ExpertView

Centre for Air Power Studies (CAPS)
Forum for National Security Studies (FNSS)
04/23

C-UAS: Detect, Disrupt, Disable, Destruct, and Intercept (D4-I)

Gurcharan Singh Bedi

16 March, 2023

Keywords: Counter-UAS, Electro-Optical/Infrared, X and Ku-band

Introduction

Given the popularity of the acronym 'C4-I,' a new term may be warranted in the discussion of the Counter-Unmanned Aircraft Systems (C-UAS) strategy. 'D4-I' is proposed to stand for 'Detect, Disrupt, Disable, Destruct, and Intercept.' The Defence Research and Development Organisation (DRDO) does refer to its anti-drone system as D4: 'Drone, Detect, Deter, and Destroy.' However, it is felt that 'D4-I' is a more inclusive expression. The measures listed under D4-I are all essential components of a worthy counter-drone strategy, though they are not necessarily employed in totality or in any particular order. What gets used fundamentally depends on what is available and, if more than one is, how the threat emerges. Successful threat mitigation calls for the application of suitable technology and strategy. Therefore, the aim is to scan for the best technologies and suggest a way forward for formulating a good strategy for Counter-UAS operations.

The Threat

There are daily reports of drone intrusions in the Punjab sector, most likely for drug smuggling, but they can take any form. The availability of low-cost commercial off-the-shelf systems has exacerbated the problem. Almost every defence stall at the recently concluded Aero India show in Bengaluru had a drone presence in some form or another, ranging from large wingspan fixed-wing platforms to hovering quadcopters. A drone can conduct intelligence, surveillance, and reconnaissance (ISR) missions to collect real-time intelligence as well as carry weapons. A small drone's ability to direct fire can transform a legacy firing gun into a sniper rifle, significantly increasing

the fighting potential. Similarly, the presence of small drones in the flight path of an aircraft, particularly in the take-off or landing funnel, can prove disastrous.

The Challenge

While traditional radars used to detect conventional aircraft would be adequate for large fixed-wing UAS, the low, slow, and small (LSS) category has emerged as a concerning challenge. The Counter-UAS response is based on threat evaluation of what is seen and documented. Therefore, it is necessary to develop a capability in which nothing goes undetected to develop an effective C-UAS response.

Detection

A drone can be detected through electro-optical/infrared (EO/IR) cameras, acoustic sensors, radio frequency (RF) detectors, or radar systems. The limited field of view of an EO/IR device will need cueing, which can only be provided by radar. Additionally, these devices will be adversely affected by atmospheric obscurities and emissivity. The acoustic signature produced by LSS drones will invariably get masked by the normal urban environmental noise, providing a very short detection range. Therefore, while high-definition EO/IR cameras, acoustics sensors, and RF detection can play an important role in creating a multisensory solution, a real 3D situational awareness can only be built with radar.

Detection Radar

Drones were deemed more similar to birds in terms of characteristics and behaviour, so the majority of drone detection radars were modelled after avian radars, which evolved from marine radars designed to detect slow-moving targets on a flat surface. Therefore, the most prevalent avian radar systems utilised readily available marine band radar technology (S-band and X-band) optimised for detecting and tracking birds.[1] The S-band was commonly used to track long-distance migratory birds, while the X-band was effective for tracking smaller birds near airports. However, according to a study commissioned by the Federal Aviation Administration (FAA) titled “Bird detection radar effectiveness,” the detection probability was not particularly high.[2] While a false negative (not showing when something is present) or a false positive (showing something when it is not present) would not be catastrophic in the case of a bird hazard, a drone that goes undetected can be extremely hazardous.

A drone detection radar, in general, should be able to detect a small radar cross-section object moving at a very slow speed, from ground level upwards. It should be able to distinguish between objects that are close together in both range and azimuth. It must have very high-class algorithms and the necessary artificial intelligence/machine learning (AI/ML) functions to reject false positives such as birds, kites, balloons, and so on in its area of influence while completely eliminating false negatives.

The X-band is a popular band in modern-day drone detection radars. However, the Ku-band has not received the attention it deserves in this domain. In comparison to the X-band, the Ku-band provides better resolution, suffers less off-boresight degradation, and can measure micro-doppler shift, resulting in better slow-moving detection. In addition, its sharp beam is 'jamming-resistant,' and its smaller antennae aid in quick mobility. This is not to dismiss the X-band entirely, but to emphasise the importance of including the Ku-band in drone detection. It may even be prudent to use a combination of both bands to cover a critical area completely, but leaving the Ku-band out of the radar equation is not desirable when developing a comprehensive drone detection solution.

