DRONESHIELD

Counter-Uncrewed Aerial Systems

Meeting the Challenge of the Defence Strategic Review

LEVEL 5, 126 PHILLIP STREET, SYDNEY NSW 200
INFO@DRONESHIELD.COM
+61 2 9995 7280

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Uncrewed Aerial Systems (UAS) have emerged as a disruptive force, challenging traditional defence strategies and systems. Their accessibility, affordability, and versatility have enabled them to transform into powerful tools that both state and non-state actors are exploiting, compelling urgent responses from defence organisations worldwide, including the Australian Defence Force (ADF).

The Defence Strategic Review (DSR) provides a comprehensive blueprint to address escalating geopolitical threats through an overarching strategy of denial amid rapid technological advances. However, there are significant gaps in the Counter-UAS (C-UAS) capabilities of the ADF that have not been fully addressed. These gaps pose risks to Australia's national security and defence resilience and jeopardise the realisation of DSR strategic objectives.

The distinct nature of UAS threats demands a forward-thinking approach that acknowledges the complexity of the challenge. For the ADF, this means confronting the sobering reality that this gap endangers domestic and deployed personnel, risks interruption to the operation of critical platforms such as long-range strike mechanisms and Integrated Air Missile Defence (IAMD) installations and undermines the safety and operational integrity of critical infrastructure such as naval shipyards.

This report makes three key recommendations:

1. The ADF should urgently prioritise the development and acquisition of C-UAS capabilities as part of its strategic preparedness plan.
2. The ADF should explore partnerships with local companies who have proven expertise in the C-UAS domain.
3. The ADF should invest in dedicated training and integration of C-UAS into its broader defence systems, ensuring personnel are ready and able to respond to evolving UAS threats.

Proactive measures to address the growing UAS threat are urgently needed. This report outlines how C-UAS solutions, specifically those produced by DroneShield, an Australian-owned global industry leader in C-UAS, could effectively bridge the existing gaps in ADF capabilities.

Photo caption Commercial drones being used in Ukraine for reconnaissance and attacks.

