THALES
Building a future we can all trust

Countering UAS Threats Whitepaper

Safeguarding against emerging threats

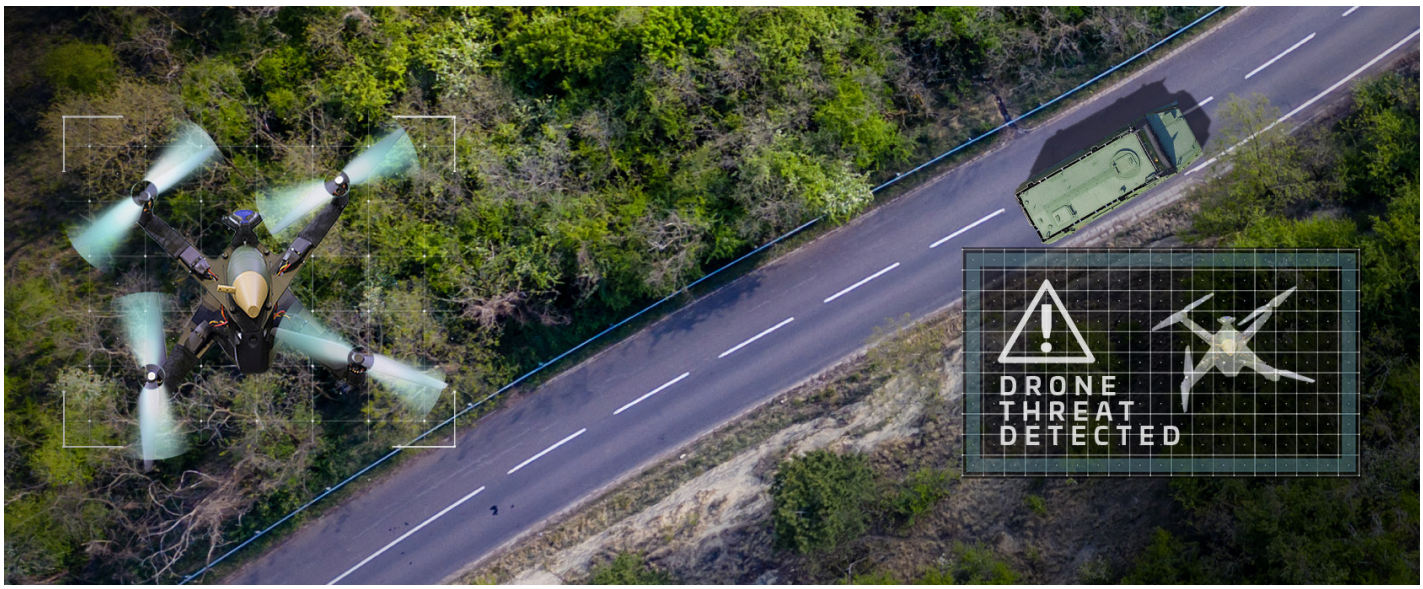
Dedrone by AXON

Introduction to C-UAS:
Safeguarding Against Emerging Threats Whitepaper

In today's rapidly evolving battlefield, Uncrewed Aerial Systems (UAS) are becoming increasingly dominant, reshaping offensive and defensive strategies. As the reliance on these platforms grows, so too does the complexity and importance of countering them. Thales Australia is proud to partner with Dedrone by Axon to develop and field the most comprehensive, flexible and effective counter-UAS (C-UAS) solutions on the market. At Thales Australia, the Protective Vehicle (PRV) team is dedicated to identifying and understanding the threats posed by UAS and actively developing and delivering innovative solutions to mitigate these dangers. Dedrone by Axon is the global leader in C-UAS technology with battle-tested, dual-use solutions.

Hundreds of commercial, public safety and military customers around the world rely on Dedrone by Axon's C-UAS solutions, including their award-winning command and control (C2) software, DedroneTracker.AI. Our combined approach is comprehensive, combining traditional fieldcraft with cutting-edge technology to ensure that our customers are equipped to operate effectively in a world where UAS threats are ever-present and continually evolving. This article examines 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.

