Reinventing Border Management: Drone Threat in Border Areas

On 14 September 2019 at 4.00am, Saudi Arabia suffered a deadly attack on its oil facility at Abaqiq and Khurais oil field, with, as stated, swarm of 18 small drones and seven cruise missiles. Very highly protected and fortified facilities, in addition to armed guards, the area had six battalions of Patriot Defence Systems, *Oerlikon* GDF 35mm *cannons* equipped with the Skyguard radar and Surface to Air Missiles (SAM). The targets were designated with pin point accuracy and hence the strikes were most effective. It destroyed nearly 50 per cent of the country's global supply of crude. The crude prices rose sharply in the international market that saw the US Secretary of State proclaiming it was an 'Act of War'. By exactitude the perpetrators were unidentified, even the trajectory of the flights of the missiles and drones could not be ascertained; only remnants of a Quds1 missile (linking it to Yemen) were displayed. The conjectures are aplenty – from drone swarms, to cruise missiles, to stealth aircraft and even ground action! This is also fallout of the usage of this modern war weaponry – plausible deniability!

Is this methodology of using drones as offensive weapons new? In 2015, a man protesting Japan's nuclear policy dropped a drone carrying radioactive sand from the Fukushima nuclear disaster onto the Prime Minister's office premises, though the amount of radiation was minimal. In January 2015, a drone crashed onto the White House lawn after its operator lost control, prompting concerns that the US President's residence may be vulnerable. In July 2018, in the UAE, terrorists claimed to have sent an armed drone to attack the international airport in Abu Dhabi, the capital of the United Arab Emirates, a claim denied by the authorities. In August 2018, a failed assassination attempt against Venezuelan President Nicolás Maduro was mounted with explosive-armed drones in Caracas during a televised national event. The drones detonated explosives above the audience, which led to a few injuries. There had been previously too reports of drone strikes by the Yemeni Houthis against Saudi Arabian targets. In March 2017, the BBC quoted US Gen David Perkins in a symposium that a Patriot missile – usually priced at about $3m – was used to shoot down a small quadcopter drone that costs US $200 at Amazon.com!

The major one was in Jan 2018, when mysteriously a swarm of ten drones rigged with explosive devices descended over Russia's Hmeimim air base in Syria while a further three targeted the Russian Naval CSS point in the nearby city of Tartus. Russia claimed to have shot down some of the 13 drones, and used electronic countermeasures to safely bring down the others, and that no serious damage was caused.

Closer home, between 09 and 16 Sep 2019, in Punjab, high alert has been sounded after multiple (stated to be ten) drones flew from across the border in Pakistan to drop arms and ammunition. In ten days attempts were made to drop AK-47 rifles, counterfeit currency and narcotics, from Pakistan. Previously too Punjab Police had recovered of a crashed 'Hexacopter Drone' on 13 August 2019 from Mohawa village in Amritsar district – a mere 1.5 kms from the Indo-Pak border.

India as a nation with its very large population is vulnerable internally too, with inimical elements seeking to avail of opportunities for disruption. A data estimation study stated that over 6 lakh unregulated drones, of various sizes and capacities are present within the country and anyone of them can be used for launching a nefarious act by disruptive elements. However, this is a subject of another analysis, and this paper will restrain itself and delve into threats in border areas.

With the intransigent attitude of the Pakistan, the border areas are greatly susceptible to this fast emerging and potent threat. In the border areas, the drones could be utilised for surveillance, spying and tracking, to electronically send video, images and other data to enable spatial reconstruction, reconnaissance and tracking movements. These can also cause physical attacks, drop dangerous explosive payload, weapons and ammunition and even subversive literature. As is evident in Punjab, it is feasible to smuggle in contraband like fake foreign currency and drugs using drones. These can be nano, micro, small, medium and large based on their weight, or their threat or damage potential.