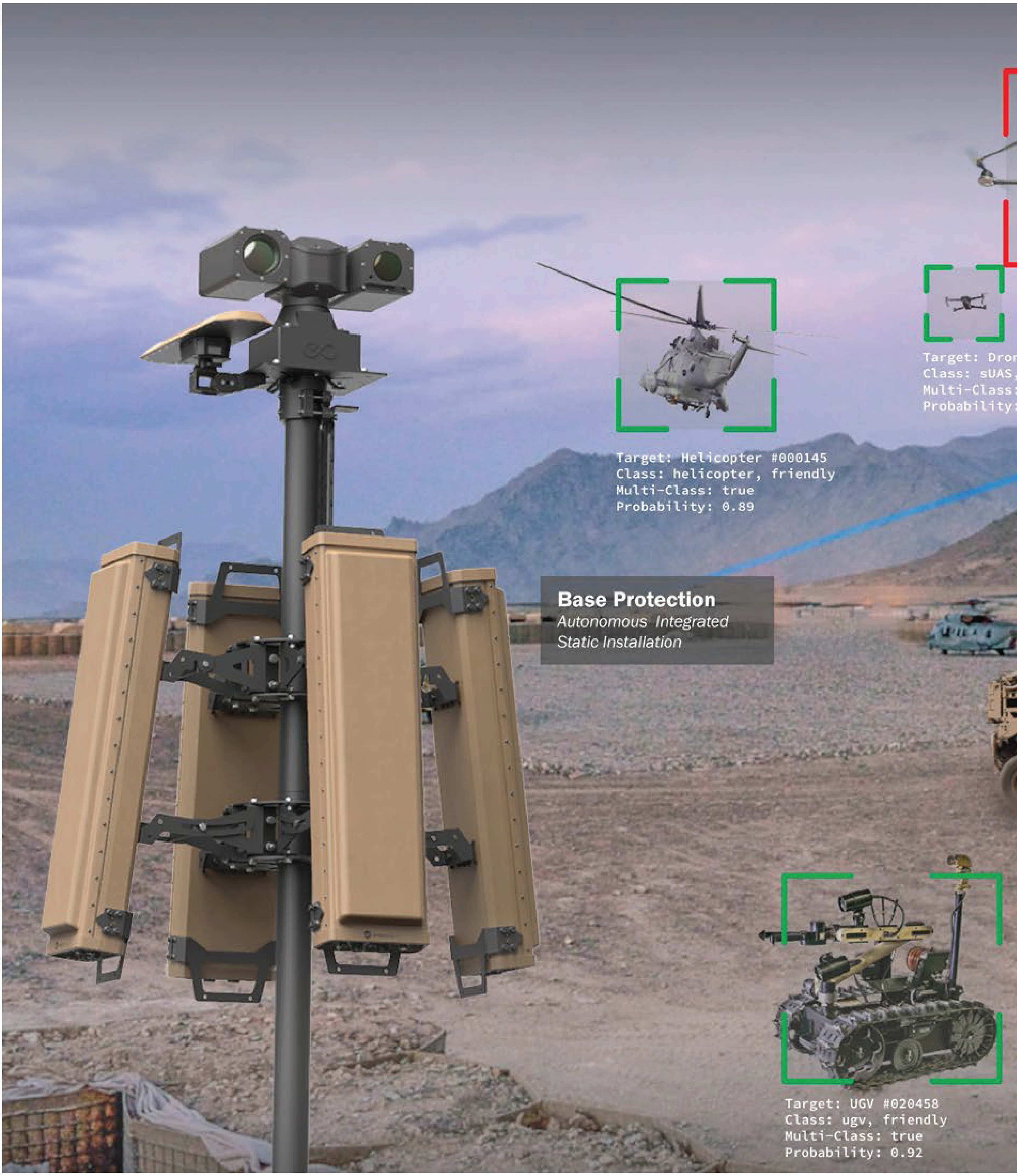
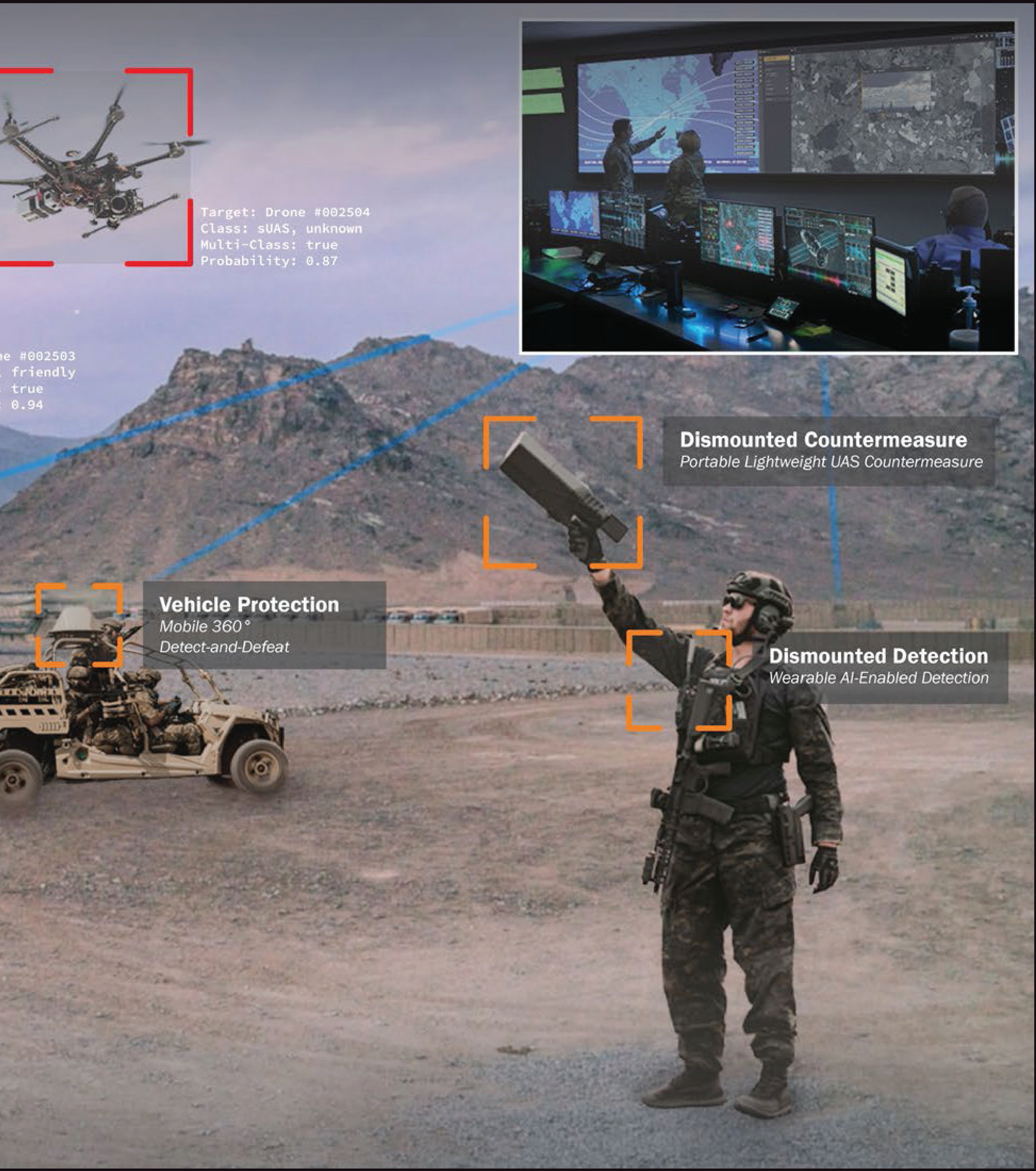


