Counter-drone technologies value chain

Leading technologies involved in this theme

Source: GlobalData Counter-Drone Technologies – Thematic Research

Radar is one of the most used ground-based C-UAS capabilities

Picture credit: Getty

SERVE AND PROTECT

Pinky Hiranandani *explains why drone security remains a critical factor as the market takes-off*

The widespread use of drones, particularly for commercial and military use cases, has increased the associated security risk. Drones interact with their base using unencrypted communication channels, exposing the sensitive information they collect. As more drones enter both public and private airspace, drone security will become paramount for national and local governments, law enforcement agencies, critical infrastructure and public venues. To counter this emerging threat, investments in Counter-Unmanned Aerial Systems (C-UAS) capabilities are essential.

Malicious drone interference has compelled commercial end-users, including industrial conglomerates, universities, utilities and sports organisations to explore drone mitigation solutions. Against this backdrop, the focus of drone manufacturers has shifted to counter UAS systems.

Biological countermeasures, such as using eagles to detect and neutralise rogue drones in restricted airspaces, are also being explored. Commercial flights are already being disrupted by drones. For instance, in December 2018, Gatwick Airport was closed for 33-hours due to a perceived threat from drones. To help resume operations, Leonardo's Falcon Shield counter-drone system was used to detect, track and mitigate rogue drone threats.

Physical security includes the use of hardware for detecting, tracking and interdicting UAS threats, while software security refers to cyber protection against hackers. The counter measures deployed in the defence industry are more likely, but are not exclusively to be used for neutralising larger UAS platforms (High-Altitude Long Endurance (HALE) and medium-altitude long-endurance (MALE) drones). In the civil market, these measures are deployed to neutralise small unmanned aerial systems (sUAS).

Counter UAS physical systems fall under three broad categories: ground-based, hand-held and aerial based. Ground-based counter UAS systems are used to detect and track incoming drone threats, and include devices such as radar, radio frequency sensors, electro-optical (EO)/infrared (IR) sensors, combined sensors and acoustic. Hand-held devices used for interdicting drone threats include unconventional and conventional projectiles. The aerial-based counter UAS systems include jamming, directed energy, and cyber tools.

Of the various ground-based systems, radar is one of the most used C-UAS capabilities. Numerous radars, such as low-frequency pulse radar, have been designed to detect large metal objects like planes and helicopters, but are less suited for detecting small radar cross-sections and carbon body objects that fly lower to the ground, as such as UAVs in Group 1 (Max gross takeoff weight of <20lbs. and operating altitude of <1200 above ground level (AGL)) and Group 2 (21–55lbs. and <3500 AGL).

One method that developers can use to increase the accuracy of their C-UAS systems, and reduce the frequency of false positives is to incorporate multiple detection and interdiction techniques into their systems. By corroborating different forms of data from multiple sensors, the system can accurately triangulate legitimate UAS threats and filter out false positives that otherwise would have been flagged.

Conventional projectiles are hand-held devices which include air-to-air munitions, surface-to-air missiles, and small arms munitions. Of these, surface-to-air missiles are perhaps the most traditional means of UAV interdiction, and for specific segments of the UAV population (Groups 3-5) they are the most effective. Cheaper interdiction methods such as small arms munitions, unconventional projectiles and DEW are a more appropriate choice for small drone interdiction.

Common unconventional projectiles include collision drones and nets. Other promising projectiles include water cannons, which the US Defense Systems Information Analysis Center regards as a low-cost defence option especially for aboard naval vessels. A water cannon was used at the 2016 US Air Force Research Laboratory's Commander's Challenge to successfully bring down a drone during a C-UAS exercise.

Under aerial-based systems, directed energy is used, which includes dazzling, lasers and high-power microwaves. Of these, lasers are a low-cost-per-shot option, requiring only electrical energy rather than chemically propelled munitions – making them an attractive choice for C-UASs.

Under jamming, RF and GNSS jamming systems are used as counter measures. RF jamming as an interdiction is being extensively used in many C-UAS products and will face more advanced threats from evolving UAS technologies. There are now commercially available UAS that utilise mobile LTE networks rather than conventional RF links.

Going forward, with the likely widespread deployment of drone swarms, jamming (RF and GNSS) and spoofing – where false GPS signals are broadcasted to UAS receiver – provide a cost-effective means of disrupting a swarm or a single UAS by preventing coordination among individual elements, collapsing the swarm so that it disintegrates into many disparate, uncoordinated elements and by preventing communication between the UAS and the operator.

The value chain graphic opposite highlights the technologies used for cyber counter drone security. Cyber-attack against UAS platforms include violations such as **data confidentiality** – where information is intercepted between the Ground Control Stations (GCS) and the platform; **data integrity** – where information is falsified in transfer between the GCS and the platform; and **data availability** – where communication between the GCS is disrupted**.**

> **DRONE SECURITY WILL BECOME PARAMOUNT AS MORE DRONES START TO ENTER INTO AIRSPACE**

Spoofing devices deceive a GPS signal by broadcasting false GPS signals to the UAS's receiver. Spoofing is considered a step ahead of jamming since the latter can disrupt a receiver but not deflect or redirect it. Additionally, regarding collateral damage, spoofing holds an advantage over jamming. The use of spoofing is more common in communications and mechanisms which do not have a high degree of security. Companies like Dedrone, Sharper Shape, DroneShield, Drone Defense and SkySafe offer software-based protection against hackers.

