DEFENCE TECHNOLOGY REVIEW

DTR

MAY 2025

# C-UAS

## COUNTER-DRONE PROTECTION

DRONESHIELD

SPECIAL SUPPLEMENT

# THE ART OF DRONE DEFENCE

With the drone threat continuing to evolve and seemingly omnipresent, agile and fully integrated C-UAS solutions are key.

ACROSS THE GLOBAL economy and in virtually all developed nations, unmanned aerial systems (UAS) are having an increased impact, from delivering coffee to consumers to working in agriculture. Modern warfare, too, is hardly immune from the march of the drone, with the rapidly-developing UAS sector outpacing the ability of forces to keep up with the rate of technological change.

Much of this has been spurred by the war in Ukraine, the abiding image of which has been that of the drone, filled with explosives, diving towards a Russian armoured fighting vehicle (AFV).

Like any emerging threat now dominant on the battlefield, Australia and the Australia Defence Force (ADF) are not unaffected – our reliance on a small number of high-value





***RIGHT: Ukrainian soldiers operating a small drone on the front line near the township of Bakhmut in the Donetsk region during May 2023.*** *Image: Getty Images*

platforms like ships and aircraft make us vulnerable in any future conflict. This poses a particular challenge for our procurement system and culture: the counters to the drone threat are evolving as quickly as the threat itself, so the real focus needs to be on rapidly integrating new counter-UAS (C-UAS) systems and software to prevail in future combat.

Integration – the art of bringing a variety of systems and capabilities together seamlessly and rapidly – is the key to a world-class counter-drone solution, and long a hallmark of DroneShield, a Sydney-based global leader in counter-drone technology.

## THE THREAT AND THE CATALYST OF THE UKRAINE WAR

In the early years of their battlefield employment, where large payloads and higher costs were primary characteristics, drones were used as reconnaissance and precision strike tools. Here, exquisitely-engineered but expensive, high-end platforms like those from the MQ-9 Predator and Reaper families dominated, while at the other end of the spectrum smaller hand-launched platforms could take a look over the next couple of hills. It took the fighting in Ukraine to bring on the proliferation and widespread use of small, weaponised and expendable drones as a mainstay capability by both sides by both Ukrainian and Russian forces.

The numbers of UAS/drones being used in the Ukraine-Russo war on a daily basis are staggering, with estimates putting rates of expenditure in the single-digit thousands. This should ring alarm bells for nations contemplating annual UAS orders in the hundreds.

Procurement-wise, Ukraine's Ministry of Strategic Industries last year indicated a drone production capacity of up to 3 million a year. It could be reasonably assumed that these numbers are matched by Russia. Remarkably, Ukraine was able to increase from seven to 200 drone manufacturers in a little more than a year, with an innovative partnership between fundraising channels and private industry, established outside conventional procurement channels, driving production rates and innovation.

Drones have, perhaps, become the ultimate in asymmetric weapons. Compared to the cost of a multi-million dollar armoured vehicle, a $500 kamikaze drone targeted at an open commander's hatch is a very cheap way of delivering a battlefield effect disproportionate to its unit cost. At the more expensive and sophisticated end, the Turkish-made Bayraktar TB2 drones, for instance, successfully destroyed Russian armoured columns and successfully disrupted supply lines. This prompted a change in Russian doctrine and tactics and the ability to retaliate in kind.

Drones in Ukraine, and by extension drones in future conflict, are now fulfilling a number of roles. Dr Oleksandra Molloy, in her paper Drones in Modern Warfare: Lessons Learnt from the War in Ukraine, identifies four main uses:

**1.** Precise payload delivery (dropping explosives or kamikaze attacks);

**2.** Surveillance (scouting enemy positions, co-ordinating an attack, artillery observation);

**3.** Nuisance/loitering (infrastructure disruption, using drones to jeopardise the safe operation of major facilities such as airports); and

**4.** Cyber attack/hacking (using proximity to enemy networks to hack in via drone and degrade or infiltrate the networks).

Effective counter-drone technology provides a force its freedom of manoeuvre and ability to operate in contested environments. It is now a critical component of battlefield survivability and the maintenance of the moral of troops operating in the field.

Drones enhanced through innovation across their sub-systems are delivering battlefield effects. For example, drone swarms supported by autonomous decision-making have made easier the challenge of co-ordinating the attacks of drone swarms on a single target. For example, instead of 10 individual drones controlled by 10 individual operators trying to co-ordinate an attack on a target, one operator with the right software and technology can mount a co-ordinated attack with hundreds of drones, overpowering quite sophisticated and costly air defence systems optimised for a small number of attacking aircraft.