At Thales and Dedrone by Axon, we aim to foster collaboration, deepening our understanding of UAS vulnerabilities while empowering our customers to adapt, innovate, and thrive in this new warfare landscape. *For the purposes of this paper, the term "drones" and "UAS" will be used interchangeably and are intended to mean the same thing.*

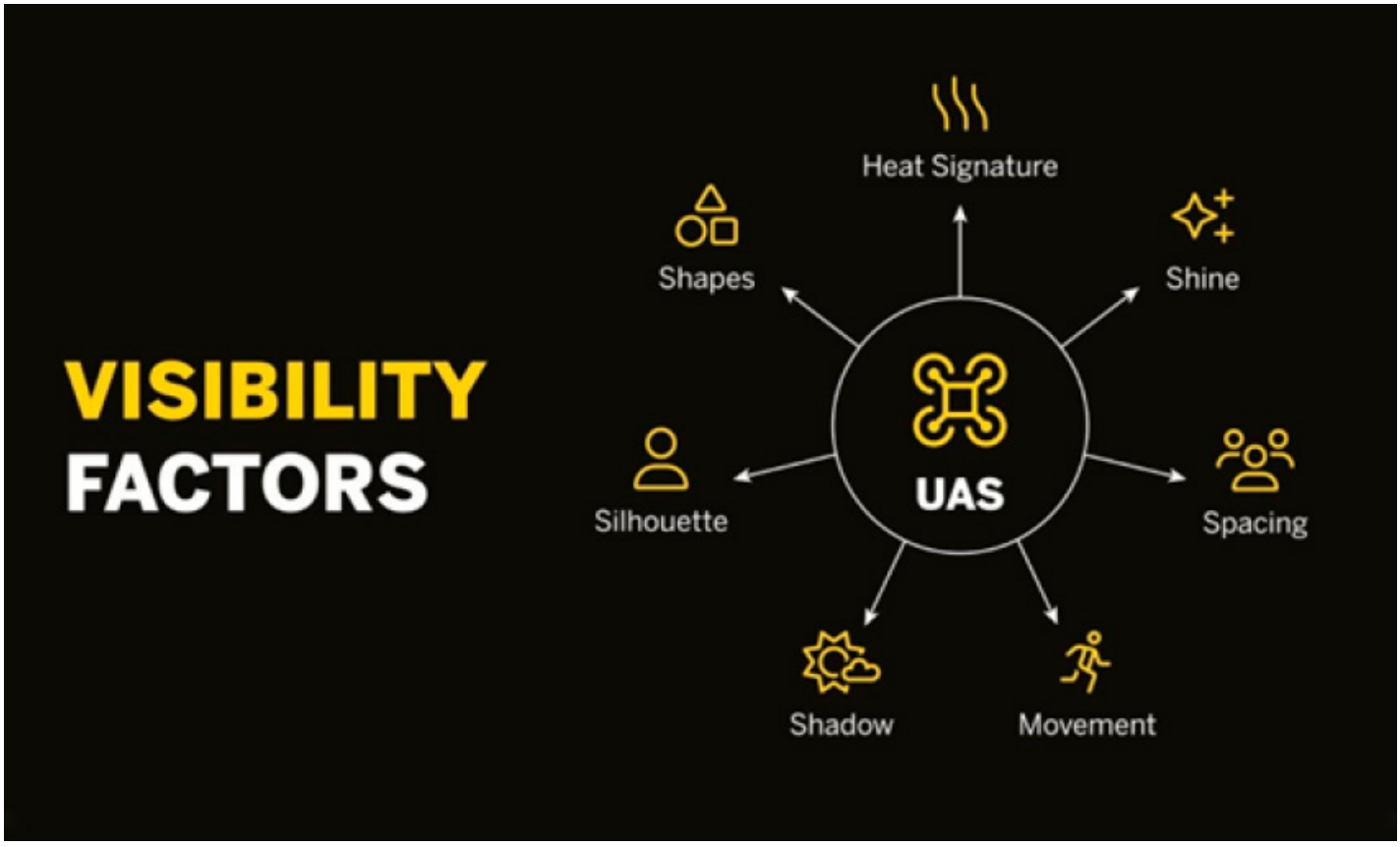


Understanding Why Things are Seen: Seven Key Factors

In the modern theatre of war, staying hidden from aerial threats- especially small drones - has become a vital skill. Drones have fundamentally altered the surveillance game, making it imperative to minimise detectability. Remaining unseen and undetected is crucial for survival, and seven primary factors influence your visibility to drone systems: **shape, silhouette, shadow, shine, spacing, movement and heat signature**.

1. **Shape:** A drone's sensors can easily spot the distinct outlines of personnel or vehicles. By blending with the natural features of the environment, you can distort or mask recognisable shapes, making it harder for drones to detect you.
2. **Silhouette:** An unmistakable silhouette is highly visible, particularly against a bright backdrop. Staying low, using the landscape to obscure your outline, and avoiding ridgelines are crucial to reducing exposure.
3. **Shadow:** Shadows betray your location, particularly in open areas. Being conscious of the sun's position and using a natural cover can help mitigate the risk of shadows revealing your location.
4. **Shine:** Reflective surfaces like metal, glass or glossy gear can catch the eye of drone operators. Ensuring that equipment has matte finishes and avoiding unnecessary shine dramatically reduces the chances of detection.
5. **Spacing:** Personnel or vehicles grouped closely together present an obvious target for aerial surveillance. Maintaining appropriate spacing between assets enhances operational flexibility and makes it more difficult for drones to identify large, clustered formations.
6. **Movement:** Various drone payloads, such as radar, electro-optical and infrared (EO/IR) cameras, and LiDAR, can quickly detect erratic or fast movements. Moving slowly and deliberately, while using the terrain to conceal movement helps avoid drawing unwanted attention.
7. **Heat signature:** Heat signature detected by drones, identifies infrared radiation emitted by objects. This enables detection of people, vehicles, or equipment, even in darkness, camouflage, or dense terrain. To counter drone heat detection in combat, use thermal blankets, decoys, and active cooling to shield emissions. Operate near heat-masking environments (brick or concrete structures), deploy smoke screens, and limit movement during cooler times. Further, employ counter-UAS systems to jam sensors, and use terrain for concealment to minimise detection risks.

