DEFENCE TECHNOLOGY REVIEW

DTR

MAR 2025

BUSHMASTER

COUNTER UAS

SPECIAL SUPPLEMENT

BUSHMASTER LOOKS TO THE SKY

A collaborative effort sees the venerable Bushmaster platform take on the drone threat.

THALES AUSTRALIA, IN partnership with Dedrone by Axon, has successfully tested a modified Bushmaster protected mobility vehicle (PMV) in the counter-uncrewed aerial system (C-UAS) role.

The effort has seen the successful integration of Dedrone C-UAS technology into the Bushmaster PMV – adding another battlefield capability to the evolving Bushmaster vehicle.

The Bushmaster C-UAS testing was undertaken near Thales Australia's Bendigo facility in Victoria, and involved simulated battlefield conditions replicating those common to a current European theatre. The tests, Thales Australia told *DTR*, were effective in repelling drone attacks from the moving vehicle.

"We've watched the changes in modern warfare in Ukraine, taken the lessons learned there, and built them into the Australian Bushmaster," Jeff Connolly, Thales Australia and New Zealand chief executive officer said. "It means we are ensuring the iconic vehicle is fit for purpose for both current and future conflicts – a modern vehicle with advanced capabilities.

"The successful testing of Dedrone's counter-drone capabilities while in motion is a game-changer for the Bushmaster and those forces who use it. In dynamic and unpredictable combat environments, the ability to defend against drone threats offers a clear tactical advantage. We're excited to partner together with Dedrone by Axon to bring this important innovation to the battlefield."

The addition of a C-UAS capability further enhances the Bushmaster's versatility and is part of a suite of upgrades already completed, underway or planned for the combat-proven Bushmaster platform, which has seen an ongoing evolution of the baseline design to improve protection, habitability, performance, capacity and payload. Other improvements which will evolve the Bushmaster include a digital dashboard, crew access side doors and a cold weather start kit. A hybrid electric drive version is also in planning.

More than 1,300 Bushmasters have been produced to date, with these in service across eight user nations outside Australia, including the UK, New Zealand, the Netherlands, Japan and Ukraine. Dedrone C-UAS technology is equally as proven and in use in 33 countries across 926 sites, including 53 airports and 64 stadiums, 17 US federal entities and 30 non-US governments. A global leader in C-UAS technology, its C-UAS solutions include the proven DedroneTracker.AI command and control (C2) software.

The partnership combines Thales' and Dedrone by Axon's respective core competencies into a vehicle-mounted C-UAS system able to detect, track, identify and mitigate (DTI-M) Groups 1-3 UAS.

Aaditya Devarakonda, CEO of Dedrone by Axon, said that the integration of the group's mobile C-UAS technology on the Bushmaster provides warfighters with the ability to manoeuvre "while having increased situational awareness and mitigation capabilities against the asymmetric threat of small UAS".

The Thales-Dedrone by Axon team will continue to mature the Bushmaster C-UAS capability.

Conception and development of the Bushmaster C-UAS variant is set against today's rapidly evolving battlefield; an operational environment where UAS are becoming increasingly dominant and pervasive to the extent where their presence is reshaping offensive and defensive strategies.

As the reliance on these platforms as battlefield tools grows, so too does the complexity and importance of countering them. Together with Dedrone by Axon, Thales Australia is developing what it believes to be the most comprehensive, flexible and effective C-UAS solution on the market. The Protected Vehicle team at Thales Australia is dedicated to identifying and understanding the threats posed by UAS and actively developing and delivering innovative solutions to mitigate these dangers.

This combined approach is comprehensive, combining traditional fieldcraft and vehicle craft with cutting-edge technology to ensure that end users are equipped to operate effectively in a world where UAS threats are ever-present and continually evolving.

The following will examine the dynamic nature of UAS challenges, exploring how foundational fieldcraft techniques can be combined with C-UAS full kill-chain solutions to neutralise threats posed by malicious UAS.

