Cyber takedown – the next generation of more effective counter-UAS technology

By Philip Butterworth-Hayes

A White Paper from www.unmannedairspace.info

September 2022

Cyber takedown – the next generation of more effective counter-UAS technology, Unmanned Airspace

Navigating the maze of the counter-UAS systems market

One of the biggest hurdles facing agencies responsible for counter-uncrewed air systems (UAS) (C-UAS) operations is the large and ever-expanding number of competing technologies and companies now active in the market. The *Unmanned Airspace Global Counter-UAS Directory and Buyer's Guide* (https://www.unmannedairspace.info/counter-uas-industry-directory/) lists more than 300 systems aimed at locating, identifying, classifying and then mitigating the threat of rogue UAS, or drones. Some of these systems do more or less what their proponents claim but most do not.

So how does a purchasing organisation start to understand what technology types, either alone or in partnership – and then which contractor – offer the optimal solution to its particular challenge?

The first problem is to understand the nature of that challenge and this may be far more complex than at first seems.

Both civil and military agencies face a complex series of dynamic drone threats. These range from very high-altitude military drones armed with precision strike weapons to low-level swarms of small kamikaze drones; from small, readily available commercial UAS drones equipped with a variety of deadly payloads to home-built "autonomous" systems which do not rely on GNSS or communications links but are pre-programmed. And sometimes drones that have just lost their way.

Defending agencies have to plan for a wide range of drone pilots, from the clueless, the careless and the criminal to the terrorist or hostile state-backed military forces. And every six months or so the threats change, as new drones and drone technologies enter the market.

The assets they need to protect may be static (such as an airport, a military base or a nuclear power station), dynamic (a fleet of VIPs or supply columns heading for the front line), or a one-off event.

Understanding the benefits and drawbacks of C-UAS legacy systems

The idea that any one single technology, or any one single supplier, can provide a complete solution to all these challenges is fanciful, especially as the challenges are rapidly escalating.

For very high value assets a layered approach is preferred, so several detection and mitigation assets are deployed and integrated within a single network. This layered approach offers technically the best solution, but it is usually very expensive and cannot always be easily integrated and updated. For those without deep pockets a measure of prioritisation and trade-off is therefore required, based on an understanding the realities of the drone threat they face. A template of what an ideal counter-UAS system looks like provides a high-level basis for understanding the trade-offs required.

Cyber takedown – the next generation of more effective counter-UAS technology, Unmanned Airspace

The ideal counter-UAS system…

- Provides very early detection of a possible threat, with minimal false positives, giving the defender time to analyse the threat level and begin formulating potential responses.
- Quickly identifies the exact threat (is it a recreational or commercial operator who has strayed off track or a genuine hostile threat?). Ideally, the operator should be able to define their own protection envelope areas based on the size and complexity of the defenced asset. This envelope will need to comprise an outer layer where a threat is first detected and classified and then a close-in area where mitigation measures are required.
- Can defeat a wide range of threats, some of which are not yet apparent. This means is quickly updated as new threats are detected.
- Provides a seamless route from threat identification to deploying appropriate mitigation measures.
- Reduces the probability of collateral damage to a minimum.
- Does not affect other communications systems.
- Recognises the identity of authorised drones and ensures they can perform their missions without interruption, even if and while mitigation actions are taken to resolve rogue drone threats
- Provides a recording function so the incident can be analysed for lessons learned and training.
- Is affordable
- Can be quickly and easily deployed – for both static and moving targets.
- Is reliable and robust
- Is able to be integrated into existing (and future) C-UAS networks and major command and control platforms
- Can work unsupervised, without a person in the loop, where needed
- Can address multiple threats in parallel, in cases where there are more than a single attacking/rogue drone.

Each technology type has its own strength and weaknesses and in a layered network these weaknesses can be mitigated by introducing complementary technologies. The strengths and weaknesses of each technology type are now fairly well understood, and most manufacturers are continuously working to refine their products. However, each legacy C-UAS system is limited by its basic architecture.