Drones frequently monitor known supply routes, seeking signs of deviation or off-road movement. Tactical use of fighting positions and shielding your vehicle's vulnerable areas reduces exposure to drones. Leveraging natural cover, such as tree lines or terrain features, can dramatically reduce the likelihood of being observed from the air. Understanding and mastering these visibility factors increases your survivability and maintains operational security against ever-watchful drone reconnaissance.



The Role of Technology in Countering UAS Threats: Leveraging Both Vehicle Craft and Innovation

While traditional vehicle craft and fieldcraft are indispensable on the battlefield; it alone is 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 general, the C-UAS mission can be broken down into four distinct phases, each of which requires special attention: **Detect, Track, Identify, and Mitigate (DTI-M)**.

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 drones that emit RF signals, to ones that are piloted autonomously by way points, 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 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 Thales 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 friendly or malicious. As drones increase in popularity, many organizations, both military and non-military, have begun to use them as productive tools in their daily operations.
    b. The C-UAS solution can then identify the drone model. The identification can include unique identifiers such as drone serial number or 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 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 units, enhancing decision-making capabilities.

4. **Mitigate:** C-UAS mitigation solutions generally fall into two broad categories: **kinetic** and **non-kinetic**, each with their 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.

a. **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 your tactical position and/or collateral damage. Examples of kinetic methods include:
    i. **Missiles and Bullets:** Conventional weaponry can be highly effective, particularly in military contexts where the priority is neutralising threats quickly. However, the risk of collateral damage may be a significant concern, especially in urban environments or densely populated areas where civilian infrastructure is at risk. One significant downside to using missiles as a C-UAS mitigation tool is that the mitigation often costs more than the threat being mitigated, eventually leading to losing a war of attrition due to economic factors. Conventional bullets also often do not have a long enough effective range to counter malicious drone threats from an acceptable standoff.
    ii. **Nets and Takedown Devices:** These non-explosive methods provide a safer, more controlled alternative to traditional firearms. 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 damage is a priority. Takedown devices and nets also can provide the opportunity to capture a malicious drone for forensic analysis and/or hardware exploitation.

