MASS ATTACK BY DRONES: FACING THE CHALLENGE

ASHEESH SHRIVASTAVA

THE SMALL AND SILENT AERIAL DRONE ATTACK

On January 6, 2018, the world woke up to a new manifestation of a threat from non-state players: the use of home-made drones to attack conventional military targets. On the intervening night of January 5-6, 2018, the Russian military air base at Humaymin (Khmeimim) and its naval base at Tartus in northwest Syria were synchronously attacked by a cluster of 13 Unmanned Aerial Vehicles (UAVs). The scale of the attack was unprecedented. Ten small UAVs with underslung Improvised Explosive Devices (IEDs) targeted the air base while another three flew towards the naval base. Russian reports claim that seven of them were destroyed by the Pantsyr-1S short range air defence system and the remaining six were intercepted by Electronic Warfare (EW)[1] units. However, three of them exploded on impact with the ground and only three UAVs could be recovered for forensics.

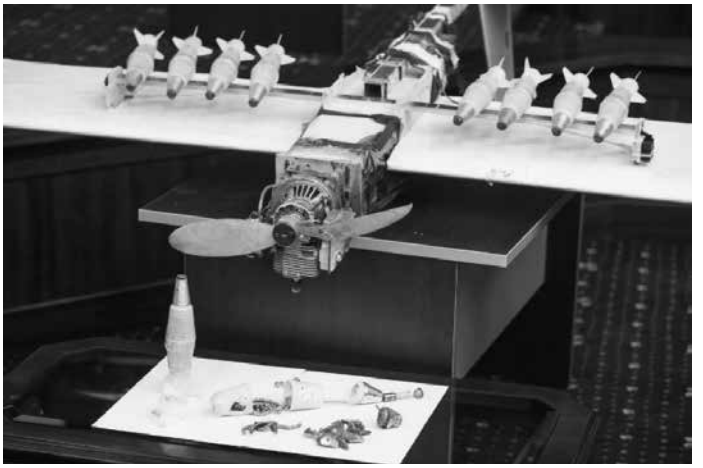
The US Federal Aviation Administration (FAA) defines 'drones' as an Unmanned Aircraft System (UAS), which is an aircraft without a human pilot onboard, and is controlled by an operator on the ground. This article discusses the emerging threat of the use of micro and nano[2] UAS, or small drones, as a potential weapon by militaries as well as by terrorist groups to strike high value targets. This paper also analyses the investments by agencies in developing smart drones as a formidable weapon system, and

Wing Commander **Asheesh Shrivastava** is Research Fellow at the Centre for Air Power Studies, New Delhi.

1. Electronic Warfare (EW) is a generic term that represents the military use of the electromagnetic spectrum – including radio, infrared or radar signals—to sense, protect, and communicate. At the same time, it is also used to deny or disrupt adversaries the ability to use these signals.
2. Nano Drones: MTOW < 250 gm and Micro Drones: MTOW < 2 kg.

also the methods to counter this threat. In this respect, India's preparedness quotient, to counter threats evolving from this new concept of conflict; i.e. drone attack, is analysed in this paper.

Fig 1: Inverted Photo of UAV, with Underslung Bombs, Captured by the Russian Troops



Source: Ministry of Defence of the Russian Federation, Facebook page.

THE SYRIAN CHRONICLE

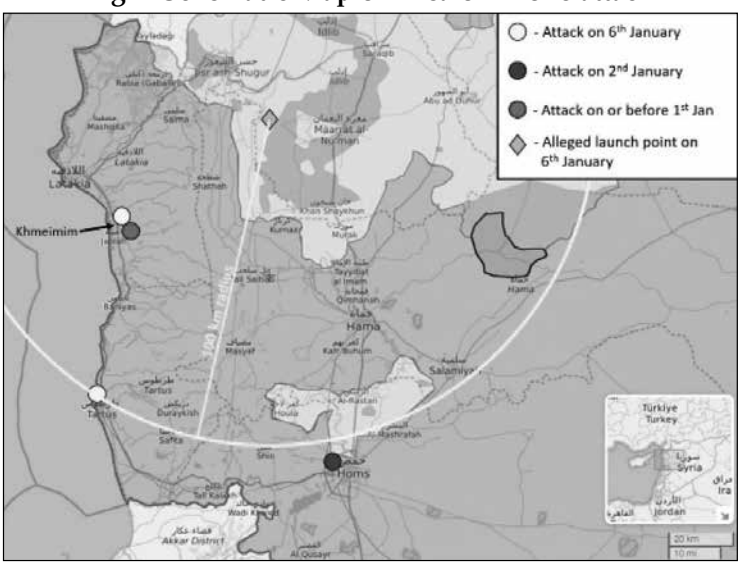
Details made public by the Russian military commanders[3] stated that the aerial vehicles used in the January 5, 2006 attack were guided and controlled by a rudimentary Global Positioning System (GPS) sensor and Global System of Mobile Communication (GSM)[4] enabled remote control module. The drones were powered by small piston engines with sufficient fuel to enable 1-2 hours of flight. Therefore, it was inferred that their launching site and control stations could have been more than 50-100 km away. The UAVs also carried explosive devices fitted with advanced impact fuses. However, the construction of the vehicles (refer Fig 1) did not display any sophistication

