New Threat Vector and the South Asian Milieu

Debashish Bose

In the month of March 2017, an attack took place on an ammunition depot at Balakliya, Eastern Ukraine. Balakliya is said to be the largest ammunition dump in the world. The attack was carried out using a small drone, which was loaded with a one-pound Russian ZMG-1 thermite hand grenade. Thermite is a pyrotechnic substance, a mixture of iron oxide Fe_2O_3 (rust) and aluminium powder. When it is ignited, the aluminium powder reacts with the O_3 part of the rust in a highly exothermic reaction, and the resulting product is molten iron. When ignited, thermite produces very high temperatures (over 4,000 degrees F), along with generous amounts of molten metal, which can easily get through wooden crates to detonate the ammunition inside. The resulting massive explosion and fire destroyed some 70,000 tons of ammunitions, which costs close to a billion dollars. One person was killed in the attack and five were injured.

This is not the first attack that Ukraine has faced from the Russian Army and its proxies. There was an earlier attack on the same base in December 2015. In that incident, the drone dropped 14 grenades, but the fires were all extinguished. In end October 2015, a similar attack had taken place on an ammunition dump at Svatovo, Ukraine. In that incident, 3.5 tons of ammunition had been destroyed, in addition to

Colonel **Debashish Bose** is Senior Fellow, Centre for Land Warfare Studies, New Delhi.

N.B. The views expressed in this article are those of the author in his personal capacity and do not carry any official endorsement.

almost completely destroying the town. Similar incidents occurred this year at an ammunition storage depot in Zaporozhye region, in Gordovka village, and at an Army training facility at Donetsk.

The Islamic State (IS) in northern Iraq has also effectively used this attack vector. In fact, it had announced the setting up of a Mujahideen Unmanned Aerial Vehicles (UAV) unit. This unit was supposed to be equipped with a fleet of drones fitted with bombs. There were claims of a number of successful hits. Kurdish forces spotted these drones at least as early as the winter of 2015. On October 02, 2016, in Irbil, Iraq, the French Special Forces members along with two Kurdish soldiers, had intercepted a drone of the Islamic State. They were trying to take the drone back to the base to deconstruct it and analyse the technology. However, the drone was booby-trapped and it exploded in their hands. It led to the death of the two Kurdish soldiers and injuries to the French Special Forces members. The attack was possibly the first where a drone fitted with an improvised explosive device inflicted casualties on troops from a Western nation. Compared to the expensive military drones used by the United States for attacks, the IS is converting small, cheap commercial models into one-way weapons.

Things have progressed to such a stage that the Iraqi federal police has, in turn, used these low cost, commercial off-the-shelf drones to attack the Islamic State. In the month of March 2017, there were reports that the Iraqi federal police had been surveilling Islamic State positions in western Mosul and attacking using weaponised quadcopters, giving them a taste of their own medicine. The Islamic State has conducted numerous drone attacks during the Mosul campaign and now after its defeat at Mosul, there is no reason why its expertise should not spread out of the war zones. Thus, the day may not be very far away when Islamic terrorists use the same against civilian targets with explosives as payloads or even chemical/biological weapons.

Closer to home, it was reported in 2013 that Al Qaeda operatives in Pakistan have developed small attack drones. The engineers were in the stage of testing their work when the police discovered them. This kind of attack is a new threat vector for destroying ammunition depots, and attacking camps where troops are staying in tents, carrying out training in the open—equally applicable in the Indian context also. In fact, this is an elegant attack method because of its stark simplicity and innovativeness. This kind of attack implies that low cost equipment, available off-the-shelf in commercial stores, which can be procured by any person without any restriction, can now be very easily converted into effective weapons for causing very respectable amounts of damage. Thus, supposedly harmless toys have been converted into lethal weapons. The icing on the cake is that this whole activity can be undertaken by an amateur as a Do It Yourself (DIY) activity, with no specialisation required.

This is also a new threat vector because the attacker does not have to bring the explosive to cause the explosion. The explosive is already available at the target site. In the words of Thomas Hammes, the attacker just brings in the detonator. In this kind of attack, it is not only the ammunition dumps which are vulnerable, other kinds of sites could also be extremely sensitive, for example, sites storing highly inflammable fuels/chemicals/fuel dumps. The storage facility of dangerous chemicals might not explode when targeted, but if the chemical leaks, it can have disastrous effects. We all remember the Bhopal Gas Tragedy of 1984 and the number of deaths that it caused. Heavy capacity aircraft, which have been refuelled and are parked, waiting for take-off, will also be vulnerable to this kind of attack, since their wings would be laden with highly flammable aviation fuel.