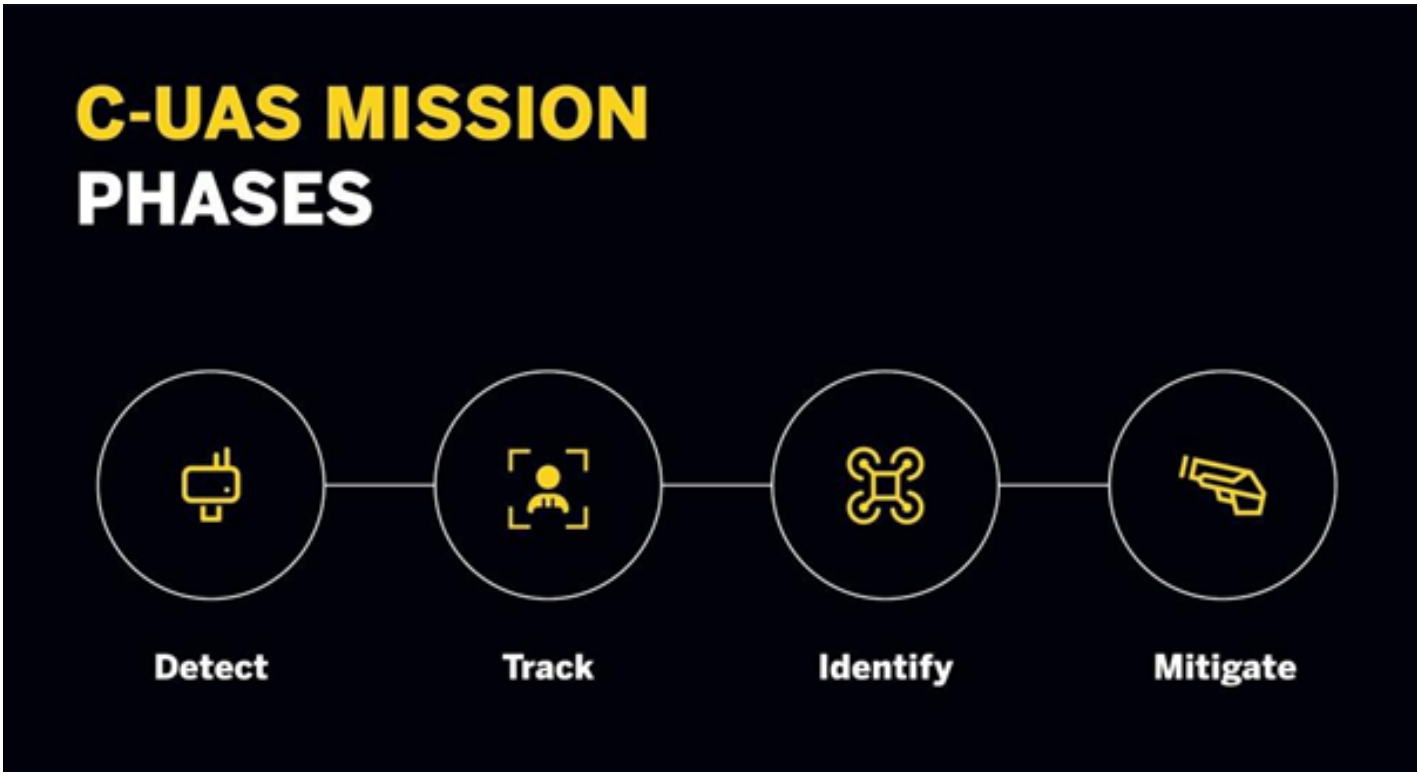
b. **Non-Kinetic Methods:** Non-kinetic approaches, by contrast, focus on disrupting a drone's operations without kinetic energy or physical interference. The complexity of these systems means they must be regularly refined to remain effective against new UAS capabilities. Methods include:
    i. **Electronic Warfare (EW):** Radio Frequency (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 way of mitigating a drone by taking 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. This is an elegant way to mitigate a drone when it works. The success rate of cyber-takeover is often quite low for two reasons. The mitigating controller must be able to predict the frequency hopping of drone and must 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.