3. Jeremy Binnie, "Russians Reveal Details of UAV Swarm Attacks on Syrian Bases", *HIS Jane's Defence Weekly*, January 12, 2018, http://www.janes.com/article/77013/russians-reveal-details-of-uav-swarm-attacks-on-syrian-bases. Accessed on March 2, 2018.
4. GSM or Global System for Mobile communication is a global standard developed for use by cellular mobile devices. The technology also enables extending internet connectivity to mobile devices. Plug-in internet dongles with GSM SIM card can be used to control drones via the internet using a PC or smart phone over a long distance.

in technological acumen, leading investigators to conclude that these may have been assembled in a backyard without any aviation expert support. The small Internal Combustion (IC) engine and the control system used on these platforms are also available 'commercially-off-the-shelf' and, thus, are easily procurable by any aeromodelling enthusiasts. The wings of the aircraft were made from polystyrene and reinforced with balsa wood slats. Each wing had an underslung rack with a releasable mechanism to drop bombs. Four bombs weighing 50 gm each, containing Pentaerythritol Tetranitrate (PETN) explosive with impact fuses were strapped under each wing. Each UAV, carrying 400 gm of explosives was intended to cause noticeable losses to military Vital Areas/ Vital Points (VAs/VPs), with low investments.

There is an emerging threat of the use of micro and nano UAS, or small drones, as a potential weapon by militaries as well as by terrorist groups to strike high value targets.

Fig 2: Schematic Map of Area of Drone attack



Source: Nick Waters and https://syria.liveuamap.com/

The Russian military was luckily able to fend off the attack because the improvised drones were not very sophisticated and reckonable ground

intelligence[5] about a UAV attack was available to them. On two previous occasions i.e. January 2, 2018 and January 3, 2018, similar looking drones were recovered by locals after they crashed near the Military Engineering Academy, Homs and Khmeimim air base. According to reports,[6] the drones were probably assembled and launched from a small hamlet, Muwazarra, located northeast of Humaymin air base. Muwazarra had been designated as a 'deescalation zone' under the existing agreement among Russia, Turkey and Iran (a schematic map[7] of the area showing previous attacks is placed as Fig 2). Reports in the media and events before the D-day suggest that ground intelligence of the potential threat and likely methodology may have been known to the Russians. However, it cannot be ruled out that in another scenario, a better coordinated, intelligent formation of drones with more nimble and networked command and control gadgets could have left the Russian forces much embarrassed.

Fig 3: Pantsir-S1 Anti-Drone System

To fight off the 'mass attack by drones' launched by the *jihadists* against their bases in Syria, the Russians used the Pantsir-S1 (refer Fig 3) mobile surface-to-air missile/ anti-aircraft artillery system. The system, also called

5. Nick Waters, "The Poor Man's Air Force? Rebel Drones Attack Russia's Airbase in Syria", https://www.bellingcat.com/news/mena/2018/01/12/the_poor_mans_airforce/, January 12, 2018. Accessed on January 29, 2018.
6. David Reid, "A Swarm of Armed Drones Attacked a Russian Military Base in Syria", *CNBC News Network*, January 11, 2018, https://www.cnbc.com/2018/01/11/swarm-of-armed-diy-drones-attacks-russian-military-base-in-syria.html. Accessed on January 21, 2018
7. Waters, n.5; and Map of Syria, https://syria.liveuamap.com/

'Gvozd' (Russian for 'nail') is capable of firing 5,000 rounds per minute of 30mm ammunition or concurrently launching anti-aircraft missiles from its 12 launch canisters. The system has an effective standoff range of 10-15 km and has proved very effective against low flying objects or armed UAVs. As stated earlier, seven of the 13 drones were shot down by this weapon system.[8] The remaining six drones were hacked using the Krasukha-4 Electro-Magnetic Pulse (EMP) shield weapon. The EMP weapon made the drones crash or force land outside the target area. Three of these drones were recovered by the military authorities and were exhibited during the press briefing.

THE NEW AERIAL ARSENALS

This mass drone attack on the well-fortified Russian garrison at Syria highlighted the factual danger that small UAVs pose to strategic assets or public facilities/ infrastructures across the globe. Defence experts have long been advocating that use of small armed drones could soon become a common feature in an urban battlefield. These low cost, easily produced, low technology weapon delivery platforms comprise a dangerous manifestation of capabilities by both small anti-establishment groups as well as large nations. These devices/ platforms can be equally employed by sophisticated nations, low-tech rebel groups, or non-state militaries. The January 6, 2018 terrorist attack showed that the threat from synchronously flown UAVs is real and unchecked proliferation of this idea could cause widespread losses at military establishments and civilian infrastructure alike.

