4

Armed sUAS Swarm: Big Threat of Small UAS–C-sUAS Development and Threat Mitigation by India

RK Narang

Introduction

In the past, manned aircraft came into being by imitating birds and now, the swarming behaviour of bees, animals and birds has inspired the development of Unmanned Aircraft System (UAS) swarms.[1] The recent progress in Artificial Intelligence (AI) facilitated the collaborative operation of multiple UAS as swarms by utilising the inbuilt intelligence of each UAS.[2] The weaponisation of the UAS swarm and its ability to carry out simultaneous attacks from multiple directions in a coordinated manner makes it a serious threat for air defence planners.[3] The miniaturisation of systems, sensors, weapons and their increasing lethality led to the development of armed swarms comprising small UAS (sUAS). The sUAS swarms, being small in size, flying at low speeds and low altitudes, and having the ability to identify targets by using onboard sensors and carry out collaborative attacks on multiple targets, pose the biggest challenge for air defence planners. They are ideally suited for striking high-value military assets, strategic installations, large gatherings and even targetted killing. The unsuitability of existing air defence systems to detect, identify, track, neutralise and destroy slow moving and low flying sUAS makes matter even more challenging for air defence planners. The potential for employment of civil sUAS for armed attacks by terrorists and insurgents further increases the challenges for air defence commanders. Therefore, a need was felt for developing Counter-small Unmanned Aerial Systems (C-sUAS) technologies to address this challenge. As a result, several countries and leading aviation companies started developing C-sUAS technologies. The rapid progress in UAV swarm technology and gaps in C-sUAS technology necessitated that an interim strategy be formulated to mitigate the threat posed by sUAS swarms till reliable and effective C-UAS systems are developed.

The development of armed sUAS swarms and their ability to strike aerial, ground and surface targets has special significance for India. Its northern neighbour, China, demonstrated the armed sUAS swarm concept, which is in the advanced stage of development, at the Zhuhai Air Show in 2018.[4] The possibility of passing it on to Pakistan, its closest ally, cannot be ruled out. Though Pakistan does not have the sUAS swarm capability, it has reasonable experience of producing small and tactical UAS on its own. It is also known for utilising terrorism as a tool for achieving its political and strategic objectives and it could overtly or covertly employ multiple sUAS (in swarms) for carrying out armed strikes on India's civil-military installations. The Indian defence forces are aware of this emerging threat as they had projected the requirements of C-sUAS systems in their Technology Perspective Capability Roadmap (TPCR) issued in 2018.[5] Indian Research and Development (R&D) agencies have been pursuing projects to develop C-sUAS technologies, which are in the development phase. This paper, therefore, deliberates on the following aspects:

- To examine the emergence of armed sUAS swarms.
- To examine the C-sUAS systems being developed globally.
- To examine the sUAS swarm threat to India, its strategy for countering the threat and developing C-sUAS capability.

Emergence of Armed sUAS Swarm: An Intelligent Surveillance and Strike Package

Collaborative Attacks

An sUAS, having a relatively smaller radar cross-section than a fighter aircraft, tactical or Medium Altitude Long Endurance (MALE) Unmanned Aerial Vehicle (UAV) and cruise missile, is difficult to detect and neutralise. It does not have the pronounced aural signature and long approach followed by fighter aircraft and missiles; its electric motors do not have a significant thermal signature; all this reduces the chances and range of detection. The size and payload carried by each sUAS may not be much, but as a group of tens, hundreds and thousands, sUAS can cause considerable damage. The employment of multiple intelligent, armed sUAS, carrying different sensors, and weapons, attacking civil-military installations, poses new challenges for air defence personnel. Even if the defender detects the sUAS, it will find it difficult to identify the type of sUAS, ascertain its size, numbers and payloads.[6]

The employment of sUAS for collaborative attacks by terrorists in the recent past validated the enormous potential of employing armed sUAS for military applications

as well as brought to the fore the limitations of the existing C-sUAS systems. In one such attack, a Russian air base in Hmeimim and a naval base near Tartus, located in western Syria were subjected to simultaneous armed sUAS attacks in January 2018. The strikes were carried out by 13 fixed wing low-cost plywood sUAS having strap-on munitions.[7] Out of these, seven armed sUAS were shot down by the Russian air defence systems comprising air defence guns and Pantsyr Surface-to-Air Missiles (SAMs) while the remaining six were neutralised by cyber air defence systems, which disrupted their command and control and Global Positioning System (GPS) navigation systems.[8] However, composite counter-sUAS systems comprising SAMs, anti-aircraft guns and cyber defence systems costing millions of dollars against cheap sUAS (costing less than a thousand dollars) was an uneconomical way to counter armed sUAS.[9] Another incident involved an assassination attempt on Venezuelan President Nicolas Maduro by two armed quadcopter sUAS that were launched by militant groups. The sUAS, armed with C4 explosives had injured seven soldiers during the military parade in the capital Caracas on August 4, 2018.[10] In another incident, an sUAS equipped with a thermite grenade caused extensive damage to a Ukranian ammunition facility.[11] Similarly, the Islamic State in Iraq and Syria (ISIS) employed sUAS to carry out 200 such attacks in 2017.[12] The above attacks cannot be termed as swarm attacks as these sUAS did not possess the required level of Artificial Intelligence (AI) and automation to communicate with each other and respond autonomously to unforeseen contingencies during the flight. But they provided a glimpse of the enormity of the threat and the complexity of defending against such attacks.[13] They also highlighted that militaries unprepared for sUAS attacks could face serious consequences in the future.

Armed sUAS Swarms

Armed sUAS swarms have generated enormous interest globally. The UK's Defence Secretary, Gavin Williamson, called for the formation of "swarm squadrons of armed drones that could confuse the enemy and overwhelm their air defences to exploit the military potential of the UAS swarm technology".[14] The USA and China have led the development of sUAS swarms. China's North Industries Corporation caps demonstrated the concept of armed UAS swarm employment for combat roles during the Zhuhai Air Show in China in November 2018. It envisaged employment of a swarm comprising multiple MR-40 series (four rotors) and MR-150 series (six rotors) sUAS equipped with a variety of sensors for surveillance, detection and targeting. The MR-40 and MR-150 are small UAVs, which can carry different types of lightweight weapon payloads, which include air-to-air missiles, air-to-ground Blue Arrow-5 and Blue Arrow-7 (semi-active

laser homing) guided missiles with high explosive or fragmented warheads, 40 mm LG25A automatic grenade launchers, parachute retarded[15], rocket-propelled munitions and machine guns to strike targets on the ground. This armed sUAS swarm, having a range of 30 km and endurance of one hour, could become a complete tactical surveillance and strike package for the military. Also, the same sUAS swarm, equipped with suitable sensors and weapons could be employed in the anti-sUAS swarm role.[16]

The United States Navy (USN) had demonstrated a ship launched sUAS swarm consisting of 30 Coyote sUAS in 2015[17]. The United States Air Force (USAF) simultaneously initiated the "Gremlins Project" in 2015 with an aim to launch 20 large UAVs from C-130 transport aircraft, which would fly a distance of 300 nautical miles (nm), return after loitering over the target area for one hour and be retrieved by a C-130 in the air.[18] In the meantime, the USAF also demonstrated a launch of an unarmed swarm consisting of 103 Perdix fixed wing sUAS from three F/A-18 fighter aircraft in 2016.[19] However, the US, in the process of developing cutting edge sUAS swarms technology for its air force and navy, overlooked the sUAS swarm segment for the land forces, which China had been eyeing since the beginning. The focus of China on sUAS swarm can be gauged from the fact that it miniaturised a number of sensors and weapons, including lightweight bombs, missiles, Precision Guided Munitions (PGMs), etc.,[20] which is likely to facilitate early operationalisation of its armed sUAS swarm. However, the effectiveness and ranges of miniaturised sensors and weapons would be less, which would limit their employability. Also, China lags behind the US in developing air-launched sUAS swarms but continues to make progress in developing sUAS swarms for the land forces, which could become its niche arms export segment.