iii. **Directed Energy:** Directed energy weapons such as high-energy lasers (HELs) and high-power microwaves (HPMs) provide a low collateral damage, non-kinetic option for engaging malicious drones. HELs concentrate 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 a large up-front cost, the low "per shot cost" makes them attractive C-UAS options.

HPMs send out a blast of directed energy which can be used to "fry" electronics. The main benefit of HMPs is that they can be effective tools against UAS swarms, but they are unable to engage targets at longer ranges.

Mounting solutions on a Bushmaster enhance deployment flexibility while leveraging its robust platform for precision execution. The Bushmaster's unique combination of protection, mobility, and modularity makes it an invaluable asset in C-UAS operations. By bridging traditional vehicle craft with cutting-edge technological innovation, it empowers operators to detect, track, identify, and mitigate UAS threats in an increasingly complex battlespace.



Ultimately, the operator must have an effective tool to manage the DTI-M C-UAS cycle. Dedrone by Axon's award-winning, purpose-built C2 software solution, DedroneTracker.AI, serves as a single-pane-of-glass user interface. DedroneTracker.AI allows the operator to monitor and control all parts of the DTI-M process. The advanced artificial intelligence/machine learning (AI/ML) driven C2 platform incorporates advanced proprietary algorithms and machine learning techniques to ingest and fuse multiple sensor inputs such as RF, EO/IR camera, and radar. 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 fibreoptic 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 UAS 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.

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

1. **Fixed-Site:** Hardware deployments are permanent or semi-permanent installations designed to protect critical infrastructure locations like airports or military bases by providing a comprehensive defence against drone incursions. These setups typically incorporate an array of sensors and response mechanisms for long-term security.
2. **Expeditionary Kits:** Offer a portable solution, allowing rapid deployment in remote or temporary locations where immediate drone threats may arise. These kits are ideal for tactical missions requiring flexibility and quick set-up.
3. **On-the-Move (OTM):** Portable, vehicle-mounted solutions 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 this capability, manoeuvring formations often bog down into trench warfare as currently seen in Ukraine.

A Layered Approach to C-UAS: No One-Size-Fits-All Solution

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

A layered C-UAS defence strategy requires combining fieldcraft and multiple layers of C-UAS detection, tracking, identification, and mitigation methods into an all-encompassing 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, such as 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 each other, creating a defence that is flexible, adaptive, and difficult for adversaries to circumvent. This layered strategy ensures that the operator is not merely reacting to UAS threats but actively anticipating them and then proactively defending against them. By fostering a culture of continuous innovation and tactical adaptability, the user can stay one step ahead of adversaries, better equipping themselves to address the complexities of the UAS landscape with both precision and foresight.

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. We outlined the most significant evolutions below.

Directed Energy Weapons (DEWs) are becoming a major focus, particularly laser systems that can disable or destroy drones with precision, minimising collateral damage in sensitive environments. HPMs are also being developed to disrupt drone electronics, providing a non- lethal option to neutralise threats without relying on traditional ammunition. Similarly, HELs are being developed which can disable malicious drones from longer stand-off distances, while minimizing collateral damage to friendly personnel, infrastructure, and aircraft. These technologies will rapidly evolve to become more capable, reliable, and cost-effective C-UAS tools.