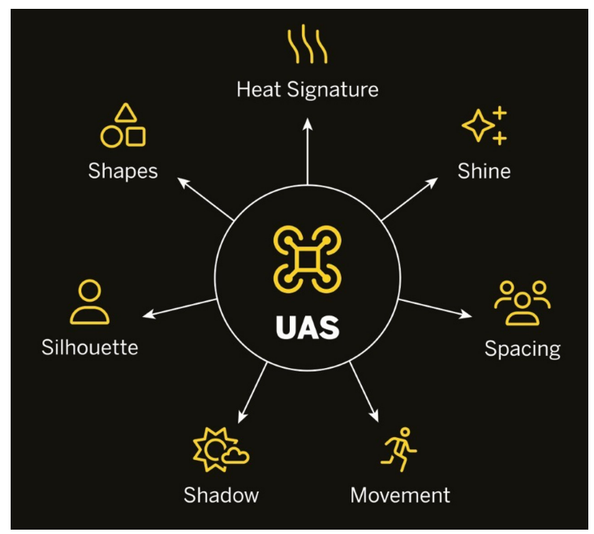
WHY THINGS ARE SEEN: 7 KEY FACTORS

In modern theatres of war, staying hidden from aerial threats – especially small drones – has become an absolute necessity. Drones have fundamentally altered the tactical surveillance game, making it imperative to minimise detectability. Remaining unseen and undetected is crucial for survival, and seven primary factors influence a platform's or individual's visibility to drone systems:

1.Shape: A drone's sensors can easily spot the distinct outlines of personnel or vehicles. Blending with the natural features of the environment enables distortion or masking of recognisable shapes, making detection by drone sensors more difficult;

2.Silhouette: A large silhouette is highly visible, particularly against a bright or contrasting background. Staying low, using the landscape to obscure outlines and avoiding ridgelines are crucial to reducing exposure;

3.Shadow: Shadows betray location, particularly in open areas. Being conscious of the sun's position and using natural cover can help mitigate the risk of shadows revealing an asset's or soldier's location;



ABOVE: Depiction of a Bushmaster PMV performing C-UAS activities. *Image: Thales*

RIGHT: Addressing the various components involved in drone detection of targets will become increasingly important in survivability on the modern battlefield. *Image: Dedrone*

4.Shine: Reflective surfaces like metal, glass or glossy gear can catch the eye of drone operators. Ensuring that equipment and vehicles have matt finishes, covering windscreens and windows and avoiding unnecessary shine dramatically reduces the chances of detection;

5.Spacing: Personnel or vehicles grouped closely together present an obvious point of interest for aerial surveillance and targeting. Maintaining appropriate spacing between assets enhances operational flexibility and makes it more difficult for drones to identify formations;

6.Movement: Various drone payloads, such as radar, electro-optical and infra-red (EO/IR) cameras and LiDAR, can quickly detect erratic or rapid movement. Moving slowly and deliberately, while using the terrain to conceal movement helps avoid drawing unwanted attention; and

7. Heat signature: Heat signature detected by drones identifies IR radiation emitted by objects. This enables detection of people, vehicles and equipment, even in darkness, under camouflage or amongst dense terrain. To counter drone heat detection on operations, use thermal blankets, decoys and active cooling to shield emissions. Operate near heat-masking environments (masonry or concrete structures), deploy smoke screens and limit movement during cooler periods of the day. Further, employ C-UAS systems to jam sensors and use terrain for concealment to minimise detection risks.

Drones frequently monitor known supply routes in search of signs of deviation or off-road movement. Tactical use of fighting positions and shielding a vehicle's vulnerable areas reduces exposure to drone sensors. Leveraging natural cover, such as treelines or terrain features, can dramatically reduce the likelihood of being observed and targeted from the air.

