guidelines'.[40] The worldwide drone incidents and the attack on the Jammu Air Force camp forced the government to prevent any opportunity that can be exploited by rogue drone operators to expose our vulnerabilities. Consequently, two committees with multiple tasks/roles have been formed: The Steering Committee and the Implementation Committee. Apart from this, the government along with the Ministry of Civil Aviation came up with new guidelines as part of a policy response to control and keep an eye on civil drone usage in India.

Policy Response: Legal Guidelines for Drone Usage

The Ministry of Defence has been in close touch with the Ministry of Civil Aviation to counter rogue drone activities in India. Consequently, the Director General Civil Aviation (DGCA), under rules 15A and 133A of the Aircraft Rules, 1937,[41] announced a Civil Aviation Requirement (CAR), Drone CAR 1.0, for civil drone operators in India.[42] As per the CAR, since December 2018 it is mandatory for all drone operators to register with DGCA's DigitalSky (Digisky) platform and share information regarding the flight plan of drones

and other such information required by the agency.[43] The purpose behind DigitalSky is to promote regulated drone operation in the national airspace. After registration, the platform provides an Unmanned Aircraft Operator Permit (UAOP) to identified Remotely Piloted Aircraft (RPA) operators and issues a Unique Identification Number (UIN). Regarding safety and security clearances, all drone manufacturers have to follow DGCA's strict guidelines of No Permit No Take-off (NPNT). Further, RPA manufacturers have to follow instructions authorised by DGCA under Drone CAR 1.0.

Meanwhile, operation of drones without registering and informing DGCA would be considered a violation of CAR and treated as an aerial threat. Besides the DGCA guidelines, MHA has issued Standard Operating Procedures (SOPs) for 'Handling Threats from Sub-Conventional Aerial Threats' in collaboration with the Indian Air Force (IAF).[44] The guideline provides concerned officers with various procedures to detect, identify, inform and execute unauthorised drones. The decision to execute rogue drones is vested with the IAF, police and a special agency deployed at government or security installations. Here, both Drone CAR 1.0 and MHA's guidelines authorise penal action under the provision of Indian Penal Code for operating rogue drones.

The application of rogue drones made India develop guidelines for countering such incidents. Although the government came quickly into action and formulated guidelines in 2019 when India was registering its initial drone incidents, the policy has some limitations that need to be considered.

(a) The policy is more concerned with rule-making procedures for local drone operators to comply with. This is for better transparency. The licensing registration and NPNT clause are made mainly for drones with commercial purposes.
(b) The policy had no measures for drones already developed or procured (from within and outside Indian territories) and in operation before the establishment of the rogue drone policy.

Operational Response: Counter-drone Development

Apart from the organisational set-up and the legal guidelines for the regulation of civil drones, the Indian government has also stressed on the application of rogue drones operated from both outside and inside the Indian territory. The rising cases of drone incidents since 2019 have alarmed Indian security agencies and forced decision makers to employ effective detection and intervention measures at the border and vital assets of the nation. As a

result, security agencies have signed various contracts with domestic firms for the Counter-Unmanned Aerial System (C-UAS). To understand the response mechanism and evolving challenges, we first need to understand the functions of the C-UAS mentioned in Figure 2.

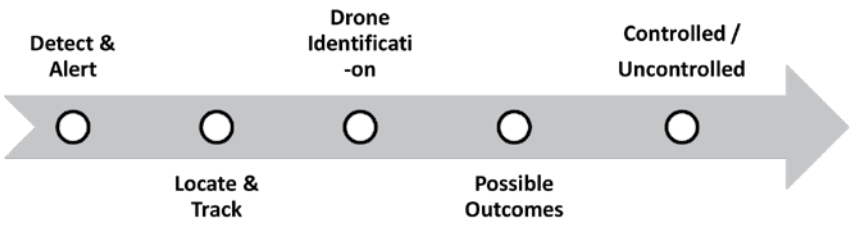

Figure 2 Flowchart of a C-UAS cycle
Source: Author's own

Figure 2 shows the lifecycle of drone usage and its intervention. The first three stages of the cycle include the detection of the drone, tracking the location of the drone and its operator and identification of the drone's specifications and properties to enable the security agencies to respond accordingly. For the first three stages, security agencies use measures such as radars, Electro-Optical or Infrared (EO/IR) sensors, acoustic sensors and Radio Frequency (RF) before deciding on outcomes. The last stage of the cycle includes controlled (passive) and uncontrolled intervention (mitigation) against rogue drones. The Counter Rogue Drone Guidelines of India have suggested a range of detection and intervention measures along with a deployment plan for the C-UAV systems.