Countering the Armed sUAS Swarm Threat

Detection and Tracking

The threat posed by armed sUAS swarms to civil-military targets in the last few years created urgency to develop Counter-sUAS (C-sUAS) systems. The C-sUAS mechanism comprises five activities, i.e. detection, identification, tracking, neutralisation and destruction by kinetic or non-kinetic means. The challenge for designers was to develop a system that could detect multiple rogue slow moving sUAS operating at very low levels (including between obstacles and buildings in urban areas), track their movements, and neutralise and destroy them. However, the existing radars were optimised for detection, identification and tracking of fast and large manned or unmanned aircraft. And some of the radars that could pick up slow-moving objects were not able to differentiate between

slow-moving sUAS and birds. Also, these sUAS, while operating in the autonomous mode and having the onboard anti-collision system, could fly at very low levels, which further added to the challenges for air defence personnel. Therefore, designers experimented with the detection of sUAS by developing new radars, Radio Frequency (RF) Electro-Optic (EO), and Infra-Red (IR), and acoustic sensors, individually as well as through a combination of sensors. A radar could detect large manned and unmanned aircraft due to their radar signature; however, it needed algorithms for detecting and tracking multiple sUAS. Also, its range had to be reduced to optimise it for detecting slow-moving sUAS. The radar system, despite design modifications, could not provide a foolproof solution against small and slow-moving sUAS. Therefore, an RF system that could scan the frequencies of drone operations and employs algorithms to detect sUAS and pinpoint their geographical location through their RF emitter was also tested. The third system to detect sUAS was the EO/IR system in which EO detects the visual signature while the IR system detects the location of the UAS through its heat signature.[21] The fourth system employed by some countries involved electronic monitoring of sUAS by installing the Global System for Communication (GSM) Subscriber Identification Module (GSM SIM) and Radio Frequency Identification (RFIDs) on UAS and tracking their movements through mobile towers. Such a system is ideally suited to identify known UAS operating in the urban environment that had the network and adequate coverage of mobile towers. It allows ground-based sensors to differentiate friendly sUAS from those (rogue sUAS) that are not equipped with these sensors. The fifth system was by installing an Automatic Dependent Surveillance-Broadcast (ADS-B) system on it. The ADS-B is a system that identifies the sUAS' position from satellite receivers and broadcasts it for the benefit of the other aircraft in the air as well as the ground stations. However, all these systems, except the ADS-B, have certain limitations and do not provide assured detection, e.g. an EO system can be employed during day-time but its effectiveness reduces during the low visibility period. As a result, designers started employing more than one detection sensor to overcome the limitations of individual systems and improve the effectiveness and reliability of the detection system, e.g. Israel Aircraft Industry's "Drone Guard" system employed a combination of three dimensional (3D) radars and EO systems for detection. The system has an option of using different radars, with each radar being optimised for detecting at different ranges, i.e. ELM-2036D for 10 km (short), ELM-2026B for15 km (medium) and ELM-2026BF for 20 km (large) detection distances. The aim of developing three different radars for slight variations in detection ranges appears to be for optimising radars for different sizes of drones and different speeds. Also, difficulty in tracking multiple sUAS by the EO system necessitated the development of algorithms for tracking

multiple sUAS.[22] However, these detection systems continued to have certain limitations, which forced designers to look for innovative and technological solutions. The recent technological developments facilitated the employment of Active Electronically Scanned Array (AESA) radars to autonomously detect, identify and track targets in the advanced C-sUAS systems. AESA radars are more effective compared to IR systems, which may not be able to pick up micro and mini UAS having a very low heat signature.[23] Some designers started using the modular Passive Electronically Scanned Array (PESA) and Frequency Modulated Continuous Wave (FMCW) technologies to detect micro UAS and larger unmanned aircraft systems from zero (hover) to inflight speeds in their C-sUAS systems. The Digital Drone Detection (D3) technology facilitated extraction of tiny reflections from plastic bodied UAS even when flying close to the ground or near buildings, which enabled them to detect, track and identify a drone up to a range of 3.5 km within 10 seconds.[24] As a whole, the technological developments in detection technologies helped designers in overcoming the limitations of the earlier detection systems; however, the ranges of these systems that were optimised for detecting small and slow UAS are much lower than the sensors meant for picking up larger and faster manned and unmanned aircraft.

C-sUAS Systems: Neutralisation and Destruction

The rogue sUAS posed a serious threat to civil-military targets and, thus, needed to be neutralised and, if possible, destroyed. The existing air defence systems namely, anti-aircraft-artillery guns, anti-aircraft surface-to-air missile systems, etc. were optimised for destroying hostile fast and larger combat aircraft but not suited for detecting and neutralising a swarm of slow-moving sUAS in a cost-effective manner. Therefore, new systems were needed to neutralise or destroy the sUAS. The first method for neutralisation of rogue sUAS was by jamming or spoofing of the RF link between the rogue sUAS and its operator, and the satellite links of its GPS or Glonass or BeiDou navigation systems to make the hostile sUAS land on the ground or initiate its 'return to home' mode or take over its control. The second method would be to use Directed Energy Weapons (DEWs) like lasers, which can be employed for dazzling of EO/IR sensors (neutralisation) or for the destruction of critical airframe components of the sUAS (destruction). The high power microwave systems provide another option for neutralising sUAS as microwaves damage the electrical circuits of the sUAS' motherboards and cripple their command and control systems. The last and time-tested system is by employing guns, missiles and other hard kill systems for shooting down the sUAS. In addition to the above, innovative solutions like drone net guns were developed for disabling the rogue sUAS. However, the

inability of any single C-sUAS systems to provide assured protection against armed sUAS swarm attacks convinced sUAS designers to explore the option of employing multiple neutralisation and destruction systems to enhance their effectiveness and reliability. After having discussed some of the emerging C-sUAS systems, it would be prudent to deliberate on their functioning, strengths and limitations in detail to understand their employability for the C-sUAS role.[25]

Lasers: A laser is a line of sight system that can physically damage an sUAS provided its beam is kept focussed on the target for the required duration to burn it. The time required may vary depending on the type of target and the power being radiated by the laser. However, the effectiveness of lasers degrades in bad weather and dusty conditions, which limits their employability. On the other hand, the power required by laser cannons is very high, which requires a large power source. As a result, the complete equipment becomes heavy and, thus, has to be mounted on a truck or a ship. Also, their ranges are limited, e.g. China's laser cannon has a maximum range of 4 km.[26] Intensive research is being undertaken worldwide to miniaturise lasers to make them lighter; however, they still comprise a work in progress and would take some time to mature as a C-sUAS system.

Anti-Laser Weapons: On the one hand, the laser weapon is being developed to destroy aircraft and UAS while, on the other, researchers are looking for its antidote, i.e. the anti-laser system. China's research and academic institutions, including the Naval Aeronautical Engineering Institute of the People's Liberation Army (PLA), has developed an anti-laser capability comprising anti-laser reflectors and paints for protecting airborne and ground-based sensors against laser attacks. They are meant to deflect or absorb laser beams to reduce the effectiveness of laser weapons. However, such coatings have certain limitations as they would be effective only against certain types of lasers.[27] The development of anti-laser paints and reflectors could enhance the resilience of rogue sUAS to laser attacks, which will add to the challenges for the air defence personnel in countering the drone threat.

High Power Microwave: The High Power Microwave (HPM) system works at atomic levels as the HPM beam passes through the airframe and other structures and directly impacts the semi-conductors of the sUAS. As a result, the circuits of the semi-conductors get heated up and are distorted, thereby making their command and control systems inoperative. The HPM transmission, unlike lasers, can be emitted in a cone-shaped beam, which can disable multiple UAS simultaneously since the energy required for neutralising semi-conductors is small. Therefore, HPM systems, being reusable, have the potential to develop as C-sUAS and provide protection against the sUAS swarm

threat. However, the literature on HPM systems suggests that they have a low effective range (below 1 km), are heavy, and ,thus, suited for terminal defence.[28] The United States Air Force Research Laboratory had spent $15 million by 2019 to develop a High Power Microwave Operational Responder (THOR) C-sUAS system. It would need another $10 million to manufacture these and their induction into the armed forces could take three to four years.[29]

Surface-to-Air Missiles (SAMs): SAMs have remained one of the viable means for destroying rogue sUAS despite their high cost. The threat posed by sUAS forced designers to develop Synthetic Aperture Radars (SARs) and missile seekers that can pick up targets with low Radar Cross-Section (RCS) and at low altitude as well as destroy them at close ranges. This ability of the SAMs was demonstrated when Russia employed a combination of RF and Pantsir SAMs to neutralise the attack by multiple sUAS on its bases in Syria in January 2018.[30] The SAM system might have done its job of destroying the rogue sUAS during the attack; but such systems may prove to be extremely expensive if employed against low-cost commercial sUAS swarm.