Anti-drone radar detection solutions work most effectively when they are correctly designed, implemented, and integrated with the security response capability of the facility being protected. Their capacity to deal with multiple simultaneous or overlapping incidents in different parts of the facility, and the effectiveness of systems classifying the threat, so that the appropriate response can be deployed in time to be of benefit are critical design considerations – Battlespace, "Counter-UAS radar systems proliferate to defeat UAVs on the battlefield:"

Cyber takedown – the next generation of more effective counter-UAS technology, Unmanned Airspace

Systems that rely on video imagery analysis as their primary detection and tracking sensor suffer from varying performance because they rely on reasonable weather conditions and visibility. Regular updates of visual drone 'fingerprint' imagery recognition data are required such that the system can keep up with the exponential increase in available drone platforms. They also struggle to detect and track drones due to environmental interference, e.g. drones crossing in front of cluttered backgrounds, or the sun, etc. -"QinetiQ Counter-Drone Technologies Evaluation report"

When a UAV is far away from the microphones…. the signal is weak compared to noise and both broad and narrowband approaches struggle to achieve reliable results. This raises a challenge for UAV detection, localization, and tracking, as observation of the acoustic signal at long range is usually highly desirable. - The Journal of the Acoustical Society of America- "Acoustic detection of unmanned aerial vehicles using biologically inspired vision processing"

Legacy C-UAS technology types, strengths and weaknesses

Detectors		
Technology type	***Strengths***	***Weaknesses***
Radar	Depending on range and software filtering capability can detect small UAS at relatively long range	Radars that are not very limited in range are expensive, can return many false positives, cannot always detect small, low-flying targets with low radar signature, especially in cluttered environments. They are also very sensitive to reflections and refractions in urban environments. Normally an active sensor can be identified by hostile forces. They normally cannot identify friend/foe and cannot detect the drone pilot.
RF detection (Directional Finder)	Very effective at detecting and identifying commercial drone signals. Passive sensor. Can also detect the remote controller.	Limited capabilities against autonomous drones or commercial drones not yet identified. Cannot track or locate. Cannot identify friend/foe.

Cyber takedown – the next generation of more effective counter-UAS technology, Unmanned Airspace

Acoustic	Good at identifying individual drone types through the rotor/propellor noise signature	Limited in range and can be confused by other acoustic signals, especially in noisy (such as urban) environments. Cannot locate or track.
Infra-red	Good at identifying individual drone types through heat signature	Limited to daylight operations and a direct line-of-sight to the target
Optical/video	Good at identifying individual drone types.	Normally requires good weather conditions and a direct line-of-sight to the target
Mitigators		
Technology type	***Strengths***	***Weaknesses***
Net capture systems	Reduces the risk of collateral damage.	Limited range; normally "one-shot" capability – if they miss, the drone escapes.
Jamming/spoofing	Relatively low cost, portable.	Will normally interfere with other nearby communication systems, and will prevent similar but friendly drones from operating
Counter-drone drones	Very precise engagements	Expensive, rely on accurate targeting, normally only capable of engaging a single target. Collateral damage likely. Extremely unreliable vis-à-vis fast flying drones.
Munitions and missiles	Currently available systems can be adapted to C-UAS operations with training	Relies on accurate targeting, with heavy risk of collateral damage. Very few civil applications. Not always effective against small drones
Directed energy	Very precise engagement	Still in its infancy. Expensive, requires high power, accurate long-range targeting and with some weather limits. Mainly a military solution,

The proliferation of small-UAS

Over the past few years commercially available small-UAS (s-UAS) have become by far the most important challenge facing civil and military counter-UAS agencies. Social media footage of the war in the Ukraine has highlighted the increasing capabilities of s-UAS by proficient operators and these capabilities are evolving all the time.

Overall, the commercial sUAS market has been moving toward smaller, lighter, and more-difficult-to-detect systems. There have also been notable increases in speed, range, and endurance and decreases in acoustic signatures. Certain sUAS models have adequate payload capacity to carry a

Cyber takedown – the next generation of more effective counter-UAS technology, Unmanned Airspace

significant amount of explosive material or illicit goods. – RAND Corporation "Small Unmanned Aerial System Adversary Capabilities"

The drone market is expanding rapidly. *Business Insider Intelligence* predicted consumer drone shipments hit 29 million in 2021. Total global shipments of enterprise drones are expected to reach 2.4 million in 2023 – increasing at a 66.8 percent compound annual growth rate.

For civil agencies, commercial sUAS are by far the largest threat. Criminal and terrorist activities – including the transport of contraband - will always be the number one challenge but in terms of workload it is the clueless and the careless operators of recreational or commercial drones which present the most persistent challenge in terms of detection and finding a C-UAS solution which matches the level of threat. As drones are legally classified as aircraft in many parts of the world they cannot be destroyed in flight.

