Expanding Anti-UAVs Market to Counter Drone Technology

Dinakar Peri

In the wee hours of the morning of January 26,2015,a small quad-copter named DJI Phantom available in the market for a few hundred dollars, crash-landed on the lawns of the White House, the official residence of the US President. The sophisticated radars of the White House failed to detect the incoming drone, as it was too small and Secret Service officials who saw the drone did not know how to intercept it. It was later revealed that it was flown by a government employee a few blocks away who lost control over it and the drone accidentally landed on the lawns. Nonetheless, this incident raised several questions on the security of the President of the United States. The White House incident is one in a series of several drone breaches that have happened across the globe in the recent past, from Japan to France.

While these incidents were either accidents or attempts of activism, they brought to the fore the threat posed by such drones proliferating across the globe and available off the shelf for a paltry amount.Then there is the threat from larger Unmanned Aerial Systems (UAS) being increasingly acquired by nations across the globe by virtue of their low cost as also low risk as there is no human on board. India too is not immune to such threats. The recent use of quad-copters to deliver pizzas

Mr **Dinakar Peri** is Defence Correspondent for *The Hindu*.

and medicines is proof of this. If an Unmanned Aerial Vehicle (UAV) can deliver a pizza into the wrong hands, it can deliver deadlier stuff too. Adding to that, during every major national celebration, there is an advisory from the intelligence agencies of the possibility of terrorist groups employing UAVs to carry out attacks on VIPs or key targets. This is a reminder of the threat level India has from errant and rogue UAVs.

Counter-UAV Technologies

Nations usually have Air Force fighters and missiles on standby as part of their Air Defence (AD) protection. But in the case of threats from small drones, they are null and void. So how does one detect, target and neutralise threats from UAVs? There is no one single solution but a range of options needs to be employed. To handle such threats, countries and companies are investing huge amounts in developing counter-UAV technologies and while they are still in various stages of development, important progress has been made recently. On the other end of the spectrum, two major developments in this direction showcase the progress made in the developing counter-UAV technologies. One is a test by the US aircraft major Boeing in which a small drone was shot down with a high energy laser and the second is a project underway by Thales as part of a French government project to bring down intrusive and non-responsive drones.

In the first case, in early August 2015, Boeing's Compact Laser Weapon System (CLWS) used a 2 kW laser to shoot down a UAV during Exercise 'Black Dart'. The CLWS system did this by pointing the laser beam on the tail of the UAV at Point Mugu in California, for 10-15 seconds which burnt the tail and the UAV veered off course and crashed due to the resultant instability.CLWS is a relatively small,two-man portable system and, according to Boeing, it identified and tracked ground and airborne targets from ranges of up to 40 km, with a mid-wave

infrared sensor.In an earlier case, Boeing had shot down a small drone with a vehicle mounted laser system.

But lasers are not the only way of shooting down drones. After several incidents in France, most notably when two unidentified quad-copters were seen overflying a French nuclear power plant in 2014, the French government began a programme to develop the requisite technologies. Since then, there have been 59 unauthorised flights over critical infrastructure in France. The result was project ANGELAS—"Systematic Analysis and Global response to UAS threats to critical infrastructure and events"—coordinated by ONERA, the French Aerospace Lab, and seven industrial and academic partners. The 18-month project initiated in March 2015 is intended as an experimental developmental project in the framework of civilian applications for combating non-cooperating UAS. During a visit to Paris as part of a press tour ahead of the Paris Air Show 2015 on the invitation of Thales, this writer had detailed presentations on the technologies under development by Thales, both as part of the project and beyond. Thales is responsible for three parts of the project: electromagnetic sensors and neutralisation technologies; surveillance, tracking and system supervision; and test and evaluation which include validation and exploitation.

To detect and locate a hostile UAV, Thales has put forth a combination of its radar, acoustic detection, direction finders, radio and video locators, and laser scanner technologies. Once detected, neutralisation can be achieved by a variety of methods: kinetic force (anti-aircraft guns or sniper rifles), through laser dazzling, selective jamming, GPS (Global Positioning System) spoofing (to take control of the UAV), electro-magnetic pulses, or by interception using another UAV equipped with jamming equipment. Thales has also made some progress in ways to defeat Combat UAVs (U-CAVs). Though an overview was provided, company officials declined to give specifics due to the confidential nature of the project. The typical process of neutralising a hostile drone involves

several steps: detection, identification and neutralisation. Each step has its own set of challenges.

Detection The major challenge in tackling UAVs is their detection. Particularly, the smaller drones cannot be detected by most radar networks and can be easily mistaken for a bird. Even if the existing high end radars are tweaked or their software upgraded to detect the smaller drones, they will buzz at every bird or tree fluttering in the wind. This is exactly what happened in the incident at the White House. The small drones have small signatures at all levels: visual, thermal, acoustic and electromagnetic. Even the high end UAVs are tough to detect as they are capable of flying at very high altitudes beyond the range of normal radars and have lower signatures compared to manned flights. Detection can be done by active and passive methods. Active detection is done by air defence radars which can range from doppler to pulsed array radars. But most active radars in the air defence role today need some tweaking to perform this role. Passive detection is by direction finders, coherent locaters and acoustic sensors. The advancement in passive technologies has enabled this which is also cheaper than active technologies.

