Drone Policy: Formulation, Promulgation and Implementation

Brig **Akhelesh Bhargava** (Retd), an Army Air Defence officer, was commissioned in June 1983. He has tenanted various command and staff appointments. Presently he is Chief Instructor (CI), PROMEX, CLAWS.

Drones have been in discussion for quite some time in various circles—armed forces, civil administration, police, paramilitary forces—not just here in India but the world across. What can be done and achieved is well known. An increasing number of ways of its usage is quite bewildering. Most importantly, weaponisation of drones including quadcopters/multicopters, is a cause of concern and makes the airspace to be more complicated and complex for purposes of security. A series of incidents between September 14 and 22, 2019 calls for a serious discussion on the subject.

Previous Incidents

● On September 14, 2019, drone attacks hit two major oil facilities run by the state-owned company Aramco in Saudi Arabia. A swarm of 10 explosive laden drones were used by Iran-backed Houthi rebels in Yemen. The group claimed responsibility. They targeted the site of Aramco's largest oil processing plant at Abqaiq, about 60 km south-west of Dhahran and Khurais oilfield,

Key Points

1. Drones are available the world over in different sizes, make, endurance, capacity, etc.

2. Drones' usage as a weapon of attack, arms and ammunition delivery and espionage/surveillance.

3. Many types of autopilots are available commercially which provide flight control capability to a drone.

4. For any drone carrying out a hostile act, action has to be initiated; before taking off or while flying.

5. A case for IDS to become lead agency to formulate and enunciate drone policy.

6. Need to create a grid of TCR, FCR and LLLR under Army AD in all sensitive areas for increasing the probability of detection at low level.

Drone Policy ...

the second largest oilfield of Saudi Arabia, located 200 km further south-west. The kind of damage inflicted was unthinkable; affecting half the Saudis' oil production and supply. In turn the incident sent oil prices soaring and rocked the world stock market by a few billion dollars.

- On September 22, 2019 a group of four members of Khalistan Zindabad Force (KZF) were caught delivering arms and ammunition from across Pakistan using Global Positioning System (GPS) controlled 5-kg capacity Chinese drones at the behest of ISI handlers. The drones made multiple transits (8 sorties over 10 days) to drop, 'five AK-47 rifles, 16 magazines 472 rounds of ammunition, four Chinese made .30 pistols along with eight magazines and 72 rounds, nine hand grenades, five satellite phones with ancillary equipment, two mobile phones, two wireless sets and fake currency amounting to Rs. 10 lakhs'.

- On September 14, 2019 at 1845h, two US citizens, father and son (Peter James, 65, and Guillaume Leadbetter, 31) were detained for flying a drone mounted with a camera and spotted over Rashtrapati Bhawan, New Delhi. The camera was found to contain footage of the central secretariat and nearby buildings.

Welcome to the world of drones' usage as a weapon of attack, arms and ammunition delivery and espionage/ surveillance. All the while we have been talking of the benefits of drone—be it pizza delivery, covering live cricket match, action shots for movies, live video streaming at concerts, etc.

Who needs high-tech weapons when the aim can be achieved by very low cost options? The Saudis have deployed Patriot Air Defence Missile system for the country's protection—the best system in the world costing billions of dollars and one which has foolproof surveillance capability. Yet the Houthis, using low cost multiple drones, carried out a pre-dawn successful

attack; one which took the sheen away from 'the Patriot System'. It gave Putin a chance to make a mockery of US air defence system and appealed to Saudi Arabia to rely on Russia's S-400 system.

The delivery of arms and ammunition from Pakistan through International Border Sector in Punjab is an eye-opener. The Indian surveillance radars remain on high alert 24x7. What went wrong? Not once, not twice but multiple times the drone flew in and out. How can we afford to miss out, especially when we as a nation were/are expecting some trouble from across due to ongoing heightened tension? What happened to our satellite network? What happened to our border outposts (BOPs) look-outs? Luckily the half burned drone along with the handlers were captured by police at Taran Taran.