The use of unmanned aircraft in military campaigns is not a new concept. The possibility of using remotely controlled weaponised aerial platforms in active combat was first discussed by Lee De Forest and UA Sanabria in 1940[9] in the *Popular Mechanics* magazine. Between the two World Wars, many militaries experimented with different strategies and approaches for

8. Raf Sanchez, "Russia Uses Missiles and Cyber Warfare to Fight Off Swarm of Drones Attacking Military Bases in Syria," *The Telegraph*, January 28, 2018, https://www.telegraph.co.uk/news/2018/01/09/russia-fought-swarm-drones-attacking-military-bases-syria/. Accessed on February 4, 2018.
9. "Robot Television Bomber", *Popular Mechanics*, December, 1940, https://books.google.co.in/books?id=19kDAAAAMBAJ&pg=PA805&redir_esc=y#v=onepage&q&f=false. Accessed on March 12, 2018.

From a tactical approach, the Gulf War of 1991 is called the first war with UAVs. Large fixed-wing aerial platforms with longer endurance than manned aircraft, and armed with appreciable surveillance capabilities continuously dotted the skyline during the entire period of conflict.

drones. The 1973 Yom Kippur War[10] saw Israel use drones effectively for real-time surveillance, reconnaissance, electronic warfare and also as decoys. From a tactical approach, the Gulf War of 1991 is called the first war with UAVs. Large fixed-wing aerial platforms with longer endurance than manned aircraft, and armed with appreciable surveillance capabilities continuously dotted the skyline during the entire period of conflict.

Fig 4: Chinese Swarm Drones

From the earlier days of fixed-wing single-engine UAVs, technology has not only miniaturised the platform but also made it autonomous and optimally packed with sophisticated sensors and armament. The era of nano-drones and micro-drones with 'autonomous' capabilities has begun, with drones ranging from lab-scale prototypes to mass scale production models.

10. The first UAV squadron on the Israeli Air Force was established on August 1, 1971, at Palmahim air base. It was then equipped with the US manufactured Northrop 'Chukar' UAVs. On October 7, 1973, the Chukars flew towards the Golan Heights, making the Syrian AD radars believe that a massive combat air strike had begun. The Syrians activated their anti-aircraft missile systems, thus, exposing them for attack by the Israeli fighter which were following the UAV at a safe distance. http://www.iaf.org.il/4968-33518-en/IAF.aspx. Accessed on March 4, 2018.

These autonomous drones are designed and developed with a certain degree of decision-making capabilities like adaptive formation flying, obstruction avoidance, target acquisition, etc. This new concept of using a flock, usually more than 100 small UAVs, arming them with Artificial Intelligence (AI) and remotely instructing them to carry out a mission is popularly labelled as the "swarm drone". While large UAVs have distinct advantages in the conventional battlefield, nano (and micro) drones have demonstrated a different set of capabilities best suited for urban/ low intensity conflicts. Open-source literature suggests that many countries, across the globe have invested in technologies to develop drones for military as well as civilian purposes. According to media reports, some nations that have demonstrated reckonable capabilities in developing drones include the US, China, Russia, Israel, Iran, India, Pakistan, UK, Turkey, France, North Korea, etc.

Amongst the large military powers, China has invested in technologies to develop low cost drones with AI.[11] The Chinese State National University of Defence Technology (NUDT)[12] has been conducting experiments involving over two dozen small UAVs (refer Fig 4). These fixed-wing small aircraft are capable of flocking together autonomously after launch, carrying out surveillance and reconnaissance of a designated area and even destroying selected targets which match the pre-programmed profile, characteristics or radiation signature. According to Professor Shen Lin Cheng, chairman of NUDT's Institute of Artificial Intelligence Science, "We have precise short, medium and long-term objectives, which are consistent with those set by the government on the modernisation of the Chinese armed forces by 2020, 2035 and 2050". In June 2017, the state-owned China Electronic Technology Group Corporation (CETC) conducted an experiment to demonstrate synchronised flying of 120 unmanned fixed-wing drones.

11. Joseph Trevithick, "China is Hard at Work Developing Swarms of Small Drones with Big Military Application", *The Drive,* January 16, 2018, http://www.thedrive.com/the-war-zone/17698/chinas-is-hard-at-work-developing-swarms-of-small-drones-on-multiple-levels. Accessed on January 29, 2018.
12. National University of Defence Technology or People's Liberation Army National University of Defence Science and Technology is a top military academy with advanced research facilities. It is under the dual supervision of the Ministry of National Defence and the Ministry of Education. It was originally founded in 1953 as the Military Academy of Engineering, and in 1978, changed to NUDT.

What is more worrisome is the fact that these improvised gadgets can be bought "Commercially-Off-The-Shelf (COTS)" from toyshops or ordered online across the globe. A slight modification to these miniature flying platforms can enable them to have additional systems like GPS guidance, digital terrain mapping camera, GSM/RF (Radio Frequency) datalink, explosive bay, bomb release mechanism, etc.