Photo caption Diagram of DroneShield detection and defeat capabilities.


Target: Drone #002504
Class: sUAS, unknown
Multi-Class: true
Probability: 0.87
ne #002503
, friendly
: true
: 0.94
Dismounted Countermeasure
Portable Lightweight UAS Countermeasure
Vehicle Protection
Mobile 360°
Detect-and-Defeat
Dismounted Detection
Wearable AI-Enabled Detection

THE ENVIRONMENT

UNCREWED AERIAL SYSTEM THREATS

THE EMERGING THREAT LANDSCAPE

Defence planning and security are facing a challenging issue: hostile UAS use. This trend is gaining prominence, particularly as UAS are being utilised more frequently in asymmetric warfare. These systems pose a significant and immediate threat to Australia's national security and defence capabilities, impacting both foreign and domestic planning and operations.

Cost reductions and increased consumer accessibility have made UAS a common, yet potent tool in contemporary conflict. Their ability to execute highly coordinated strikes and cause widespread disruptions makes them a distinct and dangerous instrument of modern warfare.

Two factors underscore the magnitude of this threat: the potential for disruption, and adversarial actors' ease of access to UAS. As the use of drone technology proliferates worldwide, it exposes vulnerabilities in defence systems and poses serious challenges to maintaining sovereignty and security.

As the use of drone technology proliferates worldwide, it exposes vulnerabilities in defence systems and poses serious challenges to maintaining sovereignty and security.

This disruptive capacity takes several forms:

Intelligence, Surveillance and Reconnaissance (ISR). The wide range of available UAS, from modifiable commercial photography UAS to more advanced devices equipped with high-end surveillance payloads, makes them an effective tool for hostile actors seeking to gather intelligence.

Kinetic Attack. UAS can serve as a platform for physical attacks, such as deploying explosives or harmful substances. The use of commercial off-the-shelf UAS modified with improvised explosives is becoming more feasible with UAS that can carry larger payloads.

Cyberattack. With advancements in cyber payloads, there are opportunities for UAS-assisted cyberattacks. The ability of UAS to gain proximity to military networks can facilitate their exploitation.

The accessibility and relative simplicity of UAS lowers the barrier of entry for asymmetric warfare, enabling hostile actors to acquire and deploy disruptive technology without warning.

Figure caption: Sample of group 1 UAS capable of heavier payload modification. Higher-end group 1 UAS are modifiable for a range of payloads, including surveillance and explosive material.

DJI Agras MG1

- 10kg payload
- 1km range
- 24 min flight time

Freefly Alta-8

- 9kg payload
- 2km range
- 16 min flight time

DJI S1000

- 6.8kg payload
- 2km range
- 15 min flight time

DJI Matrice 600

- 6kg payload
- 5km range
- 16 min flight time

IMPLICATIONS AND RISKS FOR AUSTRALIA AND THE AUSTRALIAN DEFENCE FORCE

The state of readiness and sustainment of high-quality military capabilities is integral to defence preparedness. However, the threats posed by UAS, including ISR, cyberattacks, and physical damage, may jeopardise this preparedness.