Armed UAS: Low-cost sUAS are also being developed as potential C-sUAS systems. The armed sUAS detects rogue sUAS with its detection sensors, closes in and explodes itself to destroy the rogue sUAS. The success of the armed sUAS depends upon its speed, and onboard sensors to identify and track rogue sUAS and close into the target before carrying out a suicide attack.[31] The US Army has inducted the Block 1B, an armed variant of the Coyote drone, which is equipped with a seeker and warhead for the C-sUAS role.[32]

Hybrid C-UAS Systems

UAS Jammer Guns: The ability of terrorists to launch armed sUAS from close ranges and the lack of warning time created a need for an easy to deploy short-range quick response terminal defence system. As a result, a short-range hand-held detect and neutralise rifle was developed. It had interchangeable jamming modules that were capable of suppressing GPS, Glonass, BeiDou, and Galileo satellite navigation systems up to 2 km and Global System of Mobile Communication (GSM), 3G, LTE signals, 900 MHz, 2.4, 5.4 and 5.8 G Hz frequencies at a range of 500 metres (m). As a result, the rifle can neutralise the bomb activation mechanism via mobiles, navigational signals of the GPS and command and control mechanism of the rogue sUAS. It also has a laser and a stroboscope model for blinding the EO/IR systems of the rogue sUAS.[33] However, an operator might delay its operation till the sUAS are physically identified, which could reduce its effectiveness. Therefore, incorporating an autonomous activation mechanism could have enhanced its effectiveness.

Detect and Neutralise: The lack of reaction time necessitated the development of composite drone detection, identification, tracking and neutralisation systems. Therefore, a composite C-sUAS system comprising radars and electro-optical systems for detection and radio frequency jamming system was developed to neutralise the hostile sUAS with the least delay.[34] Its portable lightweight radio frequency jammers can jam 433 MHz, 915 MHz, 2.4 GHz, 5.8 GHz and satellite navigation signals, including the GPS, Glonass, BeiDou up to a range varying between 500 m to one km.[35] The jamming of GPS and command and control data links blinds the sUAS and does not allow the continuation of the flight in the pre-planned as well as remote control modes, thereby forcing the drone to return home or shut down or crashland.[36] The threat posed by armed sUAS to dense civil traffic even prompted the Federal Aviation Authority (FAA) of the USA to acquire a C-sUAS system. This system utilises the Ku band radar, daylight and IR cameras, target tracking software and radio frequency inhibitor to detect, track, classify, disrupt UAS up to a distance of six miles.[37] In a similar endeavour, Russia tested the "Repellent" system, which can jam miniature UAS less than a foot long upto a distance of 35 km.[38]

Detect, Neutralise and Destroy: The uncertainty about the effectiveness of detection, neutralisation and destruction system necessitated the development of composite counter-sUAS systems to destroy hostile sUAS. The composite systems not only had detection and neutralisation systems but also had lasers for the physical destruction of targets if neutralisation were to fail, however, their ranges are limited. In one such endeavour, the composite system sensors could detect a drone at 3 km, radio frequency at 2 km, acquire a drone at 2.5 km, neutralise its data links and GPS at 2.5 km and if the hostile sUAS survived, it would be destroyed physically at 800 m by using a laser burner.[39]

Innovative Technologies

Hacking sUAS: Hacking of the data links of the sUAS was undertaken by experts sitting on the ground; however, it could become an airborne activity as the sUAS that are being developed would be able to hack and track the rogue UAS. To test the viability of the concept, a drone fitted with a Pi computer hacked a wireless mouse from outside a building in 2017. The capability of the UAS to operate out of sight of the victim sUAS and hack its command and control system makes it a potent C-sUAS system.[40]

Swarm Versus Swarm: Air defence commanders would find it difficult to defend their bases against a collaborative attack by tens and hundreds of armed sUAS. Therefore, the feasibility of employing armed sUAS swarm in the C-sUAS role is being explored. The armed sUAS swarm, equipped with a detection, tracking and destruction mechanism, could provide an effective C-sUAS swarm capability.[41] However, members of the air

defence sUAS swarm should not pose a collision hazard to each other while attacking the hostile sUAS swarm.[42] Also, tactics and algorithms are needed for employing swarms to neutralise rogue swarms. Towards this goal, the US Naval Post Graduate School conducted a "Swarm versus Swarm" grand challenge to develop concepts of operations and tactics for the air defence sUAS swarms against rogue sUAS swarms. The ultimate aim of the organisers was to test aerial combat between 50 attacker versus 50 defender UAS. [43] The live fly competition scenario envisaged simulating a large scale battle between swarms of sUAS to achieve aerial superiority, simultaneously defending high-value targets on the ground.[44] The US military academies also participated in the swarm vs swarm competition.[45] A study on "Threats of UAS Swarms and the Counter-Measure Needs" in 2015 has observed that employing UAS swarms for countering a UAS swarm is very expensive; however, this may change with the progress in counter-swarm technology.[46]

Escort Swarm: There may be a situation in which hostile sUAS pose a threat to a sensitive and vital area, and aggressor sUAS may need to be escorted away to protect the site. To do that, researchers at the University of Luxembourg developed algorithms which will enable an air defence sUAS swarm to form a self-organising network to capture a rogue UAS and escort it out of the danger zone. These researchers adopted a localised instead of a central approach, which made the swarm robust and less vulnerable to interference.[47] The development of such a system consisted of five phases comprising deployment, clustering, formation, chase and escort. The results of algorithm development and validation through the simulation of a UAS swarm acting as a counter UAS system were positive. The system was in the process of deployment for field testing in late 2018.[48]

Swarm Disruption: Another way to neutralise a hostile sUAS swarm is by disrupting the coordination among individual UAS so that they disintegrate into many desperate, uncoordinated elements. Though jamming may not destroy individual elements, it would prevent them from fighting cooperatively, which would make it easier for the air defence personnel to target them.[49] The endeavour of C-sUAS designers should be to identify means for jamming or interfering in the intra-group communication between various members of the hostile sUAS swarm or to jam the emitters, facilitating the position maintenance within the group.

Net Guns: One of the methods to prevent hostile sUAS from reaching their targets is by making them dysfunctional. To do that, designers modified existing shotgun cartridges to carry thin mesh and metal weights inside to capture the rogue sUAS. When the cartridge is fired, the mesh opens up close to the target and wraps around the rotors

while the metal weights cause physical damage to the rotors and other parts of the sUAS. This may result in disbalancing or disabling or causing damage to the hostile sUAS. However, a small cartridge of the shotgun allows only a small net to be carried up to very short ranges. Also, the low range of the modified shotgun and the high skill requirements limit its effectiveness in the C-sUAS role. To overcome the limitations of low range of the modified shotgun, a special net gun with a larger cartridge that housed a bigger net was developed. However, the range of this gun is about 40-50 ft and it can immobilise only the small sUAS.[50] The US military researchers have developed a grenade that carried a larger net and had greater range.[51] However, its performance could degrade with low slant visibility and lack of expertise of the operator.

UAS Net Capturing System: In addition to ground-based capturing systems, the endeavour has been made to equip air defence sUAS with synthetic ropes or the Kevlar nets to capture hostile sUAS in the air. The first UAS capturing system has an sUAS that carries a net in its underbelly and flies over the hostile sUAS in such a way that the net wraps around, and, immobilises it.[52] In the second UAS capturing system, the air defence sUAS flies above the hostile sUAS and releases the net. The net wraps around the rogue drone and immobilises it. During the same time, a parachute is deployed so that the captured UAS does not fall onto the ground and cause injury to people or get damaged. However, this system requires air defence sUAS to close in and fly over the rogue drone, which would require detection, acquisition, tracking, closing in, and then flying over the hostile sUAS, which will have its own challenges.

Munitions: The shotgun needs special munition in which shrapnel spreads out close to the target for the C-sUAS role. Similarly, special counter-drone munition with a Kevlar net and a parachute is being developed. There is a need for improving the quality and enhancing the range of the shotgun munition. The munition of anti-aircraft guns and other C-sUAS weapons would need to be modified for enhancing its effectiveness for the C-sUAS role.