For any rogue drone or unidentified objects in the air, early detection and identification are necessary to counter such acts as early as possible. It is also important at the initial stages to differentiate between friendly and rogue drones. Minister of State (MHA), Nisith Pramanik informed the Lok Sabha that the BSF has tightened up security along the border by patrolling and deploying effective manned surveillance around the clock. In addition, flood lights installation, erection of border fences and installation of technological surveillance systems such as CCTV/PTZ cameras, IR sensors and alarms and anti-drone systems have also been deployed.[45]

To overcome the evolving drone threats, India has employed various tactics and weapons as part of its C-UAV system mainly after the drone attack on the IAF station at Jammu in May 2021. In August 2021, the Indian Navy signed an agreement with Bharat Electronic Limited (BEL) for the supply of

the Naval Anti-Drone System (NADS). NADS is the first indigenous anti-drone system developed by Defence Research and Development Organisation (DRDO) and manufactured by BEL. NADS has both a static and a mobile version, with each providing both soft-kill and hard-kill options.[46] In the following month, Hyderabad-based Zen Technologies bagged the Rs 155 Cr deal from the IAF to develop and equip the IAF with the Counter Unmanned Aerial System (CUAS).[47]

Besides the Navy and the Air Force, the Indian Army has also deployed an RF-based anti-drone system that is developed by Lt Col Sadanand Chauhan of the Corps of Signals after the Aero India show in 2023. However, the system only has soft-kill capability with a limited range.[48] Recently, Hyderabad-based Grene Robotics has developed a drone dome Indrajaal to guard wide areas against rogue drone operations. Powered by Artificial Intelligence, the Indrajaal system is designed to protect against autonomous drone swarms over a radius of 4,000 sq. km and can also differentiate between friendly and rogue drones.[49]

Nevertheless, now that India has made security preparations against drone attacks, several challenges need to be considered. Firstly, the anti-drone system deployed by the Indian Armed Forces has limited capability against miniature-sized drones. In the coming years, non-state actors may use drones of varied sizes with advanced technology to deceive radars and other detection systems. Secondly, the anti-drone systems are primarily developed to secure vital security installations and government buildings and offices based in the national capital and non-border states, however, major drone incidents have occurred in the districts of the four states along the Indo-Pak border (see Figure 1).

Among security agencies, the Army and BSF units operating near the border have been facing major challenges with the anti-drone system. For mitigation, service rifles are being used, which can cause damage to civilians and wildlife. Regarding detection measures, the anti-drone system has provided limited and unsatisfactory results. According to senior BSF officials, Pakistan-based smugglers are using old drones, parts of which are picked up from different companies and are assembled locally. Behind the self-assembling of these drones, there could be two reasons: (A) to cut down costs as compared to ready-made drones, and (B) to manipulate the frequencies of the drones to deceive radars as ready-made drones fly with fixed frequency.[50] Expressing dissatisfaction over the capabilities of the current C-UAS deployment, Wing Commander Sai Mallela said, 'Only radar-based detections are inaccurate at low radar cross section (RCS) and close to the ground which is even incapable of identifying the operating radio frequency.'[51]

Moreover, hard-kill options are more suitable near borders as in crowded areas they could inflict collateral damage, hence, soft-kill options are preferred in densely populated cities. But in either case, the role of an early and effective detection system becomes all the more important, especially in a country like India, which is densely populated. The currently available detection systems are not satisfactory in terms of their effectiveness. Additionally, the weather is playing a key role in affecting the various detection systems. Radars, which are more capable against large aircraft, often fail to differentiate between small drones and birds. Extreme weather such as rain and fog also limit the capability of radars, which need clear line-of-sight to work properly. They are also sensitive to reflection and refraction coming from different directions or water droplets suspended in the atmosphere, which results in false positives during rainy and foggy conditions. The EO/IR system works on the infrared signals of the objects, needing clear line-of-sight; rain, fog and darkness often impact its working. Acoustic systems use sensors to match the sounds produced by drones to detect them. However, they seem less effective near airports, stadiums, overcrowded places and even in heavy rain as the acoustic system cannot trace the sounds produced by the flying objects and drones, which have become quieter.[52]