Similar capabilities are being developed by the US. The Defence Advanced Research Projects Agency (DARPA) recently awarded a $7.2 million contract to Raytheon BBN, Northrop Grumman Mission System and Lockheed Martin Corporation to develop challenging capabilities.[13] The project is being financed under the Offensive Swarm Enabled Tactics (OFFSET) project. The proposed swarming systems would be capable of operating in unison with small infantry units and would help them accomplish a diverse range of missions in complex urban environments. Unlike the currently deployed large and expensive drones of the US military, this programme focusses on small dispensable drones, with high end software and AI. The integrated programme would allow them to respond in harmony to the pre-fed mission objective or command. The group of drones would also operate autonomously and, at the same time, avoid crashing into each other while flying in close formation.

Large UAVs have repeatedly demonstrated their capabilities as a challenging variable in warfare tactics in the Bekaa Valley conflict, Gulf War, Afghanistan and, recently, in Pakistan. Advanced technology is demonstrating that small groups of networked and pre-programmed swarm drones could significantly change how military powers operate in the future battlefield. These new low cost, relatively quiet [low Infra-Red/ Radar Cross-Section (IR/ RCS[14])] weapon systems have many advantages as

13. Brandon Knapp, "DARPA Awards First Contract in Drone Swarms Project", www.c4isrnet.com, February 21, 2018, https://www.c4isrnet.com/unmanned/2018/02/21/darpa-awards-first-contracts-in-drone-swarms-project/. Accessed on March 2, 2018.
14. Infrared signature describes the appearance of objects on infrared sensors. RCS is a measure of how detectable an object is on a radar.

compared to conventional aerial artillery like aircraft launched air-to-ground missiles, rockets and bombs. These strategic platforms, when compared with aircraft launched weapons, are not only cost-effective vis-à-vis the scale of disruption but also have measurably higher destructive power, vis-à-vis the degree of effort. These virtues weigh heavily towards the use of drones as ideal weapons for low cost, low intensity war. Further, detection and incapacitating these small/ micro UAVs requires sustained investment in research, training, security and defence mechanism. In a worst-case scenario, one low cost drone, with a very small quantity of ammunition, can disable a fully loaded aircraft if it hits it on the ground or during take-off. Therefore, drones and are now being referred to as the "poor man's air force".

The mass drone attack at Humaymin air base gives us a glimpse of new age battlefield tactics in low intensity conflict. A group of low-cost drones can also inflict appreciable damage to military/ civilian infrastructure. What is more worrisome is the fact that these improvised gadgets can be bought "Commercially-Off-The-Shelf (COTS)" from toyshops or ordered online across the globe. A slight modification to these miniature flying platforms can enable them to have additional systems like GPS guidance, digital terrain mapping camera, GSM/RF (Radio Frequency) datalink, explosive bay, bomb release mechanism, etc. Technology may soon make these platforms a favoured means of executing aerial attacks. Other factors may also include;

- low cost of fabrication;
- stealthy operation; and
- disproportionate gains.

Further, the advantage of 'flexibility of operation' and 'large standoff distance' inherent with the use of any aerial platform is also available with these machines. A cursory scan of the internet will show multiple websites marketing low-cost, high-performance drones with several facilities. The market volume of pre-assembled aero-models including the fixed-wing, rotary-wing and quadcopter has increased manifold in the last few years. According to the Consortium of Unmanned Vehicle Systems India (CUVSI), between the

As per market experts, the Indian drone market is worth over ₹ 100 crore with an estimated Compounded Annual Growth Rate (CAGR) of 18 percent.

years 2015-17, Indians have bought nearly 40,000 drones.[15] These figures include toy drones, hobby UAVs and aerial platforms used by the media and film industry for live shots/ photography. The cost of these drones varies between INR 2,000 to INR 50,000 and they are easily available for sale across the counter without any regulatory control. As per market experts, the Indian drone market is worth over INR 100 crore with an estimated Compounded Annual Growth Rate (CAGR) of 18 percent.[16]

FACING THE THREAT

Discreetly, most military commanders (and security experts) agree with the fact that presently there is no recognised or proven strategy to counter a mass drone attack. Use of conventional kinetic weapons as defence may be successful only if timely intelligence is available. Appreciating this new trend of threat perpetration, the best solution currently is to improve surveillance and the human intelligence gathering mechanism at the local level. Understanding the risk involved, the US Department of Homeland Security issued a countrywide bulletin warning the public regarding the use of drones, by terrorist groups. According to the latest advisory, issued on November 9, 2017, "*Some terrorist groups overseas are using battlefield experiences to pursue new technologies and tactics, such as unmanned aerial systems and chemical agents that could be used outside the conflict zones. Additionally, terrorists continue to target commercial aviation and air cargo, including with concealed explosives*."[17] The circular also had a column on "*How you can help*," which solicited public