Challenge in Developing C-sUAS Systems

The US Centre for the Study of the Drone, in its report on counter-drone systems in February 2018 observed that 235 counter-drone products were either available in the market or were being developed by 155 manufacturers in 33 countries. Radar, RF, EO and IR were found to be popular systems for drone detection. However, C-UAS technology has raised practical, legal and policy challenges, and the lack of common standards in the C-UAS industry is resulting in variations in the effectiveness and reliability of the systems.[53] The report highlighted the difficulties experienced by radars in picking up

sUAS flying at slow speed and low altitude while the employment of EO systems for detection was constrained since they could be used only during daylight hours. The possibility of an EO system operator confusing birds for sUAS added to the detection challenges. Also, detection by EO, IR and RF systems remains limited to the line of sight. Similarly, acoustic and RF detection systems could only pick up UAS which were stored in their library and it may become extremely difficult to update their libraries since every day new UAS are being produced. Also, the acoustic signature of the sUAS manufactured by the adversary may not be available for updating the acoustic library of the air defence sUAS. The challenge for designers also lies in optimising the sensitivity of a detection system, as higher sensitivity would lead to a large number of false pick-ups while low sensitivity may result in the system not picking up the sUAS.[54] To address these challenges, certain C-sUAS competitions and technology challenges have been launched to fill the technology gaps and some such competitions are discussed in the following section.

MITRE Counter-UAS (C-UAS) Challenge

The MITRE[55] Corporation, a non-profit organisation of the US, launched a C-UAS challenge in 2016 to invite the academia, industry, government organisations and innovators from other countries to provide technological solutions to counter the threat from rogue UAS and improve aviation safety and security. The envisaged C-UAS was expected to be deployable in populated areas and be compliant with the safety regulations and relevant laws of the US The C-UAS system was expected to detect small UAS weighing less than five pounds during flight, determine the threat based on their geographic location and flight trajectory, interdict small UAS that are perceived as a threat and recover them in safe areas while keeping the payload intact.[56]

A total of 42 applicants from eight countries participated in the challenge and evaluation of their systems was carried out at the Marine Corps Base Quantico, Virginia, from August 10-18, 2016. The Alexandria-Virginia-based Van Cleve and Associates won an award for developing an end-to-end system having a 360-degree scanning radar, an EO/IR system and an RF jammer. The OpenWorks Engineering of Riding Milli and SkyWall 100 system (both from the UK) won the interdiction system and intelligent projectile categories respectively.[57]

DARPA's Dragnet Challenge

The Defence Advanced Research Projects Agency (DARPA) of the US launched the "Dragnet Project" in 2016 to develop a mobile system capable of detecting and tracking

hostile sUAS that are operating independently without the GPS or radio control in the non-line of sight trajectory in a congested urban area below 1,000 ft. The second objective of the project was to neutralise or destroy sUAS at a distance of 1 km or higher while keeping the cost of engagement and collateral damage to the minimum. The project was initially aimed at meeting the requirement of the military, which would be later tailored for detecting and neutralising rogue sUAS operating in the civil air space. As part of this challenge, a combination of tethered UAS was to be deployed in urban areas to detect and track sUAS operating at low levels or in between the obstacles that did not fall in the line of sight.[58] Earlier, DARPA had launched a project named "Collaborative Operation in Denied Environment (CODE), in which it had envisaged the development of algorithms and software which would facilitate the operation of UAS swarms while operating in areas where no GPS or data link is available. The Dragnet project is aimed at developing counter-measures against UAS swarms operating in the CODE environment. The US has demonstrated a parallel policy for developing cutting edge technologies (CODE project) as well as their counter-technologies (Dragnet project).

Legal Challenges

The security agencies may be required to neutralise, capture or shoot down hostile or rogue sUAS if they venture into prohibited air space without authorisation. This is essential to protect Vital Areas (VAs) and Vital Points (VPs). However, the absence of legal provisions could make the security agencies vulnerable to legal battles. To overcome this hurdle, the US enacted a law on October 5, 2018, to allow the US authorities to use reasonable force to disable, damage or shoot down private UAS without warrants if they appear to be posing a threat to VAs or VPs.[59] India would need to analyse its regulatory and legal provisions and their applicability for its security agencies undertaking C-sUAS missions.

Risk Assessment

The hostile armed sUAS swarm, when detected, provided little time for air defence planners to identify the type of sUAS, the payload carried, the feasibility of striking the base and predicting the direction and time of the attack. As a result, a need was felt for developing tools that would enable air defence commanders to assess the risk posed by sUAS. To address this challenge, a team from the US Naval Post Graduate School carried out a study titled "UAS Swarm Operational Risk Assessment System" in September 2015. The study deliberated on the development of the assessment tools to assess the risk of potential UAS swarm attacks by using simulation tools like ExtendSim9, MINITAB17

and Graphical User Interface (GUI). Since it was a naval study, the risk assessment tools were also required to calculate the absolute as well as relative position of the ship and the UAS swarm in a moving ship.[60] The choice between kinetic and non-kinetic weapons, and their kill radius was taken into consideration for selecting the appropriate anti-UAS swarm attack response solution. With these tools, an operational commander could feed in the type of UAS, the location of the UAS, own position and own defence capabilities to get a visual representation (distance and time taken by the UAS swarm to attack) of the risk of a UAS swarm attack. The estimation of the warning time enables the commander to choose the best course of action for preventing, neutralising and destroying the threat.

Armed sUAS Swarm Threat to India

Armed sUAS Swarm Threat

India faces the armed sUAS swarm threat from China, Pakistan, terrorists and insurgents. India's vital installations, its prominent religious installations, cultural events, sports venues, busy markets, political or other public gatherings are easy targets for an armed sUAS swarm or collaborative attacks by terrorists, insurgents as well as adversaries during hostilities. Its air force, naval and army bases housing a variety of strategic and high-value combat assets are vulnerable to such attacks. Such assets are not only expensive but are also limited in numbers. Its defence installations, naval warships and land forces—especially the ones undertaking counter-terrorism operations in urban areas—also become vulnerable. The sUAS collaborative or swarm attacks conducted on a large scale could cause temporary degradation in the operational readiness of the concerned base for combat.

India's northern neighbour China has developed a wide variety of UCAVs, jet, turboprop MALE, HALE, tactical and small UAS, which could be employed for collaborative operations. China has made considerable progress in its civil as well as military sUAS swarm development programme[61] and it holds the record for developing the world's largest fixed-wing sUAS swarm comprising 119 sUAS,[62] and quadcopter sUAS swarms comprising 1,384 sUAS,[63] in 2017 and 2018 respectively. The demonstration of an armed UAS concept at the Zhuhai Air Show, 2018 indicates the advanced stage of its military UAS swarm programme. China has the potential to employ sUAS swarms against Indian military positions along the border during a conflict. It could also supply sUAS swarms to Pakistan, which could be employed against Indian targets.

India's western neighbour Pakistan does not have a UAS swarm development programme; however, its public sector UAS industry, led by the Pakistan Aeronautical

Complex (PAC) and private sector industry led by MIT graduate Raja Sabri Khan's company Integrated Dynamics, have evolved over a period of time. Pakistan's focus on developing mini and tactical UAS has enabled it to produce a number of UAS of these segments for its armed forces as well as for exporting civilian mini-drones to other countries. Pakistan could employ indigenous UAS against tactical targets and forward posts of the Indian Army and Border Security Force (BSF) along the border in a collaborative manner. The employment of HALE, MALE and tactical UAS by China and Pakistan in a collaborative manner can be neutralised by India's existing air defence network. However, the most likely threat during peace-time or in a less than war situation would emerge from Pakistani intelligence agencies providing training, equipment and financial support to terror groups to employ modified (armed) civil sUAS for collaborative attacks on India. The employment of sUAS swarms could raise new challenges for the Indian security agencies.