UAS pose risks to personnel and platforms as has been seen in Ukraine, along with estate and infrastructure, particularly basing, shipyards, and supply warehousing where UAS enabled ISR poses a risk by potentially disclosing highly sensitive information. This threat is accentuated when the exposed information relates to allied defence planning, potentially providing adversaries with valuable intelligence to enable malicious intent.

Furthermore, a UAS attack on Australian Defence estate and infrastructure could result in secondary implications such as societal fear and disruption, and have negative impacts on Australia's international reputation. Such a scenario would significantly damage the assessment of Australia's national resilience.

UAS also present a threat to Australian military systems as platforms for kinetic and cyber-attacks. Defence estate and infrastructure are designed to protect against conventional threats but often lack provisions for UAS-enabled attacks. This gap leaves major defence capabilities and supply chains vulnerable, including the operation of expensive platforms, that consist of air and maritime assets operating from these locations.

Photo caption U.S. Marine deploying XMQ-13 instant eye UAS during exercise Juniper Cobra 2018.

THE CHALLENGE

DELIVERING THE DEFENCE STRATEGIC REVIEW

OVERVIEW OF THE DEFENCE STRATEGIC REVIEW

The DSR outlines a national approach to address the evolving strategic landscape. Two cornerstones of this strategy - pursuing a denial strategy and developing a high level of resilience - are put at risk by UAS threats.

Strategy of Denial. The strategy of denial, a fundamental aspect of the DSR, is intended to dissuade potential aggression towards Australian territories and hold adversaries' forces and supply chains at risk from a distance (anti-access) while also denying access to the ADF's primary operating region (area-denial). This strategy of anti-access/area-denial (A2/AD) serves to curb an adversary's freedom of action and reduce their ability to coerce or operate against Australia without being held at risk. The success of this denial strategy in part relies on our ability to protect and enable freedom of action for ADF personnel, platforms, and infrastructure.

Resilience. The DSR's focus on building a high level of resilience is aimed at making Australia a hard target and reducing susceptibility to coercion. The DSR highlights this through the identification of key requirements such as enhanced military preparedness, advanced munitions manufacturing, fuel security, robust national logistics, and a secure industrial base. The initiative, termed "accelerated preparedness", calls for swift overhauls of priority platforms and infrastructure to ensure national resilience.

The aspirations outlined by the DSR may be put at risk if the ADF does not address the threat from UAS. Despite its detail, the DSR lacks explicit measures for developing C-UAS capabilities, a concerning omission given the emerging threat landscape.

> ***Strategy of Denial***
>
> *A strategy of denial is a defensive approach designed to stop an adversary from succeeding in its goal to coerce states through force, or the threatened use of force, to achieve dominance.*
>
> *— DSR, p. 49.*

C-UAS CAPABILITY GAPS

The prevailing gaps in addressing hostile UAS incursions cover three critical areas - the protection of ADF personnel, safeguarding military platforms, and preserving defence infrastructure:

Personnel. The ADF’s protection against UAS attacks is insufficient. Without appropriate safeguards, personnel are vulnerable to UAS attacks on both tactical and strategic levels - from battlefield disruptions to targeted assassinations. Therefore, systems capable of detecting UAS and intercepting them before causing harm are imperative.

Platforms. The DSR’s denial strategy largely depends on advanced, costly military platforms. However, these expensive yet sensitive platforms, such as long-range strike and IAMD installations, are attractive targets for hostile UAS which can cause substantial disruption at minimal expense. Hence, it is vital to establish early warning and area defence capabilities to protect these assets against asymmetric threats.

Infrastructure. Secure infrastructure is essential for the maintenance and operation of ADF personnel and platforms. Currently, a hostile actor can easily monitor and disrupt defence infrastructure crucial to resilience building, including munitions, fuel, basing, and shipbuilding. Implementing mechanisms capable of detecting and neutralising hostile UAS activity is crucial.

Persistent capability gaps expose the ADF’s personnel, platforms, and infrastructure to UAS threats. LAND156, one of the ADF’s major C-UAS programs aimed at providing capabilities for domestic and expeditionary contexts, has been pushed into Horizon Three (2031 and beyond). Pushing the delivery of these crucial systems past the five-year period will prolong the ADF’s vulnerability to UAS. This invites adversaries to undertake intelligence and disruption actions, leading to substantial damage before defensive measures can be implemented. C-UAS measures are vital to dissuade opportunistic use of UAS.

