Counter-Unmanned Aerial Systems and Equipment

Advanced Technologies and Smart Targeting

Dr. Mahmoud Al Maharmah

Researcher and military expert, former delegate of Jordan to IMCTC

Drones, or mini/micro unmanned aerial vehicles (UAVs), are one of the most prominent weapons that terrorist organisations strive to acquire and utilise in their criminal operations. They are inexpensive, simple to operate, capable of avoiding security monitoring, precise in hitting targets, and do not eliminate the human factor. They are utilised not only for sophisticated attacks, but also for espionage, intelligence gathering, and drug trafficking, the proceeds of which are used to fund these groups.

Escalating Use

According to the Global Terrorism Index (GTI 2023) issued by the Institute for Economics and Peace (IEP), reliance on drones in terrorist attacks is growing very rapidly. The report identified 65 organizations capable of using drones in their operations, including Daesh, Boko Haram, and the Houthi group. It warned that the lack of rapid and robust measures makes these UAVs a major concern now and in future .

In the light of these indicators and the absence of a legal or ethical framework that prevents these drones from finding their way into the hands of terrorist organizations, there has been competition within military and security institutions for developing Counter-Unmanned Aerial Systems (C-UAS) that would destroy these drones, or prevent them from achieving their subversive goals, taking into account the difficulty of spotting these drones with the naked eye, and the inability of air defense radars—designed to monitor large UAVs—to detect them. However, while some old-fashioned C-UAS are effective against small drones, their high cost—compared to the low cost of UAVs—makes them a complex issue and an unsustainable solution. For example, a single Patriot missile costs about $1 million, while a small drone costs less than $500.

Regarding the countering of these UAVs, there are various technologies in use and under development, known as Counter Unmanned Aerial Systems (C-UAS). They use a

variety of sensors to detect the physical components of drones and the command centers that control them, as well as integrate and analyze data related to the detection, tracking, destruction, or mitigation of the threat. The system also allows for the development of a comprehensive perception of the magnitude of the threat posed by these UAVs, and for making the right decisions in due course .

Phases of the Drone Targeting Process

Targeting drones goes through several phases as follows:

Phase 1: Detection: It is the process in which the control center senses the presence of the drone and distinguishes between drones, commercial drones, or any other objects. C-UAS use different detection techniques to identify these drones in the airspace such as radar, radio frequency (RF) scanners, acoustic sensors, and optical sensors. Radar systems can detect drones and recognize their size, speed, and flight patterns. RF scanners monitor the radio frequencies that drones use for communications. Acoustic sensors can detect unique acoustic signatures. Optical sensors can visually detect and track them .

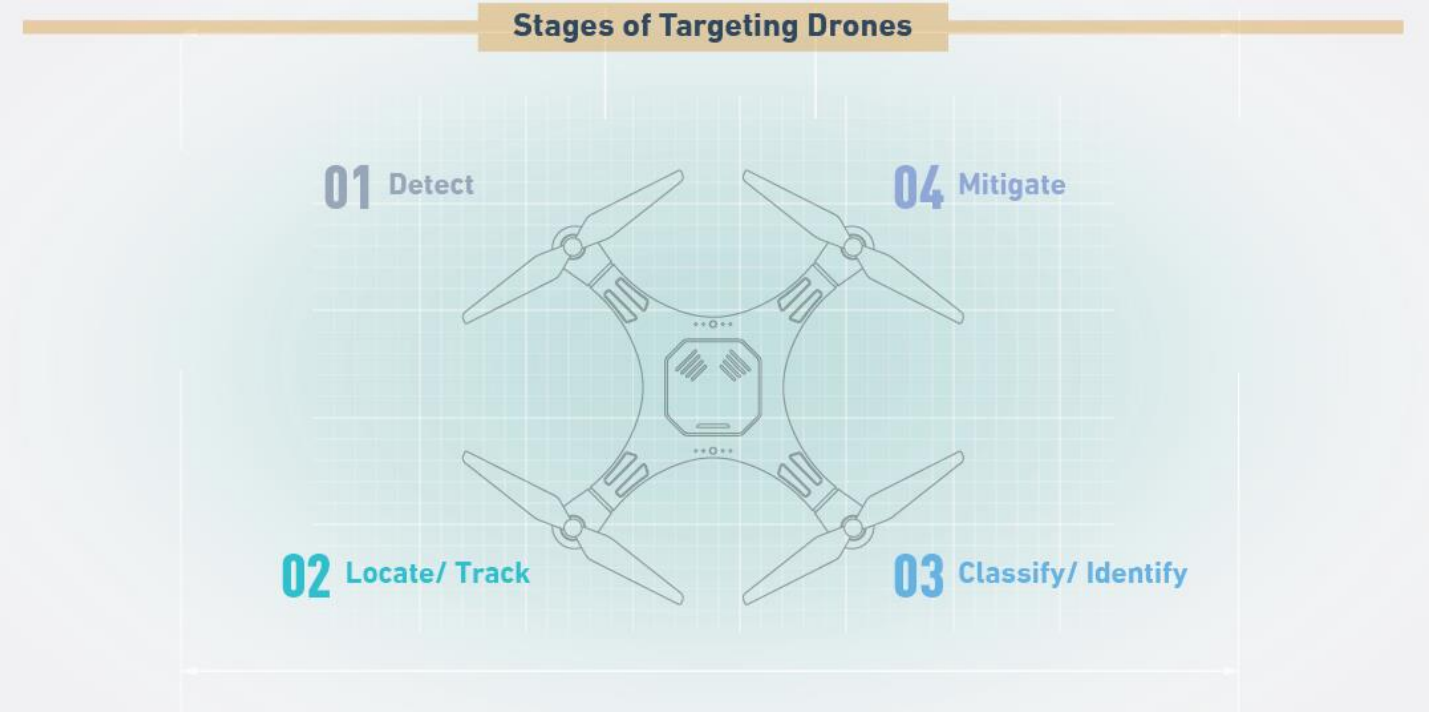
It should be noted that there is no single technology capable of detecting or tracking all types of drones under any circumstances. Electro-optical (EO) systems only operate during the day, while EO and infrared systems, as well as some RF systems, need a direct line of sight to the target, meaning that the countermeasure may no longer be able to detect and track it in certain situations.