The first and basic issue is detection of drones, which are much harder to detect that manned aircraft, especially if they fly below the radar envelope. There are varied of methods that can be utilized like human observers (sentries or villagers), who can use their smart phones to capture photos of detected drones and obtain confirmation from a centralized database. Radio Frequency (RF) scanners and spectrum analysers are primarily used to detect drone radio signatures by detecting bands that are known to be used by drones and other radio signatures. In dark conditions, thermal cameras and electro-optical gadgets can be very effective. Acoustic/ aural detection methods use microphone array to detect drones by analyzing the noise of the rotors, and these are not dependent on the line of sight or the size of the drone. Monostatic radar (transmitter and receiver) is a method of drone detection, which can detect the electromagnetic waves (EM) reflected from objects in order to determine a drone's range, speed, and velocity. However, the detection of the smallest consumer drones requires high frequency radar system, and for distinguishing between a drone and a bird, machine learning algorithms will have to be utilised.

Second important issue is of interdicting unauthorized drones and neutralizing their threat. Most of the methods being contemplated are either physical interdiction like a close-in weapon system to shoot to kill or exploit vulnerabilities in the communication systems of drones, which we can be termed as hacking. Sensor based interdiction (also called spoofing) can be used against drones containing motion sensors, gyroscopes, obstacle avoidance sensors, camera sensors and many others used for various flight functions. This would typically disrupt or spoof the sensor outputs of the drone to receive error signals and the drone is likely to either crash or activate an internal safety manoeuvre to land safely. Spoofing the GPS to force a drone to change its preprogrammed mission plan to another safe one is also a common interdiction methodology. The RF jamming guns typically disrupt transmission of radio signals communications between the drone operator and the drone thus breaking the communication link and initiating a default "return to home" or a "stand-by" and hence neutralising the threat.

The all important question that emanates is whose task it is to detect and destroy the unwarranted intrusion of the drones from across the borders, in peace and during hostilities in India. The responsibility for manning and guarding borders in peace time is of Central Armed Police Forces (BSF and ITBP), and in war is of the Armed Forces. Obviously, division between peace and war has been blurred; the case in point is the drones that carried war-like stores into Punjab recently.

The threat is so omnipresent and omnipotent and a newer manifestation, that a planned system must not be delayed inordinately. Hence, there is need to reinvent the border management aspects that deal with the threat that emanates from UAVs. Indian Army and Airforce have to undertake conjoined planning to this end. Following pathways are proffered:

- The Regiment of Artillery is responsible for Surveillance and Target Acquisition (SATA), deployed as units and subunits, under field formations. This systemic has outlived its utility. Dissolving the existing system of SATA units, it is recommended that the border areas be divided into SATA sectors that are permanently allocated responsibility – as an example, from River Ravi to NH1 and NH1 to River Sutlej. This permanence will be most advantageous for sectoral specialization, in creation of data bases that can be electronically correlated, and deciphered. The movement of

SATA units to differing operating environments will stand obviated, and with hybrid detection equipment and sensors, real time information will be generated. The transition to war scenario will also be seamless.

- In addition to physical (sentries and villagers), detection should be in real time organised in a gridded system with multi-modal sensor utilisation.
- A border-secure Air Defence / electronic warfare (EW) sectoral environment of permanent nature will be of immense advantage for targeting. This will involve direct kill using ground/ air based weapons and air defence. The EW establishments must be equipped with a system of jamming/ neutralising the terminal guidance.
- A secure communication and decision support system will be mandatory to link between detectors, destroyers and decision makers in peace and during war in a seamless manner, with requisite data base that will correlate in real time.

In sum, the threat from drones and their swarms is real, very serious and on the head – that is immediate. This mandates re-invention of border management and taking over this responsibility by the army and airforce in coordination with border guarding forces and even local inhabitants. We have to accept the challenge in all manifestations and work to deny advantage to the adversary. The threat cannot be allowed to be shackled by battle of the turf among multitude of agencies, or on human resource management issues.