15. Saillesh Menon, "Civilian Drones May Account for Bulk of UAVs in Indian Skies", *The Economic Times,* July 6, 2017, https://economictimes.indiatimes.com/industry/transportation/airlines-/-aviation/civilian-drones-may-account-for-bulk-of-40000-uavs-in-indian-skies-despite-ban-by-regulator/articleshow/59464348.cms. Accessed on February 5, 2018.
16. "India UAV Market (2017-2023): Forecast by UAV Types, UAV Range, Application and Competitive Landscape-Research and Markets", *Business Wire*, https://www.businesswire.com/news/home/20170907005704/en/India-UAV-Market-2017-2023-Forecast-UAV-Types. Accessed on March 5, 2018.
17. US Department of Homeland Security, "National Terrorism Advisory System", https://www.dhs.gov/sites/default/files/ntas/alerts/17_1109_NTAS_Bulletin.pdf. Accessed on February 24, 2018.

participation in recognising signs of suspicious terrorist activities and its reporting mechanism. With these actions, the department hopes to receive timely inputs (intelligence) about drones flying in unsolicited areas. Thereafter, conventional artillery can be used to destroy them.

Drones that are designed for mass attack are usually small, lightweight, slow and low flying platforms. They also have a very small IR/ radar signature (RCS).

However, if intelligence fails, preventing a swarm or mass attack by drones, using the current configuration of air defence equipment, is tough and challenging. India is no different. Military strategists and hardware developers across the globe, therefore, are now focussing on developing new technologies to face this unfolding challenge. In recent times, the following three counter-drone techniques have shown encouraging results:

- Hard kill by kinetic weapons, including anti-aircraft guns, missiles, air-burst ammunition, etc. that cause physical damage to the drone's structure, thereby disintegrating it in the air.
- Non-kinetic kill using EMP weapons, electronic jamming and lasers, that incapacitate the onboard electronic systems, causing them to miss the target or force (crash)-land outside danger area.
- Installing physical barriers like nylon mesh, jelly fish traps, etc that entangle the drones and cause them to crash.

While the first option is disproportionally expensive in terms of firepower, the results of option three are encouraging only within a restricted area. One seemingly successful way to approach this threat is the use of non-kinetic weapons or EMP guns like the Russian "Death Ray" and US "Aerial Dragnet" to detect and disable the drones. However, for these EMP weapons to work, an effective radar-based early warning system has to be in place. The radar should be able to correctly identify the target and track its flight path. Thereafter, it should be able to guide the EMP weapon to kill the electrical/ electronic system of the aerial vehicle.

The detecting, identifying and tracking drones from large standoff distances or the non-line-of-sight approach is difficult.

TECHNOLOGY BARRIERS

There are many difficulties in developing cost-effective technologies for monitoring or detecting earth flights of slow moving aerial vehicles. Drones that are designed for mass attack are usually small, lightweight, slow and low flying platforms. They also have a very small IR/ radar signature (RCS). According to Dr Michael Caris[18] of the Fraunhofer Institute for High Frequency Physics and Radar Techniques, Germany, nano UAS have an RCS of less than 0.01m^2 at a reference frequency of 10 GHz.[19] This too is generated only by the onboard batteries, electric motor, servos and engines. Therefore, detecting, identifying and tracking them from large standoff distances or the non-line-of-sight approach is difficult. Radars that have all weather capability to identify drones flying at extremely low level are still at the prototype stage. According to experts at the Institute of Electrical and Electronics Engineers (IEEE), short range surveillance radars for detecting non-metal frame drones with less than 4ft width are technically very difficult to operationalise. The hardware and software to process the radiation feedback and issue credible warning would require very high-end AI and extremely fast processors.

DRONE DEFENCES

To face this menace, the security agencies and defence forces have been demanding a formidable weapon system from the industry. They want that the system should have features like light weight, be easily transportable have omni-directional radar with built-in EW jammers and laser-guided ammunition for short range engagement. For example, on September 13, 2016, DARPA solicited innovative technical research proposals for providing a persistent, wide-area surveillance system for detecting small UAS operating below 1,000 ft in urban terrain[20]. The programme is code named Aerial

18. ˝FHR Security, Detection of Small Drones with Millimetre Wave Radar," https://www.fhr.fraunhofer.de/en/businessunits/security/Detection-of-small-drones-with-millimeter-wave-radar.html. Accessed on March 16, 2018.
19. RCS of other aircraft are B-52 – 100, F-16 – 5, Su-30MKI – 4, MiG-21 – 3, F-35 – 0.005, F-22 – 0.0001, source, Global Security.org, https://www.globalsecurity.org/military/world/stealth-aircraft-rcs.htm. Accessed on March 21, 2018.
20. "Aerial Dragnet-Solicitation Number-DARPA-BAA-16-55", FedBizOpps.gov, September 13, 2016, https://www.fbo.gov/index?s=opportunity&mode=form&id=84ea6bae9dc2a6e6437abeb570c3a77a&tab=core&_cview=0. Accessed on March 15, 2018.