Fibre optics, though impractical in certain scenarios, have started to play a role too. Not only does the cabling carry communications securely as it doesn't rely on traditional radio frequencies, detection demands more specific sensors such as optical systems and defeat requires tailored effectors capable of countering these profiles.

The drone war has also proved the perfect testbed both offensively and defensively for artificial intelligence (AI). Low cost and quick to respond, AI systems have been used to guide targeting, helping to pick patterns and targets out from the background and respond to their movements. For defensive tasks, AI helps defenders make sense of the enemy picture, fuse the inputs of multiple sensors into one intelligible picture and speed up response times.

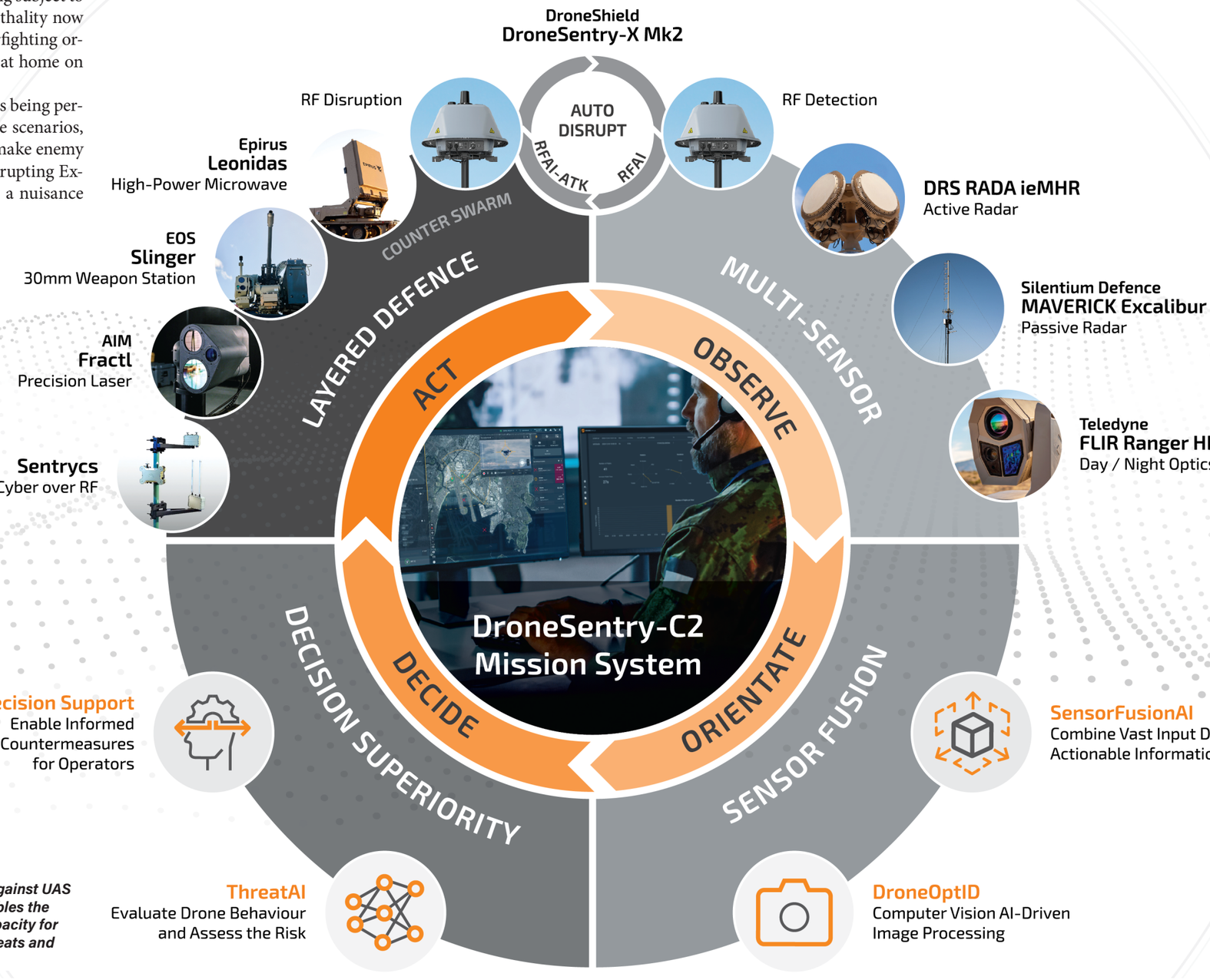
## RELEVANCE TO AUSTRALIA

Australia may be geographically remote from Ukraine, but the ADF, like all modern forces, should heed the lessons being taught and reinforced by that conflict. Given the ADF's small number of high-value platforms – think AFVs, fixed and rotary-wing aircraft, surface ships – and the vulnerability to drone attacks across a multitude of operational scenarios, the lessons are especially pertinent. It's not hard to imagine drones disrupting flight operations from the deck of HMAS Canberra as she supports operations near one of our Pacific neighbours, for example, or deployed Australian ground units being subject to drone attacks of such relentless persistence and lethality now common in Ukraine. With this, the ADF as a warfighting organisation that all elements, whether abroad still at home on base, are now drone targets.

It is also well worth noting that many of the tasks being performed by drones in Ukraine could, in alternative scenarios, fall well within the 'grey zone' of operations that make enemy action difficult to deter and attribute. A drone disrupting Exercise Talisman Sabre, for instance, could just be a nuisance or it could be conducting surveillance and reconnaissance to gauge the ADF's C-UAS capabilities. Worse case, it could well be there to conduct precise payload delivery. Even with the best available technology and threat awareness, it remains exceptionally difficult to identify the intent of a small, fast-moving drone.

The war in Afghanistan features most strongly in the collective memory of the Australian military, particularly the Army, so it is worth pause to consider how different that conflict would have been if the Taliban had widely adopted drone technology and effectively introduced armed drones – the flying improvised explosive device. Had this have been the case, defence of the forward operating bases so favoured by coalition forces would have taken on critical importance.

Australia is due to spend some AUD$5 billion on 200-odd the new Boxer combat reconnaissance vehicle fleet and another AUD$7 billion on 129 Redback infantry fighting vehicles, but has to date committed to what can only be described as seed funds on C-UAS technology. In considering the multi-million sticker price of Army's next generation of combat vehicles versus both the cost in human and operational terms of the drone threat and the low cost of C-UAS capabilities, it might reasonably be asked if this investment is sufficient going forward.