To counter this type of drone warfare, countries are investing in everything from eagles to lasers to special rifles for jamming control and communication signals. The Pentagon has announced an amount of $20 million for the development of counter-drone weapons because of the drone threat arising from the IS. The Americans have also made an anti-drone rifle. Rather than destroying a drone by shooting it down, the Battelle Drone Defender stops drones by jamming the Global Positioning System (GPS) and radio signals, causing it to lose contact with its pilot and, if possible, to make it land. The Defence Research Advanced Projects Agency (DARPA) plans to develop anti-drone lasers by 2020. To begin with, lasers are costly to build, but once developed, they are an economical option, because a shot of directed energy is cheap, so one laser system could shoot down many cheap drones, without using super costly missiles or lots of bullets to do so. Also, there is very low collateral damage. Even now, the US Army is alive to this threat. The Pentagon has given all US bases across the country permission to shoot down private and commercial drones that could pose a threat.

Attempts to physically stop drones will be a never-ending battle, because of continuous improvements in technology, however, in the meantime, we need to pay attention to improving the security layout of the targets, such as the layout of fuel and hazardous chemical storage facilities, the layout of bases where such threats are anticipated, and ensuring that all ammunition depots do not have open ammunition storages. While the damage done by bigger drones may not be stoppable, in this case, we are only looking for the attack vector using smaller, commercial off the shelf drones with a single grenade/small explosive.

Other collateral damage that unrestricted drone flying can cause is collision with commercial aircraft. One of the latest reports of a collision between a commercial aircraft and a drone is of a Skyjet flight on October 12, 2017. A drone struck the aircraft when it was going to land at Jean Lesage International Airport at Quebec City. Though the aircraft suffered only minor damage, such accidents can be deliberately engineered as terrorist attacks. However, in general, such incidents tend to be taken lightly. Thus, there are no clear-cut instructions to tackle this threat. In other countries also, there are general rules regarding drones endangering flight safety. Any violations of the rules can lead to fines ranging from $400 to $1.9 million and/or prison. Generally, all airports and helipads are "No Drone Zones".

The other problem of the existing regulations is always the excuse about ignorance of orders. A case in point is the unintended landing of a drone on the lawns of the White House. On January 26, 2015, a 31-year-old individual by the name of Usman, lost control of the drone (Phantom FC 140) he was flying and landed the same on the grounds of the White House. This particular drone cost only $400 and belonged to a friend of the individual. At 50 ft from his window, he lost control of the drone and it stopped responding to his commands, shot into the sky and eventually faded from view. This kind of incident in drone user parlance is called "flyaway", i.e. the situation when the drone stops responding to commands. After this incident was reported, the drone's producers issued a firmware update that created a "no fly zone" that extended 25 km around the Washington DC area. This is particularly of interest, because once sensitive areas are identified, the authorities can ensure that geo-fencing of such areas is carried out before the drones are sold in a particular area. The company on its part clearly says that it condemns illegal and unsafe use of aerial technology. The company has updated its no-fly zone list to include international airports, government institutions, and national borders throughout the world. The settings on the drone permit the lowering of height limits to follow local regulations. The other practical problem that was identified in this case was the fact that drones users, particularly recreational users, are flying the machines purely for fun and entertainment. They are generally not aware of the existing instructions and the problems that their drones can create. There is no structured process wherein every drone sale can be monitored and followed up with briefings of usage/test of usage. Additionally, everything falls flat if the owner is not using the drone and his/her friend is operating it.

Another major incident, which clearly highlights the terror threat potential of drones occurred in Japan in April 2015. A 40-year-old individual by the name of Yasuo Yamamoto, living in Fukui Prefecture in western Japan, landed a radioactivity-contaminated drone on the roof of Prime Minister Shinzo Abe's office. The aircraft was found laced with traces of Cesium 134 and 137, which were discovered in a container attached to the 20-inch craft. Fortunately, the individual did not have any malicious intent: he had carried out this action purely to protest against the use of nuclear power in Japan. As per the local rules, he was charged with "obstruction of official business", and given three years in prison and a fine of $4,180. As expected, at the time of the incident, Japan did not have any clear-cut legislation governing the use of drones. Things went into motion after the occurrence of the incident. Interestingly, both the above two incidents involved drones manufactured by a Chinese company, named Da-Jiang Innovations (DJI). Though this may sound as an interesting statistic, the fact of the matter is that more than 60 per cent of the global civilian-drone market comprises drones made by DJI.

DJI has been the favourite off the shelf drone supplier of the US Army. American soldiers in various government missions use these drones. However, things changed recently when the US Army Aviation Directorate issued instructions banning the use of DJI drones. This ban came into effect because certain cyber vulnerabilities were detected in the drones. It was anticipated that DJI could gather location, audio, and even visual data from flights made by the users of the drones. The location information and the media data from the drone could potentially reveal information about operations being carried out by the US Army. Once this possibility was detected, it was felt that any hacker could then use this information, even if DJI did not. If that happened, it wouldn't be without precedent. In 2009, terrorists had intercepted unencrypted Predator drone video feeds. As far as the manufacturer was concerned, it needed to monitor the flight control app to improve flight safety and to ensure that the system had the latest versions of the local maps and geo-fencing data, correct radio frequency, sufficient power, etc. Notwithstanding all this, DJI promptly reacted to the ban and has now rolled out a "Local Data Mode", which disconnects the drone from the internet during flights. The implication is that the DJI app and, in turn, the servers would not receive any flight path information, video or photos when the drone is being operated by the user. Thus, we see that even legitimate and properly licensed drones can be hacked for unlawful activities.