Dragnet. Similar Requests-For-Proposal (RFPs) have been floated by many other militaries, including the Indian defence forces.

Fig 6: Krasukha-4 Weapon System

Source: Sputnik / Pavel Lisitsyn

Concurrently, the defence industries of some countries have demonstrated or published teasers about developing a formidable array of integrated systems to detect and destroy drones. The effective range of these EW weapons is generally 3-5 km only. Most omni-directional jamming radars can disable low-flying, slow moving hostile flying objects. These EMP weapons either blind the seeker or blank the command guidance system of hostile drones. One example of battleworthy hardware is the Russian 'Krasukha-4' (refer Fig 6). It is code-named 'Death Ray' by the North Atlantic Treaty Organisation (NATO). This system was supposedly used by the Russians to bring down the six drones in Syria[21]. Its powerful microwave pulse was able to blind the navigation and guidance system of the drones using powerful directed microwave energy. During 2017, Russia's largest small arms manufacturer, Kalashnikov, displayed its electromagnetic anti-drone rifle, REX-1, at the Army-2017 Expo in Moscow. It is capable of jamming/ suppressing GSM

21. Southfront, "Krasukha-4 in Syria: One Year of Electronic Shield Over Hmeymim Airbase", October 12, 2016, https://southfront.org/krasukha-4-in-syria-one-year-of-electronic-shield-over-hmeymim-airbase/. Accessed on Feburary 24, 2018.

Most omni-directional jamming radars can disable low-flying, slow moving hostile flying objects. These EMP weapons either blind the seeker or blank the command guidance system of hostile drones.

(Communication) and GPS (Navigation) signals of drones.

Similar capabilities to shoot down drones are being developed by other countries. The British Anti-UAV Defence System (AUDS) can spot and identify unauthorised large [over 150kg All-up-Weight (AUW)] aerial vehicles at 10 km[22]. It can also sense micro UAVs (below 2 kg AUW) at about 2 km range. The AUDS uses Ku band electronic scanning radar[23] to identify the target. On recognising a threat, it uses precision infrared guided inhibitor radio signals to disable the controls of the drone. Analogous capabilities have also been developed by the French company CS Communication & Systèmes, which has developed the BOREADES integrated systems for targeting illegal drones. [24] Similarly, Airbus Defence and Space Inc, has developed a counter-UAV system against small drones which uses a combination of radars, infrared cameras and direction finders to identify a potential threat at a range of 5 to 10 km[25]. The system does a real-time analysis of the control signal and then interrupts the link between the drone and its remote pilot using smart responsive jamming technology[26]. Israel, China and Iran have also developed capabilities to counter drone attacks using a mix of kinetic and EMP weapons.

22. Martin Brooke, "British Counter-UAV Technology (AUDS) Selected by FAA for Airport Trials", http://www.blighter.com/news/press-releases/130-british-counter-uav-technology-auds-selected-by-faa-for-us-airport-trials.html. Accessed on February 25, 2018.
23. Radar is the acronym for Radio Detection And Ranging. A Ku band radar uses radio waves between 12-18GHz to determine the range, location, azimuth and speed of an object. The radar system is a radio trans-receiver. It sends a radio wave, which is reflected by the object with a slight change in frequency. The shift is analysed to determine the speed and location of object.
24. BOREADES: an operational French system to detect and neutralise malicious drones flight, https://uk.c-s.fr/BOREADES-an-operational-French-system-to-detect-neutralize-malicious-drones-flights_a584.html. Accessed on March 14, 2018.
25. Airbus, "Counter-UAV System from Airbus Defence and Space, Protects Large Installations and Events from Illicit Intrusion", September 16, 2015, http://www.airbus.com/newsroom/press-releases/en/2015/09/counter-uav-system-from-airbus-defence-and-space-protects-large-installations-and-events-from-illicit-intrusion.html. Accessed on March 4, 2018.
26. Ibid., SRJT, developed by Airbus, blocks relevant frequencies used to operate the drone, without affecting other frequencies in the vicinity

Analogous to developments in Eurasia, the US' Multi-Azimuth Defence Fast Intercept Round Engagement System[27] (MAD-FIRES) is being developed by Raytheon and Lockheed Martin in accordance with specification defined by DARPA in the September 2016 RFP. It will counter the attack from unmanned platforms by shooting a barrage of small calibre smart bullets[28]. It will also serve as a Close-In Weapon System (CIWS) for ships. According to a report prepared by Transparency Market Research[29], the global anti-drone market was valued at about US$214.7 million in 2016 and the figure is expected to climb to US$1.205 billion by 2025. The forecast growth (CAGR) is 19.9 percent which is the highest in the defence sector industry. The demand for anti-drone systems is driven by the security concerns of not only military installations but also private enterprises that want to protect their privacy. As the drones are becoming smarter and stealthier, tracking, detecting and identifying them is becoming more and more difficult. This rapidly maturing anti-drone market is led by highly competitive innovators and start-ups. Technological advances are also likely to make anti-drone systems more effective and affordable to several users. The EMP-based drone neutralisation system is the preferred method for preventing intrusion, rather than the use of kinetic ammunition. The emerging markets for anti-drone equipment are the Central Asian countries, China, India, Israel, Russia, UK, Germany and France, to name a few.