Way Forward/Recommendations

India can take various lessons from its own experiences as well as from rogue drones operated in different geographical regions. In India, the threat of drones for rogue purposes arrived in 2019. The specifications of recovered drones indicate that micro, small and medium-sized UAVs have been used so far in the states that share the border with Pakistan. India's indigenisation of drones and its countermeasures have been a welcome step in the effort to promote domestic manufacturing; however, New Delhi could adopt an explicit plan by creating a balance between indigenous development and imports to meet the urgent requirements. Israeli SMASH 2000 is a system mounted on a rifle that could enhance the ground-based capability of the land forces at borders to shoot down rogue drones from a distance. India may consider the procurement of US's Advanced Test High Energy Asset (ATHENA) laser system with a transfer of technology to plug the existing loopholes in the anti-drone system manufactured domestically.

India's counter-rogue drone deployment plan has been divided into three models—full-scale, mid-scale and basic—based on vital national assets. The three models include both detection and intervention measures that are

limited to major government buildings, state secretariats and offices, national monuments, ports and nuclear and security installations. The international border and nearby areas sensitive to the nation's security are less prioritised in the deployment model. India could consider evolving a more comprehensive plan/model that includes the border regions based on the assessment of rogue drone incidents made so far, as drones operated from outside the border need to be ceased at the initial stages itself.

India can review and form new counter-rogue drone guidelines that meet the current challenges and requirements. The existing policy was last revised in 2019 when the threat from drones had just arrived in India. Since then, the number of drone incidents involving smuggling and attacks has sharply increased. Threats relating to balloon incidents in China and glider attacks during the recent Israel–Hamas conflict could also be considered under the counter-rogue drone guidelines.

Conclusion

The potential of drones as a threat can be understood by their application over the years by non-state actors and terrorist organisations. Most of the case studies on this belong to West Asia and Latin America; however, the usage of drones for rogue activities has spread steadily across different regions from Northern Africa to South Asia. Analyses indicate that Hamas, Hezbollah, al-Qaeda, IS, Houthis, Taliban, Lashkar-e-Taiba and many other fragments have accessed UAVs and associated technology via illegal means and self-assembly (DIY) kits. Some of them have even established their own domestic manufacturing facilities at covert locations for experiments and R&D. The application of UAVs by terrorist organisations has sparked a global debate regarding its prevention. The US Congress in December 2016 passed the National Defence Authorisation Act (NDAA-2017) where special emphasis was laid on counter rogue drone measures. Further, the Federal Aviation Administration (FAA) Reauthorisation Act 2018 provided authority to the Department of Homeland Security, the Department of Justice and the US Coast Guard to counter rogue drones. India also raised concern in the UNSC against rogue drone application by non-state actors supported by Pakistan's intelligence agency.

India has been a victim of terrorism for decades and now advancements in drone technology has added to India's concerns. India has responded by enabling DGCA's Drone CAR 1.0 and MHA's SOPs for countering any unauthorised and illegal drone activities at the national and state level. A

framework for policy guidelines at the institutional and judicial levels has been prepared, but the operational setup for C-UAS needs to be geared up. The existing policies and response mechanism has some loophole that needed to be resolved at the earliest. While DRDO has developed anti-drone guns to execute unauthorised and suspicious drones, the results are not satisfactory on ground, as also mentioned by the security forces deployed near the border. Aware of its technological advancement and market value, the Government of India has been paying attention to making India a drone manufacturing hub. Accordingly, the government initiated the Drone Rules in 2021 to promote domestic drone manufacturing and ease the regulation of drone activity in India. However, it is imperative that anti-drone systems or C-UAS systems be given equal importance to plug any vulnerability against drone attacks.