The US recognises that UAS could provide its adversaries with a low-cost means of attacking or conducting ISR missions against US forces and that smaller UAS cannot be detected by traditional air defence systems due to their size, construction material and flight altitude. In light of this, in FY2023 the US Department of Defense (DOD) plans to spend at least $668 million on C-UAS research and development and at least $78 million on C-UAS procurement.

To counter UAV threats, branches of the US military have undertaken several development projects. The Air Force is testing high-powered microwaves and lasers for C-UAS missions. For example, in October 2019, the Air Force received delivery of a vehicle-mounted C-UAS prototype, the high-energy laser weapon system (HELWS), that will undergo a year-long overseas field test. The Navy is also investing in the development of DEWs, with ODIN being installed on USS Dewey in 2020 and on USS Preble in 2021.

China is the second-largest C-UAS producer in terms of the number of product designs. One of the primary factors driving Chinese investment in C-UAS technology is awareness of US investment in drone technology. State-owned China Aerospace Science and Industry Corporation (CASIC) has reportedly developed a C-UAS system consisting of multiple weapons, including land-based rockets and UAS-hunting UAS that can shoot net-based projectiles, along with capabilities in development regarding vehicle-based adaptions and small-UAS detection devices.

China has also reportedly developed rifle-shaped interdiction devices, which send out jamming signals that disrupt UAV functions, resulting in either a forced

▶

landing or diversion of the intruding UAV. At Airshow China 2018, CASIC also showcased a vehicle-based laser weapon called LW-30, which can use a directional emission high-energy laser to quickly intercept aerial targets, such as photoelectric guidance equipment, UAVs, guided bombs and mortars.

DATA FROM MULTIPLE SENSORS ALLOWS THE SYSTEM TO TRIANGULATE LEGITIMATE UAS THREATS

China is also using artificial intelligence in C-UAS products, with reports surfacing that the country is already in the process of evaluating prototypes for a C-UAS platform that leverages AI to detect and destroy intruding UAVs. In China, jamming systems appear to be the most popular way to detect and counter UAVs.

Israel has continuously worked in association with the US to make progress in the C-UAS sector. The growing accessibility and affordability of sUAS systems for personal use translates into a growing threat of terrorist organisations deploying improvised drones in attacks. Additionally, adversary states in the region, including Iran, are actively expanding their drone fleets. These incentives will drive Israeli investment in C-UAS going forward to ensure that it is capable of countering drone threats of every scale. Israel unveiled an Advance UHF AESA radar system, which is designed to search, detect and track low observable aircraft, UAVs and missiles.

C-UAS systems may not always be legal. There is significant confusion and ambiguity as to the exact legal dimensions of C-UAS technology use. This is because the technology is often subject to overlapping laws that were drafted to address other technologies, long before counter-drone technology existed.

In the US, in general, whether a detection or tracking system implicates federal criminal surveillance laws, such as the Pen/Trap Statute and the Wiretap Act, depends on whether it captures, records, decodes or intercepts, in whole or in part, electronic communications transmitted to and from a UAS and/or controller and the type of communications involved. The Pen/Trap Statute criminalises the 'use' or 'installation' of a 'device' or 'process' that 'records,' 'decodes,' or 'captures' non-content dialing, routing, addressing or signalling (DRAS) information.

In the FAA Reauthorisation Act of 2018, Congress codified the term 'unmanned aircraft' as an aircraft that is operated without the possibility of direct human intervention from within or on the aircraft. Additionally, the use of spoofing interdiction may carry further penalties due to its interference with GPS signals.

There are currently limited international standards governing proper design and use of C-UASs. Given the nascent stage and rapid growth of the industry, there has been limited opportunity for international standards to emerge.

GlobalData's Counter-Drone Technologies September 2022 report authored by Harry Boneham, reveals that Raytheon Technologies, Northrop Grumman, Leidos, Leonardo and Lockheed Martin are some of the leaders in drone security space, while Droneshield, Kratos, Accipter, and STANLEY Security are some of the up-and-coming challengers. Leaders in this space are leveraging their existing experience and expertise to carve out a sizeable position in the C-UAS market. However, mirroring the proliferation and expansion of the UAS industry, several startups and smaller existing firms are starting to enter into the C-UAS market.

With the use of drones expected to increase in the coming years and with new technologies such as AI and drone swarms maturing, the counter drone technologies market is expected to proliferate ●

Pinky Hiranandani, Principal Analyst at GlobalData, has over 10 years of experience in telecom, media, and technology industry, with specific areas of expertise including drones, artificial intelligence, wearable tech, fintech, cloud computing, RPA and IoT.

Israel has worked in association with the US to make progress in the C-UAS sector

Picture credit: Israel Aerospace Industries