Threat from Civil RPAS

The implementation of Drone Regulations 1:0 would change the air defence dynamics of India. The Ministry of Civil Aviation's plan to allow operation of civil Remotely Piloted Aerial Systems (RPAS) in India from December 1, 2018 onwards is yet to take off due to its inability to find takers for its tender for the development, hosting and maintenance of the digital sky platform.[64] The technical challenges in operationalising the digital platform and No Permission No Take Off (NPNT) provision have led to delays in RPAS pilots training by the Flight Testing Organisation and the issue of RPAS manufacturing licences by the Department of Industrial Policy and Promotion (DIPP). The ambiguity in the category for security clearance by the Ministry of Home Affairs (MHA) and issue of equipment type approval by the Wireless Planning and Coordination (WPC) wing have impacted civil RPAS operations. The operationalisation of the digital sky platform would resolve some of these issues. However, it would also lead to an increase in civil RPAS traffic. Regulatory provisions like operators obtaining the Unmanned Aircraft Pilot Licence (UAPL), Unmanned Aircraft Operator Permit (UAOP) and Unique Identification Number (UIN) would deter illegal users and help the monitoring agencies to identify legitimate operators from the illegitimate ones.[65] The equipping of civil RPAS with RFID and GSM SIM cards and digital sky software will enable them to transmit their GPS position by using mobile towers and, thus, facilitate real-time monitoring. However, implementation of the provisions related to registration of civil RPAS would be a challenge. According to one estimate, after imposition of the ban on operation of civil RPAS in India in October 2014, the number of RPAS operating in India rose to

about 5 lakh (half a million).[66] The estimate of the number of unregistered civil RPAS appears to be higher and the threat posed by such RPAS cannot be overlooked. Therefore, a special effort would be needed to register these RPAS,[67] which, if left unregistered, could become a security hazard.[68]

C-sUAS Systems Development by India

The Indian armed forces indicated their intent to develop or acquire Counter-UAS (C-UAS) capability in the Technology and Capability Perspective Roadmap-2018 (TPCR) issued by the Headquarters Integrated Defence Staff (HQ IDS). The TPCR seeks the development of anti-RPA defence system (RF inhibition) comprising electronic scanning radar target detection, EO tracking/classification and directional RF inhibition. The anti-RPA defence system seeks radars having a detection range of more than 40 km, Electro-Optic Targeting System (EOTS) having tracking/classification range of 12 km and RF with an inhibition range of 7 km. The second C-sUAS system that the TPCR seeks is the high energy lasers, which could be employed for the physical destruction of Electronic Welfare (EW) systems, communication systems, radars and antennas of RPAS. The third C-sUAS system is the high energy electromagnetic weapons system to neutralise cellular-microwave tower communication networks, avionics radars of the RPAS up to a range of 5 km in Phase-I, and more than 15 km in Phase-II.[69] On the other hand, the Ministry of Civil Aviation inviting proposals for a live demonstration of anti-drone technologies in February 2018 indicates growing urgency in India to procure the C-sUAS system.[70]

Design and Development Challenges

The Defence Research and Development Organisation (DRDO) had anticipated the C-sUAS requirements of the Indian armed forces as its Laser Science and Technology Centre (LASTEC) had tested the range and effectiveness of the1 kW laser up to a range of 250 m. It also developed a 10 kW Chemical Oxygen Iodine Laser (COIL) and 25 kW laser under the project named 'Aditya'. In addition, the High Powered Microwave (HPM) system was developed under the Kilo Ampere Linear Injector (KALI) project.[71] The development of 2 kW, 5 kW, 9 kW and 30-100 kW lasers is also planned in the future.

The Qualitative Requirements (QRs) for all the three C-UAS systems sought in the TPCR are ambitious as none of the corresponding global C-UAS systems meets all the QRs. Also, the report of the Centre for Study of UAS of 2018 found that most of the C-sUAS developed by global manufacturers performed below the standards claimed by

them. It also observed that some firms were selling existing detection and destruction systems as C-sUAS systems.[72] Therefore, the claims of the global manufacturers cannot be taken at face value and the effectiveness of the C-sUAS would need to be ascertained.

Strategy for C-sUAS Development

The successful and timely development of a C-sUAS by India would depend upon the formulation of realistic QRs and the setting of viable goals. Also, most of the radars being developed globally to detect sUAS are optimised for very short ranges and separate versions of these radars have been developed for detecting sUAS at different ranges. Also, the range of tracking radars for sUAS was between tens of m to 10 km. Similarly, the neutralisation range of RF jammers varied between 2-5 km. The range of most lasers for dazzling sensors and destroying UAS varied between 500 m to 2 km, depending upon the country and its technology readiness levels. Therefore, the QRs for the C-sUAS system being developed in India need to be reviewed to realistic levels and, accordingly, the R&D agencies need to revise their development plans. The final product should be able to do the job, with scope for improvement and upgradation. At the same time, gaps between what is desired and what has been achieved need to be filled at a rapid pace. Therefore, there is a need to review the existing approach to achieve a higher degree of success in developing C-sUAS systems.[73] India, keeping the above deliberations in mind, could consider following a three-pronged approach for building the C-sUAS capability in a graded manner, as suggested below:

- Identify existing systems that can detect, track, neutralise or destroy sUAS, improve coordination among various stakeholders, establish/strengthen communication among various stakeholders and formulate procedures for synergised C-sUAS operations.
- Modify and upgrade existing detection, neutralisation and destruction systems to meet the sUAS swarm threat. This could be done by the software upgradation of existing radars to detect and track sUAS, changeover of frequencies, power, scan pattern, networking and replacement/upgradation of sub-systems.
- Develop new and innovative technologies to counter the sUAS threat that complements existing systems by exploiting the technological potential available in the country.

India's public sector company Bharat Electricals Limited (BEL) and DRDO laboratories have been developing radars and counter-air systems respectively. The detection system of C-sUAS for detecting small and slow aerial platforms would

require optimisation for different Radar Cross-Section (RCS) and speed of UAS. Also, frequencies different from those being used in current detection systems may be required. The C-sUAS systems being developed by the DRDO laboratories have not been operationalised and may have to be modified for neutralising small UAS. Also, software and algorithms play an important role in the C-UAS systems. Indian talent in the IT domain predominantly lies with the private sector, which is the core element of most modern detect, identify, track, neutralise and destroy systems. The second option would be to explore the feasibility of modifying existing detection, tracking, neutralisation and destruction systems for the C-UAS role. The third option would be to explore the feasibility of having a hybrid detection system with two emitters and software options for changing over from detecting small and slow aerial platforms to large and fast ones. India would need to integrate the potential of the private sector with the BEL and DRDO laboratories. An endeavour should be made to harness the talent available in the National Aerospace Laboratory (NAL) and other laboratories of the Ministry of Science and Technology and representatives of the armed forces (users) in the design and development of the C-UAS system.

M-Prize: A New Template for Technology Development

The C-sUAS is not the only technology in which India has lagged or seen delays or failures. The Indian aeronautics ecosystem has often been found wanting in delivering due to various challenges, including distributed responsibility and lack of synergy among various stakeholders. India needed a platform to harness the potential of the public sector, private sector, academia and innovators to develop futuristic aviation technologies. The Indian Air Force (IAF) has shown the way by initiating the Baba Mehar Singh Competition, 2018 also known as the M-Prize, to develop UAS swarms for Humanitarian Assistance and Disaster Relief (HADR) applications. This is the first competition spearheaded by the IAF to find cutting edge technological solutions for its operational needs.[74] This competition covers all the three aspects of design, development and production, involving a prize of Rs 10 lakh, a development fund of Rs 10 crore and production order of Rs 100 crore to the winners. At the same time, an expectation of global standards from the word go would be unrealistic and if the final product can do the job with potential for improvements and upgradation, the competition would achieve its goal. This model could be replicated for developing C-sUAS system by the DRDO, HQ IDS or any of the Services in which one of them takes the lead for developing the C-sUAS system.

Mitigation of sUAS Threat by India

Indian R&D agencies will take some time to develop a C-sUAS system, however, an interim strategy is needed for countering the UAS swarm threat by taking into consideration what is available and what can be modified. As has been discussed earlier, the sUAS swarm threat to India is real and could originate from China, Pakistan, terrorists and insurgents. This paper does not dwell on the threat from tactical, MALE and HALE UAS because they can be countered by using the existing air defence system of India. It is the sUAS swarms and collaborative operations by multiple sUAS that pose a threat to India.