Notes

1. Michael Ashkenazi, 'The Future of UAVs: Lessons from the "Great War"', *Sicherheit Und Frieden (S+F) / Security and Peace,* Vol. 34, No. 4, 2016, pp. 257–62, available at http://www.jstor.org/stable/26429020.
2. 'A Brief History of Drones', Imperial War Museums, available at https://www.iwm.org.uk/history/a-brief-history-of-drones, accessed on 25 March 2023.
3. Ibid.
4. 'Iran's Drone Transfers to Proxies', *The Iran Primer*, 30 June 2021, available at https://iranprimer.usip.org/blog/2021/jun/30/iran%E2%80%99s-drone-transfers-proxies.
5. Marc Rod, 'CENTCOM Commander Warns about Iranian Drone Threat during House Hearing', *Jewish Insider*, 21 April 2021, available at https://jewishinsider.com/2021/04/centcom-iran-drones-house-hearing/.
6. Faiqa Mahmood, 'Pakistan's Indigenous Armed Drones: Precedents and Proliferation', *South Asian Voices*, 2 April 2015, available at https://southasianvoices.org/pakistans-indigenous-armed-drones-precedents-and-proliferation/.
7. Ron Friedman and ToI Staff, 'Downed Drone Managed to Transmit Photos of Joint Drill Preparations, Says Report', *Times of Israel*, 14 October 2012, available at http://www.timesofisrael.com/downed-drone-managed-to-transmit-photos-of-joint-drill-preparations-says-report/, accessed on 20 October 2023.
8. Don Rassler, 'Capabilities and Potential—Terrorists' Interest in and Use of UASs', Research Report in *Remotely Piloted Innovation: Terrorism, Drones and Supportive Technology*, 1 October 2016, available at http://www.jstor.org/stable/resrep05632.5.
9. Robin M. Frost, 'The Nuclear Black Market', *The Adelphi Papers*, Vol. 45, No. 378, 2005, pp. 11–24, DOI: 10.1080/05679320500519005.

10. Julian Borger, 'Nuclear Bomb Material Found for Sale on Georgia Black Market', *The Guardian*, 7 November 2010, available at https://www.theguardian.com/world/2010/nov/07/nuclear-material-black-market-georgia.
11. Brian A. Jackson, John C. Baker, Kim Cragin, John Parachini, Horacio R. Trujillo and Peter Chalk, 'Aum Shinrikyo', In *Aptitude for Destruction, Volume 2: Case Studies of Organizational Learning in Five Terrorist Groups* (1st edn), RAND Corporation, 2005, pp.11–36, available at http://www.jstor.org/stable/10.7249/mg332nij.9.
12. Bruce Sussman, 'The Drone Cyberattack That Breached a Corporate Network', *blogs.blackberry.com*, 21 October 2022, available at https://blogs.blackberry.com/en/2022/10/the-drone-cyberattack-that-breached-a-corporate-network, accessed on 21 October 2023; Mike Elgan, 'Why Consumer Drones Represent a Special Cybersecurity Risk', *Security Intelligence*, 7 September 2023, available at https://securityintelligence.com/articles/why-consumer-drones-represent-a-special-cybersecurity-risk/, accessed on 21 October 2023.
13. 'Ukraine War: Russian Drones Being Used to "Spread Propaganda via Text Messages", *Forces News*, 24 February 2023, available at https://www.forces.net/ukraine/ukraine-russian-drones-being-used-spread-propaganda-text-messages.
14. Emil Archambault and Yannick Veilleux-Lepage, 'Drone Imagery in Islamic State Propaganda: Flying like a State', *International Affairs*, Vol. 96, No. 4, 1 July 2020, pp. 955–73, available at https://doi.org/10.1093/ia/iiaa014.
15. Robert J. Bunker, 'Terrorist and Insurgent Unmanned Aerial Vehicles: Use, Potentials, and Military Implications', Strategic Studies Institute, US Army War College, 2015, available at http://www.jstor.org/stable/resrep11741.
16. Joby Warrick, 'Use of Weaponized Drones by ISIS Spurs Terrorism Fears', *Washington Post*, 7 April 2023, available at https://www.washingtonpost.com/world/national-security/use-of-weaponized-drones-by-isis-spurs-terrorism-fears/2017/02/21/9d83d51e-f382-11e6-8d72-263470bf0401_story.html.
17. Alyssa Sims, 'The Rising Drone Threat from Terrorists', *Georgetown Journal of International Affairs,* Vol. 19, 2018, pp. 97–107, available at http://www.jstor.org/stable/26567532.
18. 'Russia's Explanation about Who Attacked Its Bases in Syria Keeps Getting Stranger', *Business Insider*, 12 January 2018, available at https://www.businessinsider.in/russias-explanation-about-who-attacked-its-bases-in-syria-keeps-getting-stranger/articleshow/62466044.cms, accessed on 25 April 2023.
19. 'Venezuela President Maduro Survives "Drone Assassination Attempt"', *BBC News* sec. Latin America & Caribbean, 4 August 2018, available at https://www.bbc.com/news/world-latin-america-45073385.
20. Brian Barrett, 'The Explosive-Carrying Drones in Venezuela Won't Be the Last', *Wired*, 4 August 2010, available at https://www.wired.com/story/venezuela-drones-explosives-maduro-threat/, accessed on 25 April 2023.