Phase 2: Locating and Tracking: It means locating the aircraft and its trajectory at a specific time, enabling the control center to track it. Once the drone is detected, tracking systems are used to monitor its location and trajectory. These systems can use radar, cameras, or other sensors to track the aircraft's movement in real time, helping to assess the threat level and plan an appropriate response.

Phase 3: Classification and Identification: Using optical recognition, RF fingerprinting, or analysis of the aircraft's communication signals, the aircraft is classed either automatically or by the system operator, identifying its kind, operator, manufacturer, communication system, and the real IP address of the aircraft's modem. Identifying an aircraft helps determine whether it poses a threat, and whether it is being operated legally or illegally.

Phase 4: Prevention, Mitigation, or Destruction: An automatically guided interceptor drone can take off from the ground station, approach the enemy's drone, snaring it with a net. This is not necessarily the only solution to mitigate its danger. RF jamming systems can also be used, as they disrupt the drone's communications with the operator, control it, or disable it using laser grid.

The following figure illustrates the C-UAS phases, which would be a reference to understanding how different C-UAS technologies are:



Counter Systems and Equipment

There are several defense systems and equipment used to counter drones as follows:

RF Jamming Equipment: They are fixed or mobile devices, which can be carried by hand or placed on mobile vehicles, that can direct a large amount of RF energy towards the drone, disabling its control unit, and forcing one of four scenarios based on its type: (crashing it to the ground in a controlled manner, steering it regularly toward the location from which they were launched, crashing it uncontrollably on the ground, or making it fly randomly and uncontrollably). RF jamming equipment have proven highly effective in bringing down drones. They are capable of intercepting drone control

signals, hacking their software, locating them to centimeter-scale accuracy, and locating the vehicle that controls them within a radius of 10km. Then, the system generates strong interference that prevents the enemy from controlling the drone completely, thus falling to the ground, or fully controls the drone, directing it the other way to hit whoever sent it.

Spoofers: GPS spoofing devices emit false signals to the target drone to replace the communication signals that this aircraft uses to navigate, thus averting it from its true location. They can direct drones to any location by changing their programmed GPS coordinates in real time, once the spoofer gains control over the drone's GPS. However, spoofers can inadvertently disable other systems than the target aircraft, which poses a risk to civilian navigation systems. Thus, the use of these devices is limited to battlefields and is avoided in civilian operations.

High Power Microwave (HPM) Devices: HPM devices generate electromagnetic pulses (EMPs) capable of disabling electronic devices. EMPs interfere with radio links, disrupting or destroying electronic circuits in drones (as well as any other electronic device in range) due to the high voltage and currents they create. These (HPM) devices may include an antenna to focus electromagnetic pulses in a particular direction, minimizing potential collateral damage.

Electromagnetic Gun (EMG): It is a rifle that emits electromagnetic pulses that cause drones to malfunction, in the range of 4km.

Netguns: They are guns that fire nets at drones. When the net touches the aircraft, it restricts its movement by fixing its propeller blades. They are mainly used in three ways:

- Firing the net from the gun on the ground to restrict the movement of the aircraft; the gun can be carried by hand, on the shoulder, or mounted on a turret. The effective range is up to 300m.
- Firing the net from another drone. This method is used to get around the limited range of the gun .
- Firing a net attached to another friendly drone on the targeted drone .

High Energy Laser (HEL): It is a high-energy optical device that emits a light beam or a highly focused laser beam, which destroys drones by destroying their frames or electronics and control system.

Cyber Hijacking Systems: Cyber hijacking systems, or cyber removal, is a relatively new counter-drone technology. They detect RF transmissions emitted by drones and identify the drone's serial number and location using artificial intelligence (AI). If they confirm that the drone is hostile, they send a signal to penetrate, control, and direct it to a safe place.

Drone-hunting Eagles: The French military has trained birds of prey (eagles) to shoot down drones when they enter a restricted airspace. These eagles can detect drones thousands of meters away and disable or mitigate them.

Conclusion

Given the multitude of capabilities of Counter-Unmanned Aerial Systems (C-UAS), these systems cannot respond to all threats posed by such aircrafts, which necessitates the continued development of defensive technologies to win battles against drones and mitigate their danger.