Drone technology is progressing in leaps and bounds. The military application of drones found its watershed moment during Operations Desert Shield and Desert Storm when UAVs provided direct support to the ground forces in combat for the first time. As far as military use is concerned, drones have now become micro drones, exploiting swarm technology. In fact, the US Navy launched 103 micro drones (Predix drones) from three fighter jets, to demonstrate the swarm technology. Earlier, the Chinese had been ahead with a swarm of 67 drones flying together. The latest test of 103 drones has put the US back into the lead. In such a situation, micro drones are controlled collectively by a single human operator, but act autonomously within themselves. Essentially, all the drones are synchronised for the larger objective, but within the swarm, each drone has sufficient autonomy to act on its own for smaller objectives. These drones communicate autonomously with each other and use collective decision-making to coordinate movements, finding the best way to get to a target, even flying in formation and healing themselves – all without any kind of human assistance/direction/intelligence. Micro drones further reduce the cost of ownership for the drone, and if used in large numbers, they can achieve unimaginable results. The biggest strength/worry in case they are used by terrorists is the fact that they are virtually unstoppable, because they can absorb multiple attacks on themselves and keep moving for the final objective. This is primarily because of their distributed nature. Another worrying aspect of the swarm drone technology is the fact that they are terrain agnostic, thus, they can be used on air, water and land. Hence, in the wrong hands, they can become a scourge for maritime shipping. We have already seen the capabilities of autonomous boats as demonstrated by the US Navy. It is because of such features that Armies around the world are showing keen interest in drone development. The US Navy programme is called "Low Cost Unmanned Aerial vehicle Swarming Technology" (LOCUST). The Russian anti-swarm technology is called "Repellent". The UK and China also appear to be developing their own indigenous swarm technology. There is already talk about the next generation of swarm drones as cluster bomb drones. Instead of normal clusterlets, which just fall, the cluster bomb drones would navigate to the given target once released. They're also known as "suicide drones" or "kamikaze drones" as they are programmed to explode on impact, with no intention of being recovered. As far as India is concerned, there are no inputs regarding development of this technology.

Now let us take a closer look at India. The Directorate General Civil Aviation (DGCA) first issued a public notice in October 2014. This public notice implemented a total ban on drones in the Indian civil air space by any non-government agency, organisation or individual, for any purpose whatsoever. Thereafter, in the first half of 2016, DGCA issued a draft circular for obtaining unique identification numbers and operation of civil unmanned aircraft systems in India. The draft circular categorises drones into four categories of micro, mini, small and large, as per their weight. The draft guidelines also recognise the height of 200 ft, up to which anybody can fly a drone in uncontrolled air space, though it also talks about granting of permission by the local civil administration. Thus, flying of drones without permission is illegal in India, however, selling them is not illegal. So you can buy a drone from any online market place.

In the case of India, it is more important that a concerted effort be made to regulate the drone technology, to avoid a situation where each state brings out its own regulations. In case that happens, we will have a situation where terrorists may exploit the weak regulations of certain states to exploit this technology for their mala fide intentions in the rest of the country. On August 20, 2017, at the Indira Gandhi International (IGI) airport, flight operations were brought to a grinding halt for 45 minutes, with all three runways being shut as a "precautionary measure". The result was that at least 35 flights were affected during the period as departures were stopped, and incoming aircraft were asked to hold or divert. This happened because a drone-like object was spotted in the area, causing a security panic and highlighting the need for tighter rules on unmanned aircraft. This was not the first time spotting in the history of the IGI airport. Thus, it appears that this can become a real threat very soon in our context. Incidentally, a large number of farmhouses are located near the IGI airport. These locations are regularly let out for marriage ceremonies, and nowadays, aerial photography in marriage ceremonies is in great demand. Though everybody knows that flying drones in this area is banned, unscrupulous photographers are ready to oblige. They have their own self-imposed restrictions such as not flying above 20 ft, and dismantling the drone after every 10 minutes of usage so that it cannot be tracked. The police also conduct surprise raids on these locations but the point is that if the drone is caught once it is being used, and then the entire purpose of blocking these drones is defeated. Such local demands as in marriages ensure that a huge number of such drones is available in the environment, thus, posing a grave risk of being available for misuse.

There is no clarity yet as to what is the best means to circumvent this new threat vector. Till then, a lot of our establishments and physical layouts may require a second look and thereafter restructuring, so that they can effectively face this threat. However, experts the world over are unanimous in their opinion that drones, in combination with Improvised Explosive Devices (IEDs) are going to be the future weapon of choice for insurgents and terrorist groups. Another concept that the drone war is changing is the fact of asymmetry. For the advanced Armies using drones, it seems like very little risk with very little pain, but at the receiving end, it surely feels like all-out war, triggering a justifiable and proportional response.