21. Nick Waters, 'Houthis Use Armed Drone to Target Yemeni Army Top Brass', *bellingcat*, 10 January 2019, available at https://www.bellingcat.com/news/mena/2019/01/10/houthis-use-armed-drone-to-target-yemeni-army-top-brass/.
22. 'Evolution of UAVs Employed by Houthi Forces in Yemen', ArcGIS StoryMaps, Conflict Armament Research, 21 April 2023, available at https://storymaps.arcgis.com/stories/46283842630243379f0504ece90a821f.
23. 'Iran's Drone Transfers to Proxies', *The Iran Primer*, 30 June 2021, available at https://iranprimer.usip.org/blog/2021/jun/30/iran%E2%80%99s-drone-transfers-proxies.
24. Ibid.
25. 'Saudi Aramco's Jeddah Oil Depot Hit by Houthi Attack', *Al Jazeera*, 25 March 2022, available at https://www.aljazeera.com/news/2022/3/25/saudi-aramco-jeddah-storage-facility-hit-by-attack, accessed on 3 November 2023.
26. Zia Ur Rehman, 'U.S. Arms Left in Afghanistan Surface in Pakistan Taliban Insurgency', *Nikkei Asia*, 12 March 2023, available at https://asia.nikkei.com/Politics/Terrorism/U.S.-arms-left-in-Afghanistan-surface-in-Pakistan-Taliban-insurgency, accessed on 25 October 2023.
27. 'US Army Weapon Left in Afghanistan Makes Its Way to Kashmir; Terror Group Releases Video', *WION*, 20 January 2022, available at https://www.wionews.com/india-news/us-army-weapon-left-in-afghanistan-makes-its-way-to-kashmir-terror-group-releases-video-446245, accessed on 4 November 2023.
28. Sandeep Unnithan, 'Attack of the Drones', *India Today*, 14 October 2019, available at https://www.indiatoday.in/magazine/the-big-story/story/20191014-attack-of-the-drones-1605824-2019-10-04, accessed on 21 October 2023.
29. Prabhash K. Dutta, 'Decoded | Use of Drones for Terrorism', *India Today*, 29 June 2021, available at https://www.indiatoday.in/india/story/decoded-use-of-drones-for-terrorism-1820245-2021-06-28, accessed on 26 April 2023.
30. 'Pak LeT behind Drone Attack in Jammu, Target Was ATC and Parked IAF Helicopters', *Hindustan Times*, 28 June 2021, available at https://www.hindustantimes.com/india-news/pak-let-behind-drone-attack-in-jammu-target-was-atc-and-parked-iaf-helicopters-101624857978136.html.
31. 'More than 300 Drone Sightings Reported along Pakistan Border since August 2019: Agencies', *Deccan Herald*, 28 June 2021, available at https://www.deccanherald.com/india/more-than-300-drone-sightings-reported-along-pakistan-border-since-august-2019-agencies-1002523.html, accessed on 20 October 2023.
32. 'South Asia Intelligence Review', Vol. 21, No. 48, 22 May 2023, available at https://www.satp.org/south-asia-intelligence-review-Volume-21-No-48, accessed on 22 October 2023.
33. 'Punjab Police Arrest 10,576 Drug Smugglers in Seven Months', *The Hindu,* 14 February 2023, available at https://www.thehindu.com/news/national/other-states/punjab-police-arrest-10576-drug-smugglers-in-seven-months/article66507354.ece.
34. Ibid.