Behold, the Directorate General of Civil Aviation (DGCA) had issued the National drone policy which came into effect just a few months back on December 1, 2018! It gives out various "Do's and Don'ts" and very specifically highlights a 'No Fly Zone' in Lutyens Delhi. The timing (1845h) of the incident calls for deep introspection and a review of the policy. The American duo seem to be innocent tourists unaware of the Indian Policy. But they had come from the US where the drone flying policy is clearly spelt out including "A No fly zone around White House".Why were they flying around 'Indian White House'?

The three incidents within a matter of days have highlighted that the world is becoming more dangerous. The use of a low cost weapon such as a drone by the Houthis and attacking from air, which even the most formidable air defence system of the world could not counter, highlights this complex situation. It calls for a review of the National Drone Policy. The requirement of active air defence deployment 24x7 over strategic assets and elsewhere has never been as relevant as now. This, in view of Pakistan Prime Minister Imran

Khan's speech in United Nations General Assembly (UNGA) on September 27, 2019, clearly stating his intention.

Drones are available the world over in different sizes, make, endurance, capacity, etc. The one type of drone which has a potential to be very dangerous is the quadcopter/multicopter. Some of their key characteristics are as follows:

- **Structure.** The mechanical components are the frame, propellers. Carbon Fibre Composite, due to their low equivalent echoing area (EEA), lightweight and structural stiffness, are being used. The electrical components are the electronic speed control module, onboard computer or controller board, and battery.

- **Autonomous Flight.** Normally a hand-held transmitter is used to control flight path manually. Presently flight controllers use software that allows user to choose 'way-points' and create a path of own choosing and carry out its tasks. Now many types of autopilots are available commercially which provide flight control capability to a drone. The autopilot also enables them to create a swarm effect with tens and hundreds of them flying in from different places/directions and converging at a point of own choosing. For a cultural event it looks good as done during closing ceremony of 'Kumbh Mela' at Allahabad on March 8, 2019. It can create a very dangerous situation if used by rogue elements.

- **Endurance.** A battery powered drone can achieve flight time of more than two hours. With high capacity Lithium batteries the flight time can be further increased. The battery operated quadcopters are very silent as compared to electric motor ones.

- **Hovering and Flight Control.** The quadcopter type drone is much more dangerous than fixed-wing type because of it capability to hover at a point, fly Nap-of-the-earth, hide behind a tree/building, pop up at a time of own choosing. All this makes it all the more difficult to detect.

National Policy on Drones

The Director General of Civil Aviation (DGCA) finally announced its policy for remotely piloted aircraft (RPA), or drones, that came into effect from December 1, 2018 superseding policy letter issued in April 2016 and November 2017. The policy defines the classification of RPA/drone, how they can be flown and the restrictions placed on their operation. It also enumerates the no-fly zones. Other important aspects are as follows:

- **Definition.** RPA is an unmanned aircraft piloted from a remote pilot station. The RPA, its associated remote pilot station(s), command and control links and any other components forms a Remotely Piloted Aircraft System (RPAS).

- As per the civil aviation requirements—issued under the provisions of Rule 15A and Rule 133A of the Aircraft Rules, 1937—the RPAs will need a Unique Identification Number (UIN), Unmanned Aircraft Operator Permit (UAOP) and need to adhere to laid down operational requirements.

- **Classification of drones.** They are five different categories as follows:
  - ○ **Nano:** Less than or equal to 250 grams.
  - ○ **Micro:** From 250 grams to 2 kg.
  - ○ **Small:** From 2 kg to 25 kg.
  - ○ **Medium:** From 25 kg to 150 kg.
  - ○ **Large:** Greater than 150 kg.

- **Import Clearance.** All drones operators, other than the nano category, shall apply to DGCA for import clearance and based on that Directorate General of Foreign Trade shall issue licence for import of RPAS.

- **Permit for Operators.** Operators of civil drones will need to get a permit from the DGCA. There are exceptions for:
  - ○ Nano RPA operating below 50 feet (15 m) in uncontrolled airspace/enclosed premises.