LEVERAGING VEHICLE CRAFT AND INNOVATION TO COUNTER THE UAS THREAT

While traditional vehicle craft and fieldcraft are indispensable on the battlefield, these alone are not a panacea for the challenges posed by UAS. Success in countering UAS threats requires a balance between craft and technology innovation. The proliferation of UAS technology across commercial, public safety and military domains has introduced new risks and challenges, spurring a growing demand for comprehensive C-UAS technology. In broad terms, the C-UAS mission can be broken down into four distinct phases, each of which requires special attention:

1.Detect: C-UAS systems alert the operator to the presence of a drone in the protected airspace. These detection systems can take on many form-factors and can be installed as a fixed-site system or be portable, depending on the needs of the operator. Various types of sensors can be used to create a layered detection system, including passive radio frequency (RF), radar, EO/IR cameras and acoustics. The multi-sensor approach enables the operator to detect the widest range of drones, from those that emit RF signals, to ones that are piloted autonomously by waypoints, or tethered to a fibreoptic cable. A combination of detection sensors also allows an operator to detect drones that are intentionally 'spoofing' their location, a tactic in which a drone and/or pilot intentionally reports a false location within its communication signal. By using a combination of sensors, the system can deliver true airspace situational awareness and provide a common operating picture. Critical to the success of this multi-sensor approach is the sensor fusion algorithm that enables the system to virtually eliminate false positives while identifying and locating the drone with accuracy. Mounted on a platform like the Bushmaster, these systems gain mobility, allowing detection to extend across operational boundaries;

2.Track: Once a drone is detected, an effective counter-drone solution tracks the location and path of the drone as well as the location of the pilot, providing real-time airspace situational awareness to the operator;

3.Identify: Identification occurs on two important axes: identification of friend or foe, and identification of specific drone and/or drone model;

a. Dedrone's C2 software solution, DedroneTracker.AI, must first determine whether the detected drone is friend or foe;

b. The C-UAS solution can then identify the drone model. The identification can include unique identifiers such as drone serial number or media access control (MAC) address. This gives the operator valuable information about the capabilities of the drone including payload, range and speed, as well as how to potentially mitigate the drone and the threat it may pose.

The Bushmaster's scalable electronic architecture enables seamless integration of software like DedroneTracker.AI, allowing operators to manage threat identification even in austere conditions.

Furthermore, its onboard communications infrastructure can rapidly relay identification data to command elements for improved decision-making.

4.Mitigate: C-UAS mitigation solutions generally fall into two broad categories: kinetic and non-kinetic, each with distinct advantages and disadvantages. The ideal mitigation solution will depend largely on the specific customer, site requirements and the tactical situation, and may consist of a combination of both kinetic and non-kinetic methods.

Kinetic Methods: Kinetic solutions focus on physically neutralising or destroying UAS targets. Kinetic methods can be extremely effective at countering a wide range of aerial threats and often have a definitive result. These systems may, however, come with logistical challenges, such as ammunition or specialised equipment or unmasking the tactical position and/or collateral damage. Examples of kinetic methods include:

RIGHT: The Bushmaster's scalable electronic architecture and communications capability supports seamless integration of software such as the DedroneTracker.AI C2 software system for the management of threat identification in austere environments and the rapid relay of identification data to command elements.
Image: Thales

BUSHMASTER C-UAS

a. Missiles and Ammunition: Conventional weaponry can be highly effective, particularly in military contexts where the overarching priority is neutralising threats quickly. However, the risk of collateral damage may be a concern, especially in urban environments or populated areas where civilian infrastructure is present. One significant downside to using missiles as a C-UAS mitigation tool is that the effector often costs more than the threat being mitigated, eventually leading to losing a war of attrition due to economic factors. Conventional small arms ammunition natures often do not have a long enough range to counter drone threats from an acceptable stand-off.

b. Nets and Takedown Devices: These non-explosive methods provide a safer, more controlled alternative to traditional weapons. Nets physically capture drones, rendering them harmless without causing destruction. Although this approach is not effective against a drone swarm, it may prove valuable in civilian or sensitive environments where minimising collateral damage is a priority. Takedown devices and nets also can provide the opportunity to capture an enemy drone for forensic analysis and/or hardware exploitation.