Photo caption DroneShield RfPatrol utilised for asset protection.

ADDRESSING THE CHALLENGE

CAPABILITY SOLUTIONS

C-UAS CAPABILITY SOLUTIONS

In alignment with the DSR denial strategy, C-UAS provides an essential countermeasure to the escalating threat posed by UAS. Deploying C-UAS solutions leverages robust, effective, and cutting-edge technology.

Threat and Risk Management. C-UAS solutions provide robust, advanced, and adaptable defences against hostile UAS that are capable of effectively mitigating this growing threat.

Enhancing Current Systems. C-UAS solutions are designed to integrate with existing defence platforms such as IAMD installations and early warning systems for deployed force elements. They offer an added layer of protection and increase the expected return on these investments by preventing potential disruptions from UAS intrusions.

Leveraging Advanced Technology. C-UAS solutions employ advanced technologies including Radiofrequency (RF), radar, acoustic sensors, and UAS jamming capabilities. These technologies enable real-time detection and neutralisation of hostile UAS before they can inflict significant damage or disruption.

Versatile Applications. The versatility of C-UAS solutions is demonstrated in a variety of systems designed for different missions, including vehicular, shipboard, pop-up systems, fixed-site solutions, and handheld devices. Their ability to integrate seamlessly with other defence systems enhances overall security and acts as a force multiplier.

Maintaining an Asymmetric Advantage. By effectively dissuading potential UAS threats, C-UAS can help ensure that Australia maintains an asymmetric advantage in critical military technology areas.

Photo caption DroneShield DroneSentry-X ship mounted direction-finding UAS sensor (using RF technology).

> ***Asymmetric Advantage***
>
> *Military modernisation in the region, and the implications of strategic competition, mean it is no longer feasible to maintain a broad-based regional capability edge. To respond, Defence needs to focus on asymmetric advantages and ensure that we maintain parity or qualitative advantage in critical military technology areas*
>
> *— DSR, p. 71.*

THE CASE FOR DRONESHIELD

Within Australia, DroneShield is the only sovereign company with the expertise and technology to deliver sophisticated, versatile, and reliable C-UAS solutions to meet the threat facing the ADF. As Australia seeks to address capability gaps and achieve the outcomes outlined in the DSR, the need for C-UAS is paramount.

Protecting Personnel. DroneShield's cutting-edge products like RfPatrol and DroneGun Mk3 form a portable, end-to-end C-UAS capability, providing robust protection to ADF personnel in various operational settings. These tools mitigate the risk of UAS attacks at both tactical and strategic levels, ensuring the safety of personnel.

Defending Platforms. For protection of forward deployed joint force elements and costly yet sensitive platforms such as long-range strike and IAMD installations, DroneShield's multi-domain, multi-mission solutions like DroneSentry, coupled with DroneCannon RF or DroneGun Tactical, offer an additional layer of protection. These systems establish early warning and area defence capabilities that safeguard these assets from UAS-inflicted disruptions.