- Micro RPA operating below 200 feet (60 m) in uncontrolled airspace/enclosed premises—but will need to inform local police 24 hours prior.
- RPA owned and operated by NTRO, ARC and Central Intelligence Agencies but after intimating local police.

- **Restrictions on Flying.** Flying area has been divided into three zones:
  - Red zones: These are no-fly area (which include regions close to airports, national borders and military bases).
  - Yellow zones: Flying in these areas will require approvals before flying.
  - Green zones: They are unrestricted areas.

- **Penalties.** The maximum penalty for not following the policy is an imprisonment of up to two years or fine of Rs. 10 lakh or both.

Sufficiency of National Drone Policy. Is the quantum of penalty enough to deter a rogue element or a terrorist from carrying out an act of war which would end up in being a national shame? Is there a case for DGCA and the Indian Air Force (IAF)/Army AD/Integrated Defence Staff (IDS) to come together and enunciate a policy which would prevent from incidents, like the one in Taran Taran or over Rashtrapati Bhawan, from happening?

Dangerous Scenarios. How dangerous can it be? Consider the following two scenarios:

- **Swarm Attack.** An extension of what happened in Saudi Arabia. Tens of large sized drones, armed with explosives, having impact and RF fuse, equipped with Inertial Navigation System (INS) and autopilot, and fed with way points to the intended target are set off. They fly at 30 m above obstruction level (AOL) with a very low detection probability. They carry out attack in series or simultaneously. The overall effect can be as dangerous as can be imagined.

- **Hailing Application (Apps).** A sizeable number of drones armed with explosives and are equipped with 'Hailing Apps' (similar to taxi hailing app (THA)) and having simultaneous multiple hailing capability. A single smart mobile phone sets off activation signal at the point of impact and starts generating signal. The drones spread over an area, get activated, respond to the hailing signal and start moving to reach the designated destination at a specific time. Before anyone reacts to the developing situation, the explosives are detonated.

Recommendations. There is a requirement of designating responsibility and laying down countermeasures to prevent the above discussed incidents from taking place. Certain recommendations are enumerated as follows:

- **Responsibility for Policy Formulation.** Since the drone threat is both from external and internal sources; the responsibility of laying policy should be IDS. Clear demarcation of responsibility should be laid down; agency to report, agency to react, action to be taken, method of reducing collateral damage, methodology of reporting, etc.

- **Responsibility for Policy Promulgation.** There is an urgent need to promulgate the drone policy not only amongst the armed forces but also across all sections of the nation; DGCA, Paramilitary Forces, Police, Home Guard, Civil Administration and even the general population. All need to understand what constitutes a hostile act and what to do next. The lead agency should be IDS.

- **Responsibility for Policy Implementation.** To counter drone threat, we need to have low level surveillance cover, command and control structure, soft and hard kill options and training in all the aspects. These are explained as follows:
  - **Surveillance.** There is a need to increase hinterland surveillance. The radars at airports and the IAF surveillance radars deployed at the

borders are adequate but they are meant to cover medium and high altitudes whereas the drones fly at low level (below 1,500 feet). Besides, the resolution of such radars is very low both in range and bearing. The drones have very small EEA and are capable of flying at a very low level (below 30 m AOL). It is near impossible to detect and identify such a rogue entity. There is a need to create a grid of Tactical Control Radars (TCR), Light Weight Low Level Radars (LLLR)and Fire Control Radars (FCR) in all sensitive areas (red and yellow zones) for increasing the probability of detection. Since these are available with Army AD, it should become the lead agency for surveillance. These should be supplemented with the Observer Post (OP) of Army AD and Mobile Observation Flights (MOF) of IAF. In addition the high-resolution fixed and drone mounted cameras too need to be deployed and they need to be procured. The surveillance has to be made a 24x7 activity.