***RIGHT: As in Boyd's OODA Loop, effective defence against UAS requires a layered and integrated approach that enables the plug-and-play use of sensors and effectors and a capacity for rapid system refresh to keep pace with emerging threats and evolving technology.*** *Image: DroneShield*

***LEFT: A command and control platform that integrates both own and third-party C-UAS sensors and effectors to provide C-UAS awareness and reporting, DroneShield-C2 allows for remote access to deployed DroneShield systems to check status, configure settings, monitor threat levels and respond in real-time.*** *Image: DroneShield*

## HOW TO RESPOND?

In the realm of counter-drone warfare, relevance is dictated by the threat. With the drone threat evolving so rapidly and reliably, the form of C-UAS response taken is worth pondering. It is most definitely not about preparing for the last fight, but being ready for the next one, and being ready before it arrives. In the C-UAS space, staying still is falling behind.

In the C-UAS world, set-and-forget logic won't work in an environment laced with constant change and technical innovation and advances. Buying a large stockpile of drones to store on the shelf in the event of future conflict, for example, is unlikely to work for Australia as they would risk being obsolete within a couple of months.

Of course, the ADF is hardly alone in grappling with the drone threat, with most modern militaries facing the same challenges. The Pentagon's Strategy for Countering Unmanned Systems points to prioritising integrated, open and modular solutions. Relatedly, Dr Molloy's research, drawing on the Ukraine experience, calls for "multi-spectrum and layered combinations of both kinetic and non-kinetic countermeasures to achieve effective air defence".

Successful innovation at the speed of relevance in counter-drone warfare means bringing together the best of current technology, but more importantly in being able to integrate newer threat-relevant technology on an ongoing basis into the future. Any snapshot in time taken of UAS technology is already becoming out of date the moment it is taken.

Sovereignty is also vitally important. Australia must own and retain the knowledge, skills and software that underpin the C-UAS system so that in time of crisis it can upgrade and manage own systems and reduce reliance on other nations or providers that are likely to prioritise their own needs. To move quickly in response to threats, within hours or days at the most, Australia needs to be able to undertake upgrade and production in-house.

This defines a solution of a modular command and control (C2) system, underpinned by AI, and owned by Australia. Bolted onto this, according to the threat, are a variety of sensors that allow detection and feed into the C2 system and the operator: radio frequency, radar, optical and others. As new sensor technology is developed, it too can be integrated and add to a single, cohesive picture of the threat situation.