Cyber take-down – a new way to mitigate the drone threat

Over the last few years, a new C-UAS technology, cyber take-down, has emerged as a more effective and precise method of disabling rogue drones by taking over control and landing the drone or returning it to its take-off position.

Cyber take-over systems passively detect RF transmissions, based on the protocol or frequency the drone is operating, identify the drone model serial number and the operator position via an artificial intelligence function linked to a database of known drone characteristics. If the C-UAS operator detects the drone as a threat he/she can send a signal which hacks the command and control function and directs the drone to a safe landing site.

There are many clear benefits to such a technology: it is surgically precise without causing collateral damage; it allows for continuity of service as the incident is being managed (and for authorised drone operations) ; it provides a proportionality of response; it can be configured for both mobile and static applications; it gives the C-UAS operator considerable flexibility in defining the defensive envelope; it works in urban or built-up areas; it allows for a precise analysis of incidents, which can be used for forensic reporting; it can be constantly updated to take account of new threat types.

These benefits have a particular relevance for each sector. For example, with the military and special forces, cyber-take over deals with the threat and provides layers of intelligence about the operator behind the threat. For fixed installations (sports stadia, airports, government buildings, prisons, homeland security protected assets) cyber-take over systems allow for continuity of service while the incident is being managed. For mobile applications (protection of VIPs, border control), these systems are lightweight and agile while law enforcement agencies can detect and apprehend the pilot while in operation by using the

location as retrieved from the system and use the information gathered for legal prosecutions after the threat has been eliminated without harming bystanders.

But it is also a relatively new technology and there are several misconceptions about its effectiveness.

The system will only work against readily-available commercial drones

An advanced cyber take-over system will be able to recognise home-built drones from individual components which have been commercially sourced. It will identify the drone and still be able to take over control.

The system will only work against drones with an RF communications link.

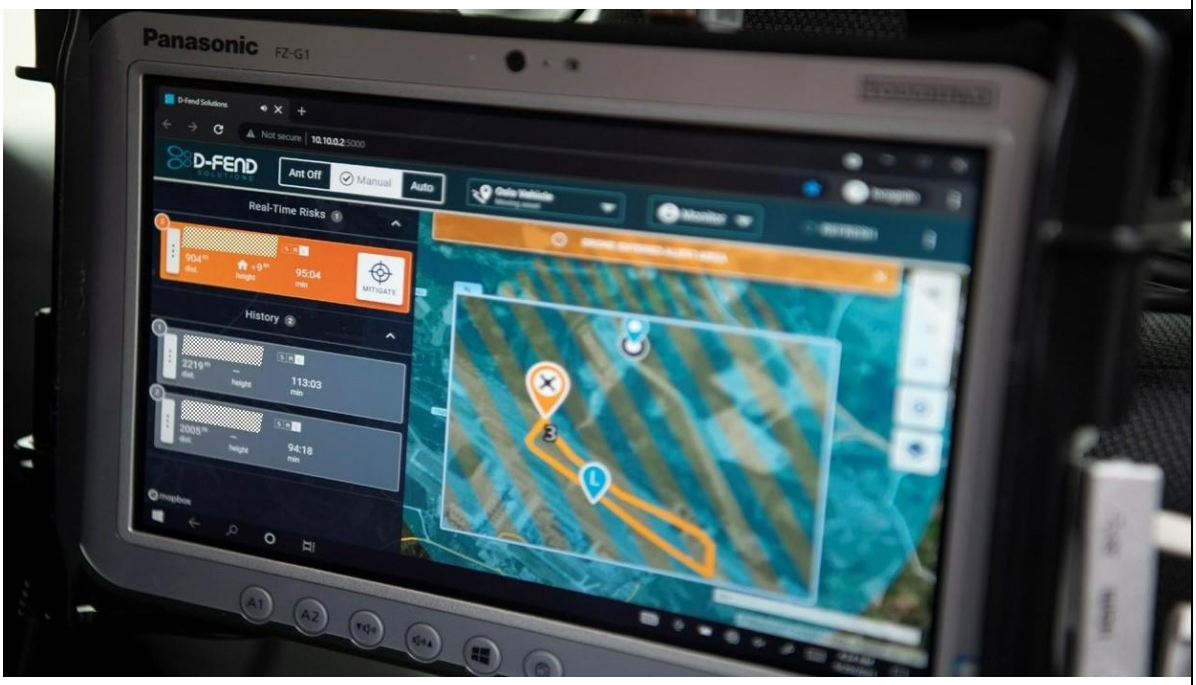
"Autonomy" is a much-misunderstood concept. Even drones flying pre-programmed paths usually transmit some telemetry data, which can be detected and overcome.