The recent collaborative attacks on the Russian air and naval bases in Syria were neutralised by the Russian forces but at high cost. The release of the C-sUAS strategy by the US Army in 2016 and "Counter-UAS Techniques" in April 2017[75] highlighted the limitations of the existing systems and the need for further research and development of C-sUAS systems. The absence of cost-effective counter-measures with a high level of assurance flagged the need for finding technological solutions, developing tactics and procedures and optimally utilising the existing resources to counter the sUAS swarm threat. Therefore, India would need to formulate an interim strategy by utilising the ingenuity and innovation of its people and pragmatic use of available resources till assured and cost-effective technological solutions are found. The proposed strategy for India to counter the threat from sUAV swarms is discussed below.

Prevention/Denial

The proactive measure to protect critical infrastructure and people from rogue sUAS swarms would be to deny anti-social elements and terrorists the opportunity to launch sUAS swarms by improving policing and keeping a close vigil on their activities. The next endeavour should be to catch the sUAS swarm operators and destroy their assets on the ground. In India, the IAF is responsible for providing air defence cover in the country while the local police is responsible for providing security clearance for civil Remotely Piloted Aircraft System (RPAS) operations. The local police would need to set up Rapid Reaction Teams (RRTs) that should have digital connectivity with the IAF air defence units and be able to neutralise rogue sUAS operators and their assets on the ground at short notice. Therefore, if the IAF detects a rogue sUAS, it should neutralise or destroy it in the air, and if the rogue sUAS survives and lands back on the ground, it should immediately identify the location and pass it on to the RRTs of the local police for neutralisation or destruction of the rogue sUAS operators on the ground.

Dispersal and Decoys

Sean J. A. Edwards (2005) has discussed the history of warfare and employment of swarming tactics in the past to draw lessons for developing anti-swarming measures. He argues that the nature of modern war-fighting is changing, and non-linear[76] and dispersal tactics would be used as a counter to swarm attacks.[77] However, dispersal and decoys have to be relooked at due to the new challenges posed by sUAS swarms. The dispersal plans and decoys meant to deceive high-speed fighters and bombers may not be fully effective against the sUAS, which could be flying low and slow, and be equipped with cameras. The dispersal of soft targets like radars and bomb dumps would also need to be relooked at due to their vulnerability to armed sUAS. Also, realistic decoys would be needed to create confusion for the attacker.

Detection and Tracking

The challenges posed in the detection and tracking of slow-moving rogue sUAS swarms necessitate that new radars are developed or existing radars modified, as has been discussed earlier in the paper. In the meantime, simple measures such as setting up of visual observation posts, utilising Air Traffic Control (ATC) and security personnel, employing ED and IR cameras and integrating them with surveillance and air defence radars, establishing communication among all stakeholders and training such personnel for detection, reporting and neutralisation of the hostile sUAS, can be taken.

Neutralisation and Destruction

The next step in developing a C-sUAS strategy is the neutralisation and destruction of rogue sUAS. The neutralisation could be done by optimally utilising existing jamming systems for disrupting sUAS navigation systems, data links, communication (intra swarm) among the swarm members as well as by spoofing and dazzling of EO/IR sensors. The rogue sUAS swarm could be destroyed by employing existing short range SAMs, anti-aircraft guns, shotguns, etc. If an sUAS swarm or some of its members sneak through and close in, then anti-aircraft guns could be used. However, if some sUAS manage to pass through the above air defence layers and survive, the feasibility of employing shotguns and other short-range C-sUAS systems could be explored . To do that, ATC personnel, armed security guards, bird shooters, etc would need to be equipped, trained and networked in the air defence network. As a whole, there is a need to identify and integrate all the resources that can be employed for the C-sUAS role in the air defence network. The capabilities of all the stakeholders and their systems need to be synergised, communication established amongst them and Standard Operating Procedures (SOPs)

formulated so that they are optimally utilised to increase the effectiveness of the C-sUAS set-up. However, there is a possibility of one's adversaries striking criticial targets with an aim to draw fire from air defence units and deplete the SAM inventory before undertaking actual operations. Therefore, a cost-benefit analysis based on the significance of the VA/VP would be needed before selecting the air defence system against sUAS.

Conclusion

The US and China have demonstrated that sUAS swarms comprising thousands of intelligent sUAS have arrived. China presented the armed sUAS concept at the Zhuhai Air Show in 2018, and going by its past record, it would endeavour to operationalise it soon. The liberal drone regulation allowing operation of civil RPAS has enhanced the potential for employment of sUAS swarm for unauthorised and nefarious activities. This would also enable terrorists to acquire them from the civil market legally or through coercion for carrying out surveillance or launching an armed attack on civil-military installations. This has added to the complexity of the air defence scenario. These events stimulated the development of C-sUAS systems comprising detection, tracking, neutralisation and destruction systems. A number of hand-held, ground-based, vehicle-mounted and airborne C-sUAS swarm systems have emerged worldwide. However, most of the C-sUAS swarm systems are ground-based due to their large size and heavy weight. The hand-held systems have a very low range, while airborne C-sUAS systems are in the development stage.

The neutralisation systems aimed at jamming of the Radio Frequency (RF) and Global Navigation Satellite System (GNSS) have emerged as most popular systems out of the existing C-UAS systems, while other emerging DEW systems such as lasers and HPM are heavy and yet to mature. On the other hand, existing counter-air systems like SAMs are not only expensive but also are available in limited numbers. The innovative solutions like drone capture nets, etc. are yet to become popular due to less probability of success, low range and their dependence on the skill of the shooter. Special munitions are needed for improving the effectiveness of shotguns, anti-aircraft guns and even short-range missiles against sUAS systems. On the other hand, the development of anti-laser paints and laser reflectors for aerial platforms by China could reduce the effectiveness of C-sUAS systems, which has added new challenges for air defence personnel.

The C-sUAS systems, despite the progress, are yet to achieve the desired degree of effectiveness and provide assured C-sUAS capability. Therefore, intensive research is being done to find an effective C-sUAS system, which gives countries like India an opportunity to catch up in this domain. However, India would need to ensure that

users lay down realistic QRs or follow an incremental model for laying down QRs in which different QRs are laid down for different stages of the development. The R&D organisations, on the other hand, would need to be honest about the actual technological levels with the users and make an R&D plan which is realistic and meets the requirements of the users. Also, it is important that the potential available in the entire country is harnessed to develop futuristic technologies like C-sUAS. The IAF's "Mehar Baba UAS Challenge" for developing UAS swarms for HADR applications is an important endeavour in this direction. It could help in reducing the development timelines, broadening the competition between public and private sector entities and giving a platform to start-ups and individual innovators. The competition could act as a template for developing the C-UAS system and other cutting edge technologies within the country.

Indian military and civil aviation, and internal security agencies need an air defence system, which provides a reasonable degree of assurance of countering the sUAS swarm threat. To do that, the C-sUAS framework must ensure that the defence forces, internal security agencies and police have inter-organisation as well as intra-organisation coordination and synergy to provide an effective response to the sUAS swarm threat. Simultaneously, the three-tier strategy as proposed in the paper may be pursued for building the C-sUAS capability on immediate, mid-term and long-term bases. However, to develop such capability, the QRs for the proposed C-sUAS system should be reviewed to realistic levels with an aim to develop a system that can do the job, and the higher performance could follow later. This approach would ensure that the sUAS swarm threat is mitigated, at low cost, and an acceptable level of air defence capability is developed within a reasonable timeframe, while keeping the scope for upgradation of C-sUAS systems to a later date.

Notes

1. Jason Brownlee, "Clever Algorithms: Nature-Inspired Programming Recipes", http://www.cleveralgorithms.com/nature-inspired/swarm.html. Accessed on December 12, 2017.
2. David Hambling, "Drone Swarms, will Change the Face of Modern Warfare", *Wired Online Magzine,* January 7, 2016, http://www.wired.co.uk/article/drone-swarms-change-warfare. Accessed on July 25, 2017.
3. Zhang Qiang, "Smart Drone Bee Swarm Will Change the Rules of Battle", March 29, 2017, http://kepu.gmw.cn/2017-03/29/content_24084029.htm. Accessed on April 30, 2018.
4. Nikolai Novichkov, "Airshow China 2018: Norinco Presents UAV Swarm Concept", November 09, 2018, *Jane's Defence Weekly*, https://www.janes.com/article/84438/airshow-china-2018-norinco-presents-uav-swarm-concept. Accessed on February 2, 2019.
5. "Technology Perspective and Capability Roadmap (TPCR)–2018", HQ IDS, Ministry of Defence, https://mod.gov.in/sites/default/files/tpcr.pdf. Accessed on November 30, 2018.