Engaging the threat is the last piece in the C-UAS puzzle, with a raft of soft kill and hard kill systems available based on the technology involved, environmental conditions and the operational scenario. Non-kinetic effectors including microwave directed energy weapons that fry the electronics of some threats, or kinetic effectors that use laser or conventional projectiles to destroy or defeat the enemy drone.

Importantly, this component of the C-UAS capability should ideally be manufacturer agnostic as no single solution can cover the gamut of threats and being able to integrate and use technology from multiple original equipment manufacturers will help ensure ongoing effectiveness.

## DRONESHIELD'S APPROACH TO INTEGRATION

The core of effective C-UAS capability, then, is systems integration. It's a term used across the defence sector but in few capability categories is it more pertinent that in drone warfare.

After making a start in individual anti-drone weapons back in 2014, DroneShield pivoted quickly to build integrated solutions to the drone threat. DroneShield's mission is not simply to deliver sensors and effectors, but to fuse them into an adaptive kill chain that can flex with the fight. The Australian company brings together radar, radio frequency (RF) detection, electro-optic/infra-red through AI-driven fusion engines and then adds layered soft and hard-kill effectors into a seamless operational counter-drone solution. These AI engines are underpinned by data from dozens of countries around the world, and constantly growing, to assist with intelligence around detection and mitigation edge cases.

This modular open solution integration approach is what gives end users of DroneShield solutions an edge. Whether it's dismounted forces in urban terrain, or mechanised units facing complex drone threats, the ability to tailor a counter-drone solution in real time is essential.

DroneShield's work with partners like Melbourne-based AIM Defence (refer Case Study) and its commitment to open systems architecture design ensures that new capabilities – whether sovereign or allied – can be brought online fast. This means a solution that will evolve with customer needs and relevance to the threat. A solution that doesn't trap the user in a single-vendor locked ecosystem or require years to reconfigure when the threat changes.

DroneShield has developed several principles for systems integration that underpin its approach to C-UAS. These are:

**Designed from the outset:** DroneShield designs its counter-drone solutions with integration in mind from the first sketch. Its code is flexible and utilises modular open systems architecture, making it easy for new systems from other manufacturers to be able to 'talk' to its system and operate together. In acknowledging that no one company possesses the answer to detecting or responding to every threat, effective systems integration has become ingrained in DroneShield's culture and way of doing business.

**Rapid testing and prototyping:** DroneShield is focussed on keeping up to date, bringing in and testing new systems and rolling out updates. Its design and production processes are rapid and iterative. Its own private test range in Australia lets it take real-world data and test the response to make sure it is effective and integrates smoothly. Its software team is based locally in Sydney and can pivot quickly to Australian priorities.

**Sovereign ownership:** DroneShield does all software development in-house, mostly in its Sydney facility. It is vertically integrated, designed, developed and has full control over its IP so it can respond quickly to the priorities that matter to the ADF and Australia. Its products are Australian-made and do not fall within the auspices of foreign regulations such as ITAR. This gives DroneShield the ultimate ability to optimise its support for the Australian war fighter.

## SUPPORTING RAPID DECISION MAKING

In any aspect of warfare, how quickly a force moves through the OODA (observe, orient, decide, act) loop will have a decisive impact on its success in battle. After his experience in the Korean War, fighter pilot Colonel John Boyd identified that as one pilot was able to determine what was happening, decide what to do and start doing it more rapidly, they quickly gained the upper hand on an opponent who was making increasingly irrelevant decisions, based on older information and executing them slowly.

Drone warfare, played out on a daily basis in Ukraine, is fast-moving, hard to predict and often conducted over short ranges, with air vehicles supporting the activity of ground troops or conducting their own strategic offensive and defensive tasks.

A key part of C-UAS operations is helping a human operator move quickly through the decision-making cycle and arrive at decisions based on a clear and integrated picture of the drone threat. AI has great potential to support each stage of the OODA loop, help a human operator make sense of fast-moving activity and support their decision making and execution.

***The DroneShield-X Mk2 Expeditionary Fixed Site Kit in the field.*** *Image: DroneShield*

## CASE STUDY: INTEGRATING AIM DEFENCE'S FRACTL SYSTEM

**Different threats,** in different contexts, need different responses. For a simple radio frequency drone, often the best defence is just to block that signal and the drone will crash to earth or return to its start point. Sometimes that isn't enough: a drone operating more like a missile on a crash course with its target, for example, or one receiving guidance through a fibre-optic cable might need a hard-kill response. Guns and other conventional weapons can often be challenging in this context – collateral damage, cost, range and speed of engagement are all often sub-optimal for the drone threat, but directed energy weapons offer a number of advantages.