The system cannot deal with swarm attacks

With the latest cyber take-over systems (see box below) once the C-UAS operator has pressed the "mitigate" button it takes just a few seconds for the system to take control of the drone. This means that a swarm of drones can be successfully controlled sequentially. In cases where it is working in autonomous mode it will tackle the attacking drones one-by-one as they appear, thus protecting the areas against attacks.

The system relies on a database of commercial drones – if the database is not up to date it will not recognise the drone and be unable to hack it.

Cyber take-over effectiveness relies on gathering intelligence on available commercial models and components. As mentioned above, even new types rely on industry standard components which can be catalogued. It is usually only State-actor drones that use a complete set of new hardware and software components.



Cyber take-over in action: D-Fend's EnforceAir system

The D-Fend EnforceAir cyber detect/takeover system comprises a 360° perimeter security scanner using omni antennas which can be autonomously operated. The EnforceAir system can be deployed to vehicles and ships or set up as stationary deployments on low or high ground. The Multi-Sensor Command & Control system (MSC2) can manage multiple systems simultaneously and remotely from a single server, so organizations can protect large tracts of land from unauthorized drones and scale up fast, regardless of the operational requirement. It takes just a few minutes to set up, as the system automatically runs its internal Built-in Test (BIT) and calibrate. Detection and fend-off are based on detecting radio control signals, onboard data link transmitters, GNSS links and other communications. Users define the threat envelope. Once the system detects an active drone (with the exact model type or defined as a "DIY drone") it identifies the operator's location and drone type and classifies the drone as a potential threat (orange) or a "friendly" approved flight (blue/grey). The system plots its progress on a map and if the drone strays into the pre-defined action area the flight drone ticket flashes red as the system is transmitting the mitigation data signal. Once the takeover is complete the ticket turns grey, giving the operator the option to mitigate (taking over control of the drone or sending it back to its original take-off point). EnforceAir transmits a precise and short signal that takes control over the rogue drone without interfering with other drones and communication signals. This allows continuity of non-threatening operations. The fend-off and mitigation procedure normally takes a few seconds. The incident is recorded for future analysis and can be used as evidence in any legal proceedings, when allowed by regulations. EnforceAir is available in both static and mobile versions with hundreds of military and security agency deployments worldwide. This ensures there is a developing network of users who can feed back intelligence on new threats and required upgrades. The system also features an open API for integration with Command & Control systems.

Cyber takedown – the next generation of more effective counter-UAS technology, Unmanned Airspace

Conclusion

Counter-UAS is a new technology and the sector's first years of evolution have been marked by a proliferation of companies promising much but often delivering little. It is therefore easy to be cynical about the real performance levels of new technologies; the only way to validate these claims is to field test the technology against a range of threats which the specifying agency is most likely to encounter.

In preparing this whitepaper, *Unmanned Airspace* had an opportunity to attend a trial of the use of cyber-takeover systems. The trial involved detecting and mitigating threats involving a wide range of drones - both "hostile" and "approved", fixed wing and multi-rotor, commercial and non-commercial – flown by an independent operator and flown at different altitudes, speeds and courses against both mobile and static defences.

Clearly demonstrated was the speed and ease of setting up the system from out of the box into full operational mode. Threats were detected and classified at a range which gave the operator plenty of time to decide the level of threat. Drone type, serial number and operator position were identified. Mitigation was achieved with a single press of a button and in all cases the drone was effectively stopped in it tracks and either landed on the pre-selected safe landing site or returned to the pilot.

Like all C-UAS technologies there are limits to the total effectiveness of cyber-takeover. It relies on a library of known commercial drone platforms and components; State actor developed drones which fly entirely autonomous missions would not be detected or mitigated by such systems.

But in combatting the challenge of proliferating sUAS threats based on commercially available systems – currently the most important threat facing military and security agencies worldwide – cyber takeover should be considered as an important component in the process of tilting the balance of power between aggressor and defender back towards defence.

D-Fend Solutions cooperated with the development of this whitepaper.