6. "UAV Swarm Operational Risk Assessment System", Naval Post Graduate School, September 2015, http://www.dtic.mil/dtic/tr/fulltext/u2/1009315.pdf. Accessed on August 29, 2018.
7. Dave Majumdar, "Who Attacked a Russian Military Base with a 'Swarm' Strike?", *The National Interest,* January 12, 2018, https://nationalinterest.org/feature/who-attacked-russian-military-base-swarm-strike-24060. Accessed on October 12, 2018.
8. David Reid, "A Swarm of Armed Drones, Attacked a Russian Military Base in Syria", CNBC, January 11, 2018, URL: https://www.cnbc.com/2018/01/11/swarm-of-armed-diy-drones-attacks-russian-military-base-in-syria.html. Accessed October 11, 2018.
9. Jeff Deniel, "Russia Says it Killed Rebels Behind Swarm Drone Attack in Syria; Experts See more Such Strikes Ahead", *CNBC,* January 12, 2018, https://www.cnbc.com/2018/01/12/russia-says-it-eliminated-rebels-behind-swarm-drone-attack-in-syria.html. Accessed on October 12, 2018.
10. Tom Mckay, "Venezuelan Officials Allege Attempted Drone Assassination of President Nicolas Maduro", August 5, 2018, https://gizmodo.com/venezuelan-officials-allege-attempted-drone-assassinati-1828117707. Accessed on October 12, 2018.
11. "RAVENS CHALLENGE: Counter-Drone Technology to be Demonstrated in Thailand: US Military Coming — American Firms Staying Home", Michaelyon-online.com, August 17, 2018, https://www.michaelyon-online.com/ravens-challenge-counter-drone-technology-to-be-demonstrated-in-thailand-us-military-coming-Camerican-firms-staying-home.htm. Accessed on October 20, 2018.
12. Arthur Holland Michel, "Counter Drone Systems", Centre for the Study of the Drone, February 20, 2018, http://dronecenter.bard.edu/files/2018/02/CSD-Counter-Drone-Systems-Report.pdf. Accessed on October 20, 2018.
13. Tim Wright, "When is a Drone Swarm Not a Swarm?", airspacemag.com, January 12, 2018, https://www.airspacemag.com/daily-planet/when-drone-swarm-not-swarm-180967820/. Accessed on October 11, 2018.
14. Gareth Corfield, "British and US Militaries Drone Swarm Hackathon Definitely isn't About Army Technology", February 13, 2019, https://www.theregister.co.uk/2019/02/13/uk_us_drone_swarm_hackathon/. Accessed on February 15, 2019.
15. Nikolai Novichkov, Dmitry Fedyushko, "Swarm Drone, New Tactics of Fighting Unique Weapons of China", November 14, 2018, https://tass.ru/armiya-i-opk/5786857. Accessed on February 2, 2019.
16. Nikolai Novichkov, "Airshow China 2018: Norinco Presents UAV Swarm Concept", November 9, 2018, *Jane's Defence Weekly*, https://www.janes.com/article/84438/airshow-china-2018-norinco-presents-uav-swarm-concept. Accessed on February 2, 2019.
17. "LOCUST: Autonomous, Swarming UAVs Fly into the Future", Office of Naval Research, April 14, 2015, https://www.onr.navy.mil/en/Media-Center/Press-Releases/2015/LOCUST-low-cost-UAV-swarm-ONR. Accessed on February 2, 2019.
18. Richard Scott, "DARPA Awards Phase 2 Contracts for Gremlins Programme", *Jane's International Defence Review,* March 20, 2017, http://www.janes.com/article/68840/darpa-awards-phase-2-contracts-for-gremlins-programme. Accessed on December 9, 2017.
19. "Department of Defence Announces Successful Micro-Drone Demonstration", US Department of Defence, January 9, 2017, https://dod.defense.gov/News/News-Releases/News-Release-View/Article/1044811/department-of-defense-announces-successful-micro-drone-demonstration/. Accessed on February 2, 2019.
20. Wendell Minnik, "Zhuhai 2016: China Unveils Anti-Ship Missiles", *Shephard Press Limited,* November 3, 2016, https://www.shephardmedia.com/news/defence-notes/zhuhai-2016-china-unveils-anti-ship-missiles/. Accessed on January 4, 2018.
21. Michel, n. 12.

22. "Drone Guard Detection and Disruption Counter UAV System", Israel Aerospace Industries (IAI), http://www.iai.co.il/Shared/UserControls/Print/PopUp.aspx?lang=en&docid=47062. Accessed on October 13, 2018.
23. Alexander George, "Stopping Killer Drone Swarms Before They Kill Us", *Popular Machines,* July 6, 2018, https://www.popularmechanics.com/military/research/a21272146/swarm-killer-drone-defense/. Accessed on October 16, 2018.
24. "Blighter to Supply Counter-UAV Technology to Liteye Systems for Multi-Million-Dollar US Department of Defense Contract", *PR Newswire,* October 25, 2018, https://www.prnewswire.com/news-releases/blighter-to-supply-counter-uav-technology-to-liteye-systems-for-multi-million-dollar-us-department-of-defense-contract-898639511.html. Accessed on October 26, 2018.
25. Michel, n. 12.
26. Jeffery Lin and P.W.Singer, "Here's how China is Battling Drones", March 28, 2017, http://www.popsci.com/chinas-new-anti-drone-weapons-jammers-and-lasers. Accessed on April 10, 2017.
27. Stephen Chen, "US Lasers? PLA Preparing to Raise its Deflector Shields", *South China Morning Post*, https://www.scmp.com/news/china/article/1444732/us-lasers-pla-preparing-raise-its-deflector-shields. Accessed on October 17, 2018.
28. George, n. 23.
29. Keving Robinson-Avila, *Task Purpose,* June 21, 2019, https://taskandpurpose.com/air-force-thor-microwave-weapon. Accessed on July 27, 2019.
30. "Pantsir-SA Arctic Short-Range Air Defence Missile System", Army Recognition Group, February 15, 2018, https://www.armyrecognition.com/russia_russian_missile_system_vehicle_uk/pantsir-sa_arctic_short-range_missile-gun_air_defense_system_technical_data_sheet_specifications_pictures_video_11604176.html
31. Michel, n. 12.
32. Joseph Trevithick, "Army Buys Small Suicide Drones to Break Up Hostile Swarms and Potentially More", *The Warzone*, July 17, 2018, http://www.thedrive.com/the-war-zone/22223/army-buys-small-suicide-drones-to-break-up-hostile-swarms-and-potentially-more. Accessed on February 5, 2019.
33. Andrew Galer, "Russian REX-1 Counter-UAV System Breaks Cover on Exercise", *Jane's 360*, September 14, 2018, https://www.janes.com/article/82990/russian-rex-1-counter-uav-system-breaks-cover-on-exercise. Accessed on October 15, 2018.
34. Dedrone, *Elbit Systems,* http://elbitsystems.com/pr-new/elbit-systems-presents-advanced-systems-market-leading-capabilities-dsei-exhibition-2017/, October 12, 2018.
35. DroneCannon RW, *Droneshield,* https://www.droneshield.com/dronecannonrw/. Accessed on October 13, 2018.
36. n. 22.
37. JR Wilson, "The Dawn of Counter-Drone Technologies", *Military & Aerospace,* November 1, 2016, https://www.militaryaerospace.com/articles/print/volume-27/issue-11/special-report/the-dawn-of-counter-drone-technologies.html. Accessed on October 16, 2018.
38. Samuel Bendett, "How Russia's Military Plans to Counter the Pentagon's Drone Swarms", January 10, 2017, http://nationalinterest.org/blog/the-buzz/how-russias-military-plans-counter-the-pentagons-drone-19014. Accessed on April 10, 2017.
39. "Skylock Anti-Drone System", Skylock, Avnon Group, https://www.skylock1.com/. Accessed on October 15, 2018.
40. Patrik Howell O'Neill, "Drones Emerge as a New Dimension in Cyberwarfare", *Cyberscoop,* February 5, 2018, https://www.cyberscoop.com/apolloshield-septier-drones-uav-cyberwar-hacking/. Accessed on October 12, 2018.