35. 'India Facing "Serious Challenge" of Cross-Border Supply of Illicit Weapons Using Drones: Kamboj', *The Telegraph Online*, 7 December 2023, available at https://www.telegraphindia.com/world/india-facing-serious-challenge-of-cross-border-supply-of-illicit-weapons-using-drones-ambassador-ruchira-kamboj-at-united-nations-security-council/cid/1928846, accessed on 22 October 2023.
36. 'South Asia Intelligence Review', n. 32.
37. 'Smuggling of Arms and Narcotics', Ministry of Home Affairs, Government of India, 1 August 2023, available at https://www.mha.gov.in/MHA1/Par2017/pdfs/par2023-pdfs/LS-01082023/1900.pdf.
38. Ibid.
39. 'Infiltration in Jammu And Kashmir', Press Information Bureau, Ministry of Home Affairs, Government of India, 25 July 2023, available at https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1942470, accessed on 23 October 2023.
40. 'National Counter Rogue Drone Guidelines', Ministry of Civil Aviation, Government of India, 2019, available at https://www.civilaviation.gov.in/sites/default/files/Counter_rogue_drone_guidelnes_NSCS.pdf.
41. 'The Aircraft Rules, 1937', Ministry of Civil Aviation, Government of India, 23 March 1937, available at https://www.civilaviation.gov.in/sites/default/files/moca_000947.pdf.
42. 'Government Announces Regulations for Drones', Press Information Bureau, Ministry of Civil Aviation, Government of India, 27 August 2018, available at https://pib.gov.in/newsite/printrelease.aspx?relid=183093, accessed on 28 April 2023.
43. 'DigitalSky', available at https://digitalsky.dgca.gov.in/home, accessed on 28 April 2023.
44. 'Comprehensive SOPs Issued to Security Forces to Tackle Drone Threats', *Republic World*, 19 November 2019, available at https://www.republicworld.com/india-news/general-news/comprehensive-sops-issued-to-security-forces-to-tackle-drone-threats.html.
45. 'Smuggling of Arms and Narcotics', Ministry of Home Affairs, Government of India, 1 August 2023, available at https://www.mha.gov.in/MHA1/Par2017/pdfs/par2023-pdfs/LS-01082023/1900.pdf.
46. Manjeet Negi, 'Indian Navy Signs Contract with BEL for Supply of Anti-Drone System', *India Today*, 1 September 2021, available at https://www.indiatoday.in/india/story/indian-navy-signs-contract-bel-supply-anti-drone-system-1848019-2021-09-01, accessed on 22 October 2023.
47. Abhishek Bhalla, 'Armed Forces Order Indian-Made Anti-Drone Systems Worth over Rs 300 Crore, More Contracts Awaited', *India Today,* 3 September 2021, available at https://www.indiatoday.in/india/story/armed-forces-order-indian-made-anti-drone-systems-worth-rs-155-crore-1848915-2021-09-03, accessed on 22 October 2023.

48. Sandip Dighe, 'Aero India 2023: Army Officer Develops Anti-Drone System', *The Times of India*, 15 February 2023, available at https://timesofindia.indiatimes.com/city/bengaluru/aero-india-2023-army-officer-develops-anti-drone-system/articleshow/97932785.cms.
49. Uma Sudhir, 'Hyderabad Firm Unveils India's First AI-Powered Anti-Drone System', *NDTV*, 4 September 2023, available at https://www.ndtv.com/india-news/hyderabad-firm-unveils-indias-first-ai-powered-anti-drone-system-4356902, accessed on 19 October 2023.
50. Yudhvir Rana, 'Pakistan Smugglers Using Assembled Drones to Cut Losses, Claims BSF', *The Times of India*, 1 December 2022, available at https://timesofindia.indiatimes.com/city/amritsar/pak-smugglers-using-assembled-drones-to-cut-losses-claims-bsf/articleshow/95900777.cms.
51. Uma Sudhir, 'Hyderabad Firm Unveils India's First AI-Powered Anti-Drone System', n. 49.
52. 'C-UAS State of Play Report 2022', Institute for Defence and Government Advancement, Washington DC, August 2022, available at https://www.idga.org/command-and-control/articles/c-uas-state-of-play-report-2022.