Disrupt and Disable

Typically, drones are controlled by their operator via an RF link. Jamming this link would disrupt their operation for the set duration, after which they could resume normal operation. It may even render them completely ineffective for the operation and cause them to return home if programmed to do so. The effect of jamming navigational guidance is similar.

Proponents of alternative counter-operational methods frequently highlight two issues with jammers. First, because the vast majority of commercially available drones are industrial, scientific, and medical (ISM) compliant and operate in common Wi-Fi (2.4 and 5 GHz) or (400 and 900 MHz) bands, the vast majority of jammers target these frequencies. As a result, RF jammers are only useful against compliant operators, while the problem is with those who do not adhere to these frequencies. Second, autonomous drones can operate independently of an RF link along a predetermined path, eliminating the need for guidance and rendering jamming useless. Furthermore, it is claimed that jamming may interfere with friendly platforms that use the same spectrum.

Russia is said to have had 90 per cent success in jamming Ukrainian drones at the start of the war.[3] Ukraine had to modify the SpaceX-supplied Starlink terminals, primarily intended for

backup communication, to guide the drones. Elon Musk had objected to this modification.[4] Regardless of the arguments against jammers' utility, it would not be prudent to exclude them from the countermeasures. They provide an immediate on-site response and, simply by being present, would close off one dimension for the opponent. They are likely to force the opponent to use more complex and expensive options, such as unconventional bands for controlling and operating drones autonomously. In the event that own platforms are jammed inadvertently, it will be reported, and the jamming can be stopped. The C-UAS arsenal must include credible GPS and RF jammers that can target bands outside the ISM spectrum.

Destruction

Jamming a drone can render it useless for its current mission, only to have it reappear later. However, if the overall threat must be mitigated for an extended period, destruction may be necessary. There are two methods of drone destruction: kinetic and non-kinetic. Under the kinetic option, small arms are used, however they have imprecise accuracy and a short range, while long-range air defence missiles are not cost-effective against a large number of potential threats. Non-kinetic options consist primarily of directed energy weapons like lasers and microwaves.

High-Energy Laser (HEL) and High-Energy Microwave (HPM) complement each other in combating drones. While HEL can destroy individual drones, HPM can eliminate swarms. It is still a work in progress, and the technology is not mature enough for use on the battlefield. Defence tech giants like Northrop Grumman and Raytheon Technologies have made substantial investments in this field. The Rapid Capabilities and Critical Technologies Office (RCCTO) of the United States Army recently awarded Epirus, a technology company in the USA, a US $66.1 million contract in support of the indirect fire protection capability-HPM program[5] which indicates that it is still a work in progress.

In India, DRDO has also developed a laser system, which was deployed at the Red Fort prior to 2022 Independence Day[6] as part of the C-UAS system. It claims to have an effective range of 1.25km based on the wattage. However, there has not been any significant HPM development reported in India to counter the UAS threat.

Interception

The falling wreckage of a Ukrainian UAV that was shot down at low altitude while approaching the Engels Military Airfield in Russia killed three technical staff members in December last year.[7]

Defending an active airfield against a drone attack presents different difficulties than defending a battlefield. Due to the presence of one's own aircraft in the area, it may be necessary to restrict the use of jammers. The destruction of the threatening drone, through kinetic or non-kinetic means, over an airfield could cause extensive damage to personnel and valuable assets on the ground. There may arise a circumstance in which drones cannot be jammed or destroyed. Intercepting and seizing the drone may be the only viable option.

Diverse types of net-and-gun-equipped drone hunters have emerged on the market. The net can be launched from the ground or by an additional drone. A drone equipped with a net can either transport a lightweight drone to a safe location or fire a net at the target, causing it to descend using a parachute. The ground radar triggers the launch of these net-firing drones, which then pursue the detected threat. The majority of them must be manoeuvred to a point where the onboard EO device can precisely locate the target and fire the net. Emerging technology, however, has integrated an airborne intercept radar onboard the drone itself. This arrangement renders the operation entirely autonomous with a very high rate of interception success. Moreover, a skilled drone hunter carries redundancy on board to cater for more than one target or reengage in case of a failed interception. An airborne intercept radar onboard the drone hunter is considered a game-changer and has the scope for a variety of futuristic applications.