○ **Control and Reporting.** While the IAF Integrated Air Command and Control System (IACCS) exist,however, there is a case for extending it into the hinterland and cover low level threat with Army AD being made responsible. The drone threat can emanate from anywhere including from within due to availability of modular drones that can be carried in parts and assembled easily. There is also a need to integrate the Air Traffic Control (ATCs) into the system for implementing the control orders. Doing it alone by a single agency will require heavy manpower and will be too cumbersome.

○ **Countermeasures.** For any drone carrying out a hostile act, action has to be initiated; before taking off or while flying; active or passive depending upon the location and the need to protect against collateral damage. Army AD

assets have to be integrated into the overall plan. Command and control of troops deployed for the purpose too have to be legislated and coordinated. The options are as follows:

□ **Quick Reaction Teams (QRT).** QRTs from the forces (army, PMF, Police) should be earmarked in respective areas of responsibility (AOR) to detain or capture elements,wherever and whenever a doubt occurs and a report is received in the control room. A drone captured on ground along with its handlers is the best thing to happen.

□ **Guns and Missiles.** Use of Light Machine Gun (LMG), Medium Machine Gun (MMG), AD Gun (ZU-23-2B) and man portable Surface-to-Air Missile (Igla-1M) are some of the weapons that can be used against hostile drones. However a K-kill may result in debris being created which may cause collateral damage.

□ **Co-flight Drone.** Own drone armed with small quantity of explosive or armed with spikes or DEW or jammer can be used to intercept, disable, destroy or crash into the rogue drone and prevent it from reaching the intended target.

□ **Directed Energy Weapons (DEW) and Others.** The DEW, Laser guns, Electromagnetic Pulse (EMP) and high-powered microwaves are a means of destroying hostile drones. However, India is just in the nascent stage of developing these methodologies. They will certainly be quick to deploy and initiate action.

□ **Soft kill.** Since any drone will have a Radio Frequency (RF) based controller both for flying and for triggering explosives, high-powered jammers will be able to jam and render them useless. There will be

... Formulation, Promulgation and Implementation

requirement of a highly efficient RF detection and analysing system or else broadband jammer has to be used.

□ **AD Aircraft.** The last resort, especially for large drones, the IAF may use its AD aircraft to snuff out the attack using front guns, rockets or air-to-air missiles (AAM).

□ **Legal Provisions.** There is a need for more severe legal provisions to ensure required deterrence in case of any misuse of these Remotely Piloted Aircrafts (RPAs).

● **Training and Education.** Training and education on drones and associated danger need to be taken up on a national basis to increase people's awareness. The Army AD College, Gopalpur has the wherewithal to carry out training on a mass scale, including for the civilian agencies.

The recent incidents have highlighted the manifold increase in danger level from drone attacks of varied kind. The National Drone Policy needs a rethink and a comprehensive review. The IDS should become the lead agency for policy formulation and promulgation and Army AD be the lead agency for implementation. The awareness level of the forces as well as the entire population is a point of urgent concern. Countermeasures against drones need to be put in place with quick reaction and response to avert damage or destruction to anything of national importance.

References

1. Requirements for Operation of Civil Remotely Piloted Aircraft System (RPAS) issued by DGCA on August 27, 2018 and effective December 1, 2018.
2. "Drone attack in Saudi Arabia hits world's largest oil processing facility," dated September 14-15,2019.https://www.cbc.ca/news/world/drone-attack-saudi-arabia-yemen-houthis-1.5283837.
3. Mohammed Ghazali,edited by Debanish Achom, "Pak drones flew low, dropped weapons in 8 'sorties' in Punjab,"September 25, 2019.https://www.ndtv.com/india-news/pakistani-drones-flew-low-dropped-weapons-in-8-sorties-in-punjab-say-sources-2106713.
4. Bobins Abraham, "Two US citizens arrested in Delhi for flying a drone near Rashtrapati Bhawan, photos of high-security areas recovered," dated September 16, 2019. https://www.indiatimes.com/news/india/two-us-citizens-arrested-in-delhi-for-flying-a-drone-near-rashtrapati-bhawan-photos-of-high-security-areas-recovered-375831.html.