Non-Kinetic Methods: Non-kinetic approaches, by contrast, focus on disrupting a drone's operations without kinetic energy or physical interference. The complexity of these systems means they must be regularly refined and updated to remain effective against emerging and evolving UAS capabilities. Methods include:

i. Electronic Warfare (EW): RF jammers interfere with the communications link between the drone and the control station. By severing the transmission link, RF jammers can cause the drone to enter a 'lost link' protocol, which often leads to the drone safely returning to and landing at the take-off location. Jammers work on all RF-controlled drones and are an effective means of counter drone swarms. EW may also include the jamming of GPS navigation signals, which results in the aircraft not knowing where it is in space;

ii. Cyber Takeover: Cyber takeover is a mitigation measure that takes control of the drone by impersonating the control station. It is done by hacking into the drone and tricking the drone to switch away from the legitimate controller. Cyber takeover lets the mitigator direct the flight of the drone and access the drone's data and camera, an elegant way to mitigate a drone when it works. The success rate of cyber takeover is, however, often quite low for two reasons: the mitigating controller must be able to predict the frequency hopping of the drone and always maintain a more powerful signal to the drone than the original remote. Additionally, cyber takeover mitigation relies on exploits which can be patched once discovered and does not work well against a drone swarm; and

iii. Directed Energy: Directed energy weapons such as high-energy lasers (HEL) and high-power microwaves (HPM) provide a low collateral damage, non-kinetic option for engaging threat drones. A HEL concentrates a large amount of directed energy into a small surface area through a line of sight 'beam', heating up said area to extremely high temperatures, burning or destroying the target. While HELs generally have high up-front costs and require the parent platform to possess sufficient power supply, the very low per shot cost makes them attractive C-UAS options. A HPM sends out a blast of directed energy which can be used to 'fry' electronics. The main benefit of HPMs is that they can be effective tools against UAS swarms, but they are unable to engage targets at longer stand-off ranges.

Mounting solutions on a Bushmaster enhances deployment flexibility while leveraging the platform's robustness for precision execution. The Bushmaster's unique combination of protection, mobility and modularity makes it an invaluable

C-UAS EFFICACY

To be effective in the C-UAS role, the operator must have an effective tool to manage the DTI-M C-UAS cycle. The DedroneTracker.AI C2 software solution serves as a single-pane-of-glass user interface and allows the operator to monitor and control all parts of the DTI-M process. Leveraging advanced artificial intelligence/machine learning (AI/ML), the platform incorporates advanced proprietary algorithms and ML techniques to ingest and fuse multiple sensor inputs from RF, EO/IR camera and radar sources.

Sensor fusion, which is built directly into DedroneTracker.AI, plays a critical role in the automatic cueing of mitigation systems, either through 'man-on-the-loop' or 'man-in-the-loop' controls. For example, some drones emit RF signals while others can operate tethered to a fibre-optic cable or programmed via waypoints. By using a combination of sensors, the operator can gain a clearer picture of the situation, which will inform the type of mitigations employed in theatre over time. DedroneTracker.AI uses these sensor inputs to provide accurate and real-time DTI and then provides the necessary interface for the user to engage a UAS threat with the best-fit mitigation method from a range of mitigation options.

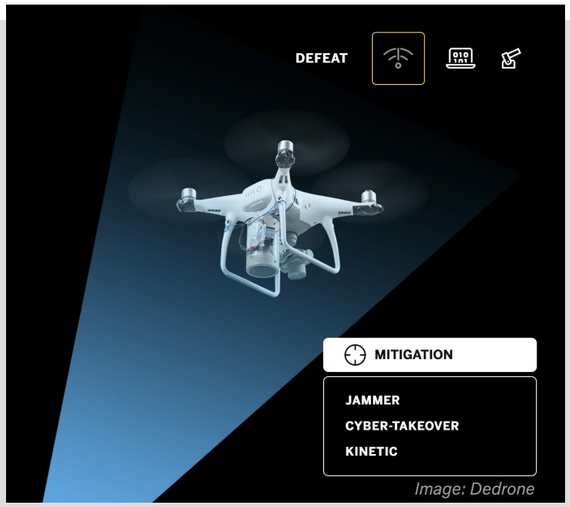


Image: Dedrone

asset in C-UAS operations. By bridging traditional vehicle craft with cutting-edge technological innovation, operators are best placed to detect, track, identify and mitigate UAS threats in an increasingly complex battlespace.