INDIAN READINESS QUOTIENT?

In the wake of all these technological developments, it becomes imperative to deliberate on India's readiness quotient. The race to improvise small aero-models and toy quadcopters as weapons has already begun amongst terrorist groups across the globe. Terrorist groups in India are no exception to this growing trend. It is only a matter of time before these skills are acquired by extremist and terrorist

27. John Keller, "Raytheon and Lockheed Martin Move Forward in Developing Smart Nullets for Surface ship Defence", February 23, 2016, http://www.militaryaerospace.com/articles/2016/02/shipboard-smart-bullets.html. Accessed on March 5, 2018.
28. Patented in the USA in 1998, by R F Barrett, it is an in-flight bullet guidance system capable of directing it along a trajectory so as to impact a laser-identified static or moving target. The bullet contains the laser detection system, guidance-control and steering mechanism. DARPA's Extreme Accuracy Tasked Ordnance (EXACTO) programme demonstrated a .50 calibre bullet hitting a moving target in 2015.
29. Transparency Market Research, Defense, *Anti-Drone Market*, July 2018, https://www.transparencymarketresearch.com/antidrone-market.html. Accessed on March 14, 2018.

groups working against Indian interests. An intelligence failure at the local level or an undetected intrusion could jeopardise India's security situation. In view of these advances, there is an urgent need to secure our military establishments, public utility service centres and critical infrastructure from drone attacks. It is time India invests in improving the defensive mechanism and acquiring capabilities to fend off the threat.

Legally speaking, flying drones is not permitted in India[30]. As per a public notice issued on October 7, 2014, by the Director General of Civil Aviation (DGCA), "Use of Unmanned Aerial Vehicles/ Unmanned Aircraft System for Civil Application", within the Indian civil air space is banned. However, the details of the prohibition were not well articulated or explained in the announcement.

Thereafter, in November 2017, the DGCA circulated a draft of proposed requirements for the operation of civil Remotely Piloted Aircraft System (RPAS) or drones. The regulation would be applicable to civil RPAs which are remotely piloted. It recommends that all RPAs have a Unique Identification Number (UIN) and all operators obtain an Unmanned Aircraft Operator Permit (UAOP). The UIN and UAOP would be issued by DGCA for all UAVs [except nano RPAs flying below 50 ft Above Ground Level (AGL)]. Nevertheless, micro RPAs can fly below 200 ft AGL in uncontrolled, unrestricted and unreserved areas with the permission of the local police administration. The draft policy also recommends a strict ban on the operation of autonomous aircraft (swarm drones).

Although the draft regulation clearly defines the procedure for registration and operation of UAVs in the Indian air space, it does not cover the manufacture or sale of RPAs. No method has been suggested to monitor this process along with any other ministry or department of the Government of India, thus indicating that items and components for fabricating/ manufacturing drones would continue to be available off-the-shelf in the Indian market, including e-commerce platforms. In this scenario, the assembly, fabrication and undetected use of drones as Improvised Explosive Devices (IEDs) for disruptive purposes cannot be been truly ruled out.

30. DGCA, *Public Notice*, October 7, 2014, http://dgca.gov.in/public_notice/PN_UAS.pdf. Accessed on March 18, 2018.

According to the proposed regulation, the permission for operation of RPAs would be issued by DGCA. All RPA flights above 200 ft AGL would be issued with an Air Defence Clearance (ADC) code before commencing flying. The Airport Authority of India (AAI) and Indian Air Force (IAF) shall be responsible to monitor the movement of RPAs within the country's air space. However, in the case of the following categories of operation, written permission from the local police authorities may be required (Table 1):

Table 1

Sl No	Category	Condition
1.	Nano RPA [All Up Weight (AUW) below 250 gm] operating upto 50 ft AGL in uncontrolled air space and indoor operations	UIN/ UAOP/ ADC not required. Local police clearance not required
2.	Aero-models, nano and micro RPAs (AUW upto 2 kg) flying up to 200 ft AGL and within the boundaries of educational institutes including indoor operations	UIN/ UAOP/ ADC not required. Local police to be informed
3.	Micro RPAs, flying upto 200 ft in uncontrolled air space and clear of prohibited, restricted and danger area including Temporary Segregated Areas (TSA) and Temporary Reserved Areas (TRA) as notified by the AAI	UIN required, UAOP/ ADC not required. Local police to be informed
4.	Mini RPA (AUW above 2 kg) and above flying in any area	UIN/ UAOP/ ADC required. ATC and FIC to be informed when flying
5.	RPA owned and operated by government security agencies	UIN/ UAOP not required. ADC required. Local police and Air Traffic Services (ATS) to be informed

The best defence against drones in an emergent scenario is a combination of genuine ground intelligence, low-level 2D/ 3D radars and a powerful EMP/ DEW weapon.