AI/ML enabled technology is becoming increasingly essential for countering UAS. AI- powered systems exist to DTI drone threats and will soon evolve to also respond autonomously to these threats, adapting to new tactics in real-time. Machine learning enhances EW capabilities, allowing for more precise jamming or spoofing of UAS communications while reducing the risk of interfering with friendly systems. Dedrone by Axon's dedicated AI/ML team recently released a next-generation computer vision (CV) model which is now powering all of Dedrone by Axon's products, including their latest sensor-fusion drone protection solutions. Three fundamental building blocks must come together to create the world's fastest and most accurate AI/ML enabled airspace security solution. These include powerful hardware, learning neural network architecture, and robust data. In each case, Dedrone by Axon has brought together the most capable components available to deliver an average 20% speed increase of our video tracker in addition to a significant improvement in accuracy, driving down both false positives as well as false negatives. This resulted in a 24.3% improvement in Mean Average Precision (mAP) and a 12.8% improvement in Mean Average Recall (mAR). AI/ML enabled C-UAS technology is still in its infancy and will undoubtedly continue to improve detection accuracy and speed, allowing for more effective mitigation.

Swarm defence technologies, another crucial development, are designed to combat the growing threat of drone swarms. These systems will be capable of neutralising multiple drones simultaneously, using either kinetic or non-kinetic methods such as jamming or launching interceptor drones.

Quantum sensor technology, though in its early stages, promises to revolutionise drone detection, especially in conditions where traditional radar may fail. Quantum radar systems could potentially detect stealth drones that evade conventional detection, offering a new level of defensive capability.

Hypersonic interceptor missiles are another cutting-edge development designed to respond swiftly to fast-moving, high-altitude UAS threats, ensuring that even the most elusive drones can be intercepted effectively.

The advent of 5G networks is further enhancing C-UAS strategies by providing faster, more reliable communication between sensors and countermeasures, improving the speed and efficiency of response.

Additional advancements include smart jamming systems which are designed to adapt dynamically to evolving UAS frequencies, countering even the most sophisticated drones, and nanotechnology to create smaller, more discreet C-UAS solutions. Also, augmented reality (AR) is being integrated into soldier systems and vehicles, providing real-time data on UAS threats to enhance situational awareness and response times.

Together, these developing technologies represent the future of C-UAS strategies, offering new layers of defence that combine innovation with flexibility. As these advancements come to fruition, they will empower defence forces to stay ahead of evolving threats, ensuring a proactive and comprehensive approach to safeguarding against UAS on the modern battlefield.

Conclusion: Building a Smarter Defence Against UAS Threats Requires Constant Innovation

The evolving landscape of UAS threats demands more than technological innovation-it requires a deep, collaborative effort from the brightest minds in the industry. At Thales Australia and Dedrone by Axon, we understand that the future of C-UAS strategies lies not in any single solution but in a layered, adaptive approach that combines fieldcraft expertise, cutting-edge technology, and operational innovation. Our mission is not to react to emerging challenges but to anticipate them, staying one step ahead in an unpredictable and rapidly changing environment.