DEPLOYING C-UAS

C-UAS systems can be deployed through various means depending on mission requirements and operational challenges. Each has its unique advantages, ensuring tailored protection against the evolving drone landscape. Examples of available form-factors include, but are not limited to:

- **Fixed-Site:** Hardware deployments are permanent or semi-permanent installations designed to protect critical infrastructure locations such as airports or military bases by providing a comprehensive defence against drone incursions. These set-ups typically incorporate an array of sensors and response mechanisms for long-term security;
- **Expeditionary Kits:** These offer a portable and rapidly deployable solution in remote or temporary locations where immediate drone threats may arise. These kits are ideal for tactical missions requiring flexibility and quick set-up.
- **On-the-Move (OTM):** Portable, vehicle-mounted solutions, such as that developed using the Bushmaster PMV, are integral for dynamic environments where mobility is crucial. These systems are mounted on vehicles and enable forces to maintain a protective umbrella against UAS threats. OTM C-UAS is critical to maintaining tactical manoeuvre capability, without which combat formations can become bogged down into more static forms of warfare as currently seen in Ukraine.

A LAYERED APPROACH TO C-UAS

When it comes to addressing UAS threats, there is no one-size-fits-all solution. The complexity, variety and adaptability of drone technology combined with the risk assessment of a specific situation requires a layered C-UAS approach. Relying solely on any single method often leaves critical gaps for adversaries to exploit.

A layered C-UAS strategy requires combining fieldcraft and multiple layers of C-UAS DTI-M measures into a unified strategy. Each element contributes to a more robust defence against UAS threats. Fieldcraft, rooted in traditional skills like camouflage and concealment, offers tactical advantages by allowing forces to avoid detection or engage in evasive manoeuvres. Fieldcraft must then be augmented with a comprehensive C-UAS system that leverages multiple types of DTI-M technology that includes various detection and tracking sensors (RF, radar, camera, acoustics) and both kinetic and non-kinetic mitigation methods.

By integrating these approaches, it is possible to create a solution that can adapt to a wide range of scenarios. In certain situations, non-kinetic methods may neutralise threats without kinetic engagement, while fieldcraft techniques may allow forces to evade detection entirely in others. The key is that no single component stands alone; instead, they reinforce and complement one another, creating a layered defence that is flexible, adaptive and difficult for adversaries to circumvent. This approach ensures that the operator is not merely reacting to UAS threats but actively anticipating and then proactively defending against them.

BELOW: Drones, particularly small to medium in size, will become an increasingly pervasive threat to deployed forces.

ABOVE: Successful testing of a Dedrone C-UAS suite integrated on a Bushmaster PMV took place in Victoria recently. *Images: Thales*

The Thales Australia and Dedrone C-UAS variant of the Bushmaster aligns with the knowledge that effective defence against battlefield drones lies in a layered, adaptive approach to capability development that combines fieldcraft and vehicle expertise, cutting-edge technology and operational innovation.

WHAT DOES THE FUTURE HOLD?

Emerging technologies are rapidly advancing in the fight against UAS threats, with several key innovations poised to transform the landscape. These include directed energy weapons, AI/ML enabled technology, swarm defence and quantum sensor technologies, hypersonic missile interceptors, smart jamming systems and augmented reality.

To meet the challenges of countering the UAS threat Thales Australia and Dedrone by Axon are committed to fostering a think tank-like culture – bringing together the 'smartest people in the room' to continuously refine, adapt and enhance our collective C-UAS strategies. By leveraging the diverse perspectives and deep expertise across both companies, an enhanced understanding of the full spectrum of UAS threats and the best solutions to meet those threats can be built. The pairing aims, a spokesperson told *DTR*, to empower end users with the means to survive in operational environments where the UAS threat is constant, complex and evolving. DTR

BELOW: Conception and development of the Bushmaster C-UAS variant is set against a rapidly evolving battlefield where the drone threat is becoming increasingly pervasive. *Images: Dedrone*

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

Thales Australia: Delivering cutting-edge capability for a future ready defence force.

thalesgroup.com/australia

THALES
Building a future we can all trust