Capability and Way Forward

The DRDO's D4 system, displayed at Aero India 2023, is an indigenously developed anti-drone system manufactured by Bharat Electronics Ltd. It is capable of countering any security threat within a 4km radius. It boasts multisensory detection with day/night cameras, radar, and soft and hard kill options via laser and jamming. Zen Technologies has also supplied a small number of C-UAS systems to the Indian Air Force with similar capabilities minus the hard kill option,[8] although the specifics are unknown. In addition, the Indian Army issued a Request for Proposal (RFP) for 20 C-UAS systems on January 18, 2023, seeking a very niche capability. According to the RFP, "the system should be able to detect, track, identify, and neutralise swarm/drones/UAS approaching

simultaneously from multiple directions."[9]Arguably a tall order, the real question is if the capability is available at par with the emerging threat.

While there are at least 500 companies in India, as per a survey done by the Border Security Force (BSF),[10] that could assist in the development of anti-drone solutions, the options for bringing down a drone are still extremely limited. Indigenous development is, without a doubt, the ultimate solution, but the process must be accelerated. The chasm between the drone threat and countermeasures is widening daily. R&D is always a time-consuming activity that must run concurrently with procurement. Nevertheless, the drone threat is imminent and real. Detection radars tailor-made for LSS threats, smart jammers catering to unconventional bands, development of safe and high-power lasers, HPM technology, and autonomous drone hunters with AI/ML features are some of the capabilities that must be possessed quick. Even with a few concessions on Indian content initially, the country may benefit from meaningful collaborations with advanced companies to acquire and develop the above-mentioned niche technologies.

Note:

[1] "Advisory Circular", *U.S. Department of Transportation*, November 23, 2010, https://www.faa.gov/documentLibrary/media/Advisory_Circular/AC_150_5220-25.pdf. Accessed on March 8, 2023.

[2] "Russia's Electronic-Warfare Troops Knocked Out 90 Percent Of Ukraine's Drones", *Forbes*, December 24, 2022, https://www.forbes.com/sites/davidaxe/2022/12/24/russia-electronic-warfare-troops-knocked-out-90-percent-of-ukraines-drones/?ss=aerospace-defense&sh=6318fb6575cf

[3] "Russia's Electronic-Warfare Troops Knocked Out 90 Percent Of Ukraine's Drones", *Forbes*, December 24, 2022, https://www.forbes.com/sites/davidaxe/2022/12/24/russia-electronic-warfare-troops-knocked-out-90-percent-of-ukraines-drones/?ss=aerospace-defense&sh=6318fb6575cf. Accessed on March 8, 2023.

[4] Joey Roulette, "SpaceX curbed Ukraine's use of Starlink internet for drones -company president", *Reuters*, February 9, 2023, https://www.reuters.com/business/aerospace-defense/spacex-curbed-ukraines-use-starlink-internet-drones-company-president-2023-02-09/. Accessed on March 8, 2023.

[5] "U.S. Army Awards Epirus $66.1m Contract For Leonidas Directed Energy System", *Epirus*, https://www.epirusinc.com/news-item/us-army-awards-epirus-661m-contract-for-leonidas-directed-energy-system. Accessed on March 8, 2023.

[6] https://indianexpress.com/article/cities/delhi/delhi-i-day-security-red-fort-counter-drone-system-8090272/. Accessed on March 8, 2023.

[7] "Ahead of I-Day, DRDO deploys its counter-drone system near Delhi's Red Fort area", *Indian Express*, August 14, 2022, https://www.ndtv.com/world-news/3-soldiers-killed-from-falling-ukrainian-drone-wreckage-at-russian-base-3638473. Accessed on March 8, 2023.

[8] "India air force orders Zen Technologies counter-drone for $21-million", Defence Capital, September 3, 2021, https://defence.capital/2021/09/03/india-air-force-orders-zen-technologies-counter-drone-for-21-million/. Accessed on March 8, 2023.

[9] "Army floats RFP for 20 vehicle-based drone jammers", *Indian Express*, January 19, 2023, https://indianexpress.com/article/india/army-rfp-vehicle-based-drone-jammers-8391062/. Accessed on March 8, 2023.

[10] "BSF to dig into pool of 500 companies for anti-drone technology", *Indian Express*, July 2, 2021 https://indianexpress.com/article/india/bsf-it-ministry-companies-border-security-drone-attack-7386310/. Accessed on March 8, 2023.