DroneShield has been working with AIM Defence, an Australian company making the Fractl tactical directed energy platform. The system directs a focussed laser beam at the target, destroying the guidance and other electronic systems and sending the drone spiralling to the ground. With the power to burn through steel and ability to track small UAS travelling at 100km/h from a kilometre away, it is one of the most capable platforms of its type, and proudly developed in Australia.

The integration process is essentially one of getting the Fractl to 'talk' to DroneShield's C2 system to enable targeting information from a range of sensors and firing commands to be transmitted to the laser system. An Application Programming Interface is developed that translates the different 'languages' and lets them communicate seamlessly.

***The Fractl tactical directed energy system.*** *Image: AIM Defence*

It's worth noting that integration, too, isn't a set-and-forget task. AIM Defence continues to evolve its Fractl system in response to threats, much like DroneShield evolves its own systems. Ongoing integration is essential to maximising the combined effectiveness of both systems as technology advances.

## THE DRONESHIELD STORY

**DroneShield was founded** in 2014, prompted by the then nascent drone threat and started with its iconic DroneGun. Now in its fourth iteration, DroneGun is a handheld system that uses a burst of RF signals to disrupt the drone's guidance and send it to the ground or back to the operator. Building on this success, in 2019 DroneShield's RfPatrol detector was delivered, now in service in Ukraine, as a handheld detector of drone guidance signals. Seeking to develop an integrated solution to the drone threat, it then released the DroneSentry-C2, which provides counter-drone awareness and reporting, while integrating multiple sensors and effectors.

DroneShield's team of more than 200 engineers located in Sydney continue to develop the company's technology, drawing on real-world feedback and insights from the users of more than 1,000 systems deployed in Ukraine. This resource it uses to stay at the cutting edge. The team works with entities in more than 70 countries. As a pure-play counter-drone company, it is fully focussed on the global demand for solutions to the drone threat.

In 2024, 91% of DroneShield's revenue was derived from export sales, meaning that for every dollar invested in Australia, around nine dollars are returned through international exports.

DroneShield is an Australian company, and proud to be a unique sovereign capability for our nation.

*RfPatrol Mk2 passive non-emitting, wearable UAS detection device.*

DroneShield's SensorFusionAI and ThreatAI does just this, bringing together information from a variety of sensors into a single integrated picture, proposing a response for human approval if needed, or executing an automated response if so enabled. To detect threats, it does not rely on a long list of individual drone protocols that would need to be kept up to date – along the lines of if you see X it is an ABC drone and the correct response is Y. Instead, DroneShield's AI has been trained over many years on a variety of systems and platforms to enable detection of threats that are brand new and unseen. The AI extrapolates based on what has been detected and what it has seen before to select and trial a response, even shifting quickly if that does not prove effective.

Increasingly, offensive drones are using AI for guidance and targeting, taking the human out of the loop for the final phase of the attack. This means there are no signals that can be targeted to defeat the drone and requiring a fast kinetic response. DroneShield's platform, with an automated response enabled, means the fastest possible decision making and responses can be implemented.

## CONCLUSION

Whilst the nature of combat is enduring, the way warfare is conducted and the tools of trade are changing rapidly, as ever more capable and numerous drones have an impact on the battlefield in Ukraine and are quickly being brought online with major militaries around the world.

What's happening in Ukraine is being watched closely by forces intent on remaining at the leading edge of land warfare capability. Drones are currently and will continue to be disruptive weapons in any future conflict, high or low intensity, whether against a near-peer enemy or insurgent actors. Australia will not be immune to this evolution in military affairs and is making moves to address the drone threat through projects such as LAND 156.

The nature of the threat dictates the nature of the response, and as the threat changes so must the response be capable of shape-shifting to keep up. This demands an integrated response, where a central C2 system underpinned by the fast decision-making support of AI, can bring together a variety of sensors and effectors to engage current threats and those that are yet to come. A successful counter-drone solution is not just one product, or one system, it's a number of them, changing over time and seamlessly working in concert.

As an integrator first and foremost, DroneShield is interconnected, modular and agile. As a sovereign Australian capability, DroneShield owns its technology and exports it around the world. It is Australia's pre-eminent and world-leading counter-drone systems integrator, because that's what the future demands. DTR

DEFENCE TECHNOLOGY REVIEW

THIS SPECIAL SUPPLEMENT IS PUBLISHED BY SABOT MEDIA PTY LTD

**Editor: Ian Bostock**
ibostock@dtrmagazine.com
subscriptions@dtrmagazine.com
advertising@dtrmagazine.com
Tel: + 61 419 204 835