41. Paul Scharre, "Counter-Swarm: A Guide To Defeating Robotic Swarms", *War on The Rocks,* March 31, 2015, https://warontherocks.com/2015/03/counter-swarm-a-guide-to-defeating-robotic-swarms/. Accessed on October 22, 2018.
42. Ben Watson, "The Drones of ISIS", *Defence One,* January 12, 2017, https://www.defenseone.com/technology/2017/01/drones-isis/134542/. Accessed on October 20, 2018.
43. Buettner, Jr and R Raymond, "A Swarm Vs Swarm Autonomous Systems Grand Challenge Competition", Naval Postgraduate School, April 19, 2018, https://my.nps.edu/web/cag/-/a-swarm-vs-swarm-autonomous-systems-grand-challenge-competition. Accessed on October 22, 2018.
44. Timothy H Chung, "50 vs. 50 by 2015: Swarm vs. Swarm UAV Live-Fly Competition at the Naval Postgraduate School", *Calhoun: The NPS Institutional Archive*, 2013, https://core.ac.uk/download/pdf/36740424.pdf. Accessed on October 22, 2018.
45. "Swarm vs. Swarm: Student Teams Compete in Service Academies Swarm Challenge – with GTRI Assistance", Georgia Research Tech Institute, March 11, 2017, https://www.gtri.gatech.edu/newsroom/swarm-vs-swarm-student-teams-compete-service-academies-swarm-challenge-gtri-assistance. Accessed on October 22, 2018.
46. Laurent Beaudoin et al., "Potential Threats of UAS Swarms and the Countermeasure's Need", March 17, 2015, https://hal.archives-ouvertes.fr/hal-01132236/document. Accessed on October 14, 2018.
47. Ingrid Fadelli, "Networked UAV Defense Swarms to Defend Against Malicious Drones", *Tech Explore,* August 31, 2018, https://techxplore.com/news/2018-08-networked-uav-defense-swarms-defend.html. Accessed on October 13, 2018.
48. "Defending against Intrusion of Malicious UAVs with Networked UAV Defense Swarms", September 2, 2018, https://arxiv.org/pdf/1808.06900.pdf. Accessed on October 13, 2018.
49. Paul Scharre, "Counter-Swarm: A Guide To Defeating Robotic Swarms", *War on The Rocks,* March 31, 2015, https://warontherocks.com/2015/03/counter-swarm-a-guide-to-defeating-robotic-swarms/. Accessed on October 22, 2018.
50. Andy Greenberg, "Watch a Test of Anti-Drone Weapons from Shotguns to Super Drones", *Wired*, July 26, 2017, https://www.wired.com/story/watch-anti-drone-weapons-test/. Accessed on October 13, 2018.
51. Feilidh Dwyear, "US Military Designs new Grenade to Take Down Enemy Drone", *We Talk UAV*, February 10, 2019, https://www.wetalkuav.com/net-grenade-to-take-out-drones/. Accessed on February 12, 2019.
52. Greenberg, n. 50.
53. Michel, n. 12.
54. Ibid.
55. MITRE operates the Federally Funded Research and Development Centres (FFRDCs) that assist the United States government with scientific research and analysis; development and acquisition; and systems engineering and integration. FFRDC projects cover various strategic domains including defence, aviation, space, energy, homeland security etc. However, FFRDC cannot manufacture products or compete with the industry. (https://www.mitre.org/centers/we-operate-ffrdcs)
56. "MITRE Challenge: Countering Unauthorised Unmanned Aircraft Systems", MITRE, https://www.mitre.org/research/mitre-challenge/mitre-challenge-uas. Accessed on October 19, 2018.
57. Bill Carey, "Mitre Names Winners of Counter Drone System Challenge", AINonline, September 14, 2016, https://www.ainonline.com/aviation-news/aerospace/2016-09-14/mitre-names-winners-counter-drone-system-challenge. Accessed on October 19, 2018.
58. "Wanted: Novel Approaches for Detecting and Stopping Small Unmanned Air Systems: *DARPA",* September 22, 2017, https://www.darpa.mil/news-events/2017-09-22. Accessed on October 21, 2018.

59. Peter Nicholls, "Trump Signs Law Allowing US Authorities to Shoot Down Private Drones Without Warrants", *RT,* October 6, 2018, https://www.rt.com/usa/440481-us-shoot-down-private-drones/. Accessed on October 13, 2018.
60. "UAV Swarm Operational Risk Assessment System", Naval Post Graduate School, September 2015, http://www.dtic.mil/dtic/tr/fulltext/u2/1009315.pdf. Accessed on August 29, 2018.
61. Elsa B. Kania, "Chinese Advances in Unmanned Systems and the Military Applications of Artificial Intelligence—the PLA's Trajectory Towards Unmanned, Intelligentized Warfare", Government Publishing Office (US), February 23, 2017, https://www.uscc.gov/sites/default/files/Kania_Testimony.pdf. Accessed on April 27, 2018.
62. "China Launches Record-Breaking Drone Swarm", Xinhua November 6, 2017. Accessed on March 13, 2018, URL: http://www.xinhuanet.com/english/2017-06/11/c_136356850.htm.
63. "EHang Egret's 1374 Drones Dancing over the City Wall of Xi'an, Achieving a Guinness World Records Title", April 29, 2018, http://www.ehang.com/news/365.html. Accessed on June 19, 2018.
64. "Development, Hosting and Maintenance of Digital Sky Portal and Mobile App for MoCA", Airport Authority of India, October 3, 2018, https://www.aai.aero/en/node/93613. Accessed on February 10, 2019.
65. "Requirements for Operation of Civil Remotely Piloted Aircraft System (RPAS)", Director General of Civil Aviation, Government of India, August 27, 2018, http://dgca.nic.in/cars/D3X-X1.pdf. Accessed on September 8, 2018.
66. n. 11.
67. Sai Pattambiram, "Regulations and Indigenous Tracking Solution will Ensure Safe Drones in India", *BusinessWorld,* October 20, 2018, http://www.businessworld.in/article/Regulations-And-Indigenous-Tracking-Solutions-Will-Ensure-Safe-Drones-In-India/20-10-2018-162590/. Accessed on October 21, 2018.
68. Sai Pattambiram, CEO, Sree Sai Aerotech Innovations Pvt Ltd, in an email to the author on October 19, 2018.
69. "Technology Perspective and Capability Roadmap (TPCR) -2018", Ministry of Defence, India, https://mod.gov.in/sites/default/files/tpcr.pdf. Accessed on October 15, 2018.
70. Notice, http://www.civilaviation.gov.in/sites/default/files/Public%20Notice%20reg%20live%20demo%20in%20March-extension.pdf. Accessed on October 15, 2018.
71. Shaurya Karangbir Gurung, "India gets a Step Closer to Laser Weaponry as DRDO Successfully Tests Laser System", *The Economic Times,* July 14, 2018, https://economictimes.indiatimes.com/news/defence/india-gets-a-step-closer-to-laser-weaponry-as-drdo-successfully-tests-laser-system/articleshow/61954646.cms. Accessed on October 15, 2018.
72. Michel, n. 12.
73. John Pyrgies, "A Kamikaze Attack by Swarming Drones: Nightmare or Reality?", http://www.securityeurope.info/a-kamikaze-attack-by-swarming-drones-nightmare-or-reality/. Accessed on December 4, 2017.
74. "Mehar Baba Prize Competition for UAS Swarms", http://indianairforce.nic.in/meharbaba/. Accessed on October 23, 2018.
75. "ATP 3-01.81, Counter-Unmanned Aircraft System Techniques", April 2017, https://fas.org/irp/doddir/army/atp3-01-81.pdf. Accessed on October 21, 2018.
76. Non-linear is a process or series of events, etc. in which one thing does not clearly or directly follow from another or is not arranged in a straight line or not sequential. http://dictionary.cambridge.org/dictionary/english/non-linear. Accessed on August 1, 2017.
77. Sean J. A. Edwards, "Swarms and Future of Warfare", Pardee Rand Graduate School, pp.66-68, https://www.rand.org/pubs/rgs_dissertations/RGSD189.html. Accessed on November 27, 2017.