In order to discharge these responsibilities, the AAI, IAF, ATS and local police administration would require additional resources, which may include technical infrastructure, manpower and a dense network of radars and observation posts. Additional financial resources for this also need to be mobilised by the concerned departments, concurrently.

Recently, the Defence Research and Development Organisation (DRDO) has demonstrated the capabilities of its low-level lightweight 2D radar (BHARANI) and 3D radar (ASLESHA). These transportable radars are capable of detecting low flying slow speed aerial vehicles having very small radar signatures. These radars have a certain degree of Electronic Counter Counter-Measure (ECCM) capabilities and can also be integrated into the existing Air Defence (AD) network for swift reaction. Radar systems like these may also be installed at civilian installations, critical infrastructures, VA/ VPs across the country. When integrated with the defence forces and police network, this arrangement may offer the first line of early warning against a mass drone attack. However, to disable or shoot down drones additional capabilities are required.

The best defence against drones in an emergent scenario is a combination of genuine ground intelligence, low-level 2D/ 3D radars and a powerful EMP/ DEW (Directed Energy Weapon) weapon. On one end, ground intelligence in the form of trained foot soldiers/ police personnel, networked mobile observation posts, IR surveillance cameras, etc would be capable of detecting unsolicited intrusions, through day and night. On the other end, post detection quick response kinetic and non-kinetic (DEWs) weapons would be required to neutralise the threat by shooting down drones.

THE WAY FORWARD

Presently, our security forces, like many others, rely profoundly on human intelligence and kinetic weapons as the primary defence against a mass drone attack. This arrangement is likely to be marred with surveillance gaps.

Appreciating this, the Technology Perspective and Capability Roadmap (TPCR)-2018 prepared by the Ministry of Defence, lists out certain technologies and equipment that the Indian defence forces would need to develop and acquire by 2020. Some of the proposed technologies/ projects are listed below[31] (Table 2):

Table 2

Sl No	Project	Description	Services
1.	Anti-UAV/ RPA Defence System	The system should be capable of disrupting and neutralising RPAs engaged in hostile airborne surveillance or any other activities. It should have combination of electronic-scanning radar target detection, Electro-Optical (EO) tracking/ classification and directional Radio Frequency (RF) inhibition capability. The system should also be able to remotely detect all RPAs from micro to Medium Altitude Long Endurance (MALE) UAVs. It can be operated in restricted/ open RF bands. Detection range > 40 km, EOTS range > 12 km and RF inhibition range > 7 km	Army and Air Force
2.	Tactical High Energy Laser System	The HMV-based laser weapon system should be able to cause physical damage/ destruction to communication/Electronic Warfare (EW) systems, including ground-based and aerial targets.	Army and Air Force
3.	High Power Electromagnetic Weapon System	The HMV-based high energy EMP weapon system should be capable to neutralise the enemy's electronic and electrical system (including RPAs) in the tactical battle area at a range of 6-8 km or more.	Army and Air Force

31. Ministry of Defence, "News-What's New", February 23, 2018, https://mod.gov.in/sites/default/files/tpcr_0.pdf. Accessed on March 12, 2018.

Technology has a way of fundamentally altering both the rules and philosophies of conflict. Recently, there has been a paradigm shift in the strategies of conflict which is centred around technology of weapons, swarms of drones, space, cyber interference, etc to name a few. Put together, these developments have made the concept of war in this century as new as the use of gunpowder in the 13th century. Drones or UAVs pose a clear and present danger to the security of our VA/VPs. It is, therefore, imperative that India take note of the changing nature of conflict. The approach adopted by various ministries to the problem are steps in the right direction, but a sense of urgency is required to tighten the noose on mass drone attacks.

While the Indian Micro Small and Medium Enterprises (MSMEs) and international aerospace giants are seriously competing for developing and producing[32] micro and mini UAVs for various applications, the anti-drone industry is yet to take off. There is a need to concurrently push for induction of anti-drone equipment and system by security agencies. Apart from working on the indigenous development of technologies for drones, the security establishment needs to understand the impact of weaponised drones on India's internal defensive capabilities. Unless this happens at a faster pace, India risks preparing for a war against 21st century militaries (and militia) with a 20th century arsenal. Consolidated efforts across the board are required to fight this challenge.

32. The Qualitative Requirements (QRs) and Trial Directives for Micro UAVs were approved by the Police Modernisation Division of Ministry of Home Affairs, GoI, on August 12, 2014. This enabled the police forces including Central Armed Police Forces (CAPFs) across the nation to procure UAVs under the Police Modernisation Programme. The action also revitalised the MSME sector to innovate and manufacture drones as per the set QRs. According to the market research portal 'Research & Market' the Indian drone market is expected to reach $421 million by 2021, primarily driven by security concerns.