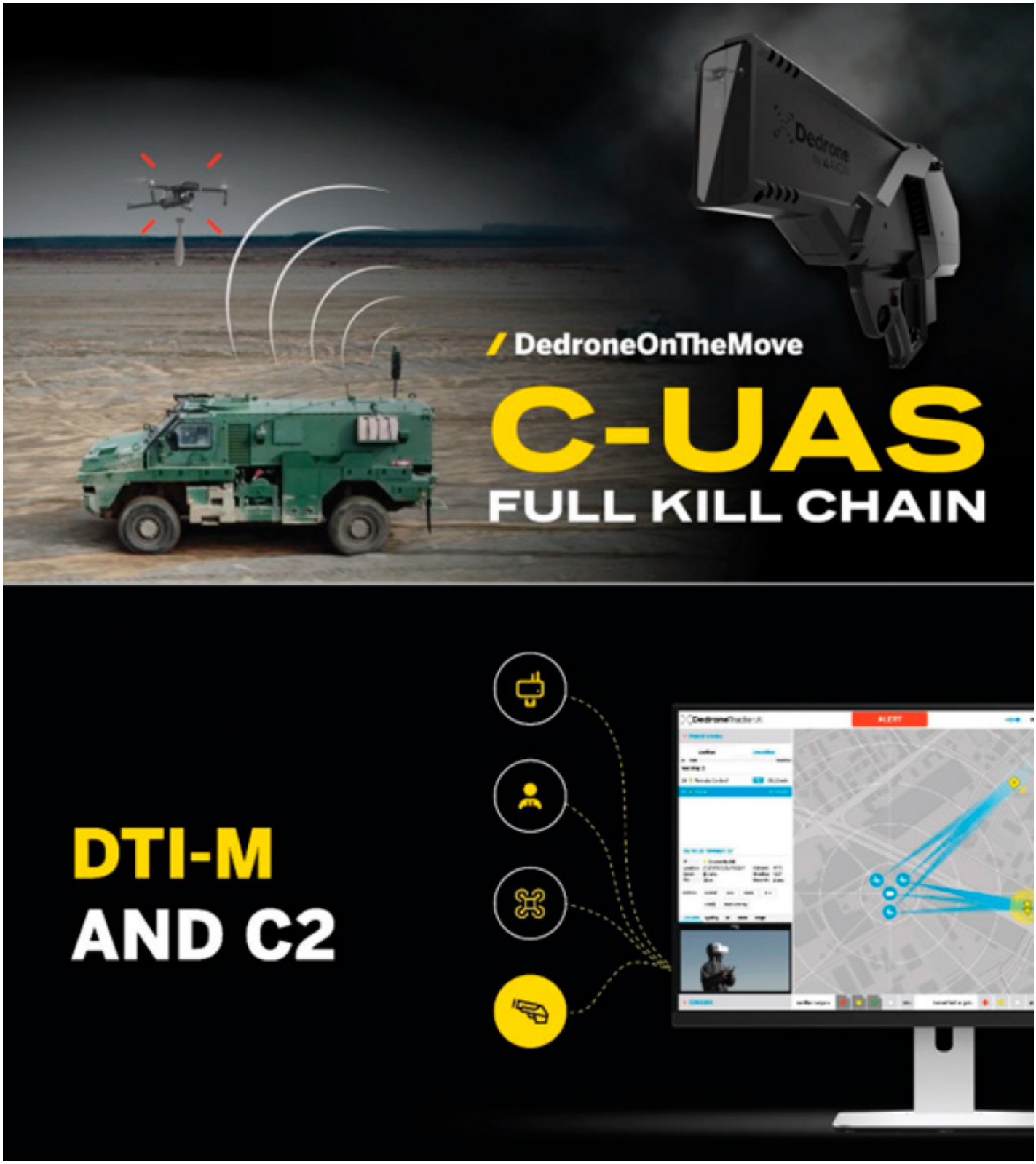
This is why we are committed to fostering a **think tank** culture - bringing together the smartest people in the room to continuously refine, adapt, and enhance our C-UAS strategies. By leveraging diverse perspectives and deep expertise, we can better understand the full spectrum of UAS threats and build robust solutions that go beyond surface-level responses.

We aim to empower our customers and partners to thrive in a world where these threats are constant, complex, and evolving.

By combining practical fieldcraft and cutting-edge technology, we can build a future-ready defence framework that not only counters UAS threats but also shapes the future of aerial warfare. Together, with the best minds leading the charge, we will safeguard our forces and ensure a resilient, forward-thinking approach to protecting against the technologies of tomorrow.

Authored by: Jason Moriarty, Product Line Manager, Thales Australia, and Michael Roche, Global Defense Marketing Manager, Dedrone by Axon

This article represents a collaborative effort between Thales Australia and Dedrone by Axon, showcasing the shared expertise and innovative insights of both organisation's mounted OTM, Fixed and Expeditionary C-UAS systems.



THALES

Building a future we can all trust

7 Murray Rose Avenue,
Sydney Olympic Park, NSW
Australia

thalesgroup.com