For instance, Drone Shield a start-up based in Washington DC, has developed a specialised product which has a network of acoustic sensors capable of identifying incoming drones from their buzzing sounds alone, from 1,000 yards away, and then sends alerts via text message or email. Drone Shield was recently selected as part of security measures for the Boston marathon. And once identified, to take the UAV down, Drone Shield developed a portable net gun which shoots a net to trap the incoming drone. But this can be employed only against mini and micro-drones flying at low altitudes.

Identification and classification of the detected threats can be done by electro-optic or infrared sensors, Electronic Intelligence (ELINT) and acoustic sensors. This is probably the easiest of the three steps in handling drone threats. However, drones range from mini and micro recreational

UAVs to large tactical and high endurance military drones, there is need for effective integration of all the assets to enable precise identification of the threat at short notice so to deploy the appropriate counter-measure to neutralise it.

Neutralisation: There is a range of options for this based on the kind of incoming threat detected.

Kinetic Kill is currently the most relied and preferable option. The response options can range from shooting down with sniper rifles, to anti-aircraft guns and missiles and even deploying fighter aircraft, depending on the situation.For low flying drones, attempts have been made to shoot them with high powered sniper rifles. This is very tricky and demands a high level of skill and expertise on the part of the shooter.For larger UAVs and U-CAVs which are easier to detect, usually fighter jets can be pressed in or taken down with Surface-to-Air Missiles (SAM). There are challenges even there as modern MALE (Medium Altitude Long Endurance) and HALE (High Altitude Long Endurance) drones fly at very high altitudes as there is no human element on board which limits the utility of fighter aircraft and missiles beyond a certain point.

The indigenously built Akash Short Range Surface-to-Air Missile (SR-SAM) system is indeed capable of shooting down UAVs upto a range of 25 km as claimed by officials of Bharat Dynamics Limited which manufactures the system.

Lasers can be used in both detection by way of scanning and neutralisation, with high energy beams focussed on the drone to physically burn the drone or a part of it. The earlier mentioned example of Boeing is a case in point. Several countries are experimenting with lasers as they present a relatively less expensive and logistically easier solution compared to other kinetic methods. Full scale development of laser weapons is underway across the globe and India's Defence Research and Development Organisation (DRDO)too has taken up projects to develop high intensity laser weapons.

Jamming is a much safer option than kinetic kill but is a tricky one as modern UAVs are specifically encrypted to withstand these very attempts. Experts say that to accomplish this, the target UAV should be identified and then targeted with an electromagnetic signal strong enough to overwhelm the system's controls. But there are certain limitations. Plain jamming can push the UAV out of control which is risky in crowded areas. Spoofing is a much better option but also technologically challenging and involves taking operational control of the incoming UAV. For the high end military UAVs, jamming is extremely difficult and, at present, the best way to bring them down is kinetic measures. According to an Army officer with expertise on the subject, "While jamming is an option, it will result in an uncontrolled crash causing collateral damage. You need a powerful transmitter to not only jam the drone's communication links but also take control of it so it can be landed safely." This brings the issue of GPS spoofing which enables the control part.

GPS Spoofing is the best option for neutralising a hostile drone as it not only removes the threat but also gives access to the adversary's technology intact for analyses. In this, the drone is essentially confused to forget its waypoints and go into auto-pilot mode and in this stage using power transmission, it is directed to obey new commands. A noteworthy example here is Iran which has twice taken down US drones in the past. In 2011, the RQ-170 Sentinel stealth UAV which was spying on Iran's nuclear facilities was brought down by Iran. Iran claimed that its cyber warfare unit had jammed the drone's communication and by GPS spoofing, made the drone land in Iran which seems believable as the drone, which was later displayed to the world as proof of Iran's claims,was unchanged and intact. Again, in 2012, Iran took control of a US Scan Eagle long endurance drone.

In Reference to the Indian Scenario

In India and the Indian subcontinent, there is a major proliferation of civilian as well as military drones. For instance, according to reports in *China Military Online,* China had in August conducted the maiden flight of its heaviest attack and reconnaissance drone, the Caihong 5 (CH-5) or Rainbow 5, at an undisclosed airfield in Gansu province. This is one of the several active UAV development programmes China is pursuing simultaneously. On the other hand, Pakistan has been procuring UAVs in large numbers from the US and China. This translates into increased surveillance on Indian border movements and air space violations, as has been witnessed in the recent past. The Indian armed forces have hardly any options at their disposal to specifically address these threats. While India too employs UAVs in large numbers for a range of tasks, it is high time the country pays enough attention to developing counter-UAV technologies.

In conclusion,as drones become cheaper, sleeker, smaller, agile, faster, stealthier and deadlier, the threat and nuisance posed by them will only go up manifold at various levels, ranging from individual privacy to national security. With that in mind, there is tremendous effort both in terms of effort and money being invested in the development of counter-UAV technologies. So it is only a matter of time before reliable and redundant methods of bringing down UAVs become mainstream and widely available.