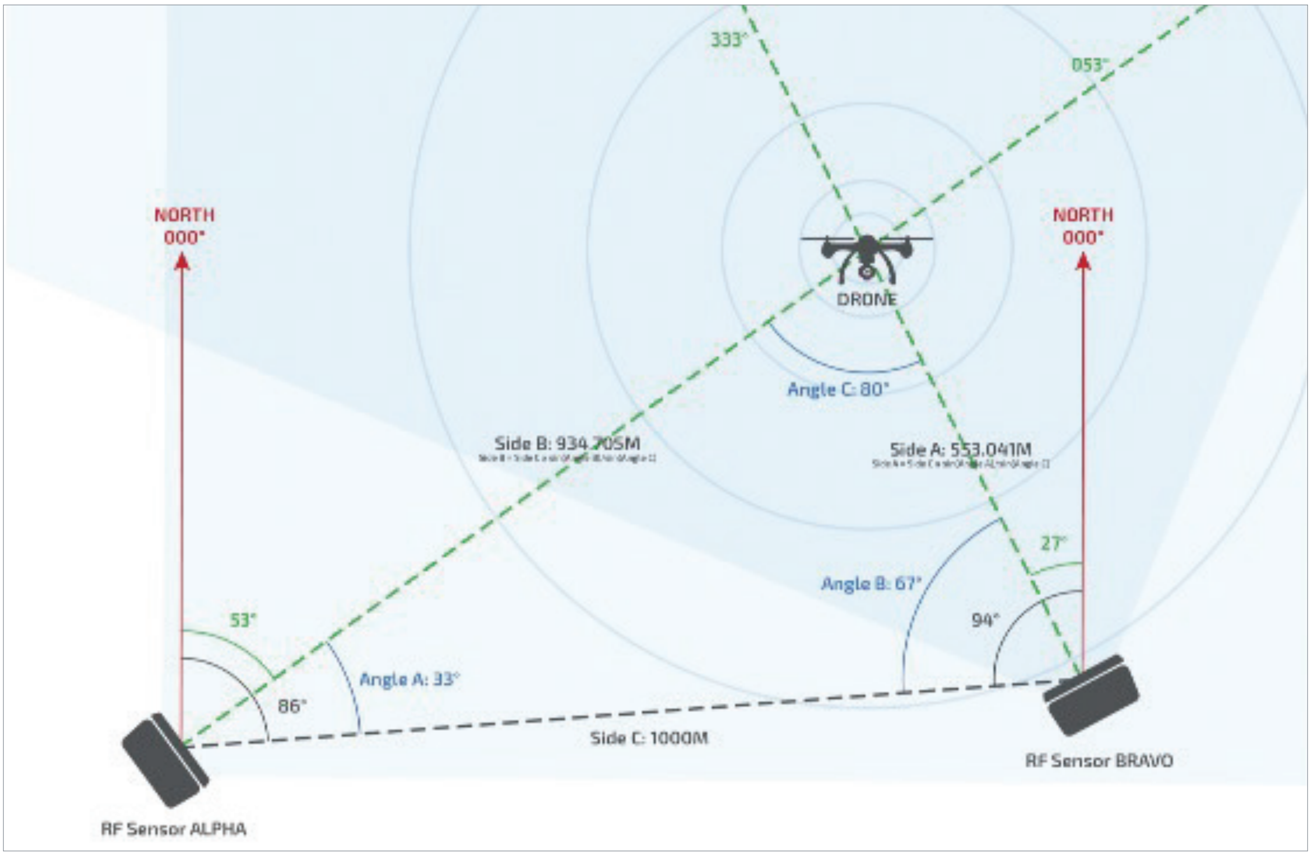
Preserving Infrastructure. DroneShield's versatile C-UAS solutions offer secure protection to crucial defence infrastructure from potential UAS threats, ensuring operational continuity and resilience of ADF personnel and platforms.

Interoperability. DroneShield has sold and deployed hundreds of handheld, vehicle and fixed site C-UAS solutions to a variety of partners. This has included multiple contracts with the US Department of Defense (DoD), US intelligence community agencies, Homeland Security and other US Government deparments and agencies. Shared capabilities and experiences will allow for frictionless cooperation between Australia and the US.

Cutting-Edge C-UAS Algorithm. DroneShield sets itself apart with smart jamming techniques that offer instantaneous and universally effective results. Unlike conventional drone defeat methods, which can take 30-60 seconds per UAS and are often model-specific, DroneShield's proactive approach targets C2 and Global Navigation Satellite Systems (GNSS) bands, enabling the autonomous detection and defeat of hostile UAS. These robust capabilities are supported by continuous firmware updates and library-less systems.

Adaptability to Rapid UAS Evolution. DroneShield's novel approach deviates from traditional library-based pattern matching algorithms. Instead, it makes use of machine learning (ML) techniques to learn and react to UAS behavior in real time. Adopting ML into time-tested methods for UAS detection, such as RF-based detection and smart-jamming, paired with its innovative software and proven neutralisation strategies, ensures a high level of effectiveness in countering evolving UAS threats.

Photo caption RF Triangulation of a Drone Location (two sensors is generally enough).



High Detection Rate and Low False Alarms. A significant challenge in C-UAS operations is balancing highly sensitive receivers with a low false alarm rate, especially in congested RF environments. DroneShield's advanced multi-sensor systems leverage AI-based sensor fusion methodology to resolve this issue. By reducing cognitive load on operators and enhancing the probability of detecting hostile UAS, DroneShield's swift and dependable C-UAS solutions can provide Australia with an asymmetric advantage.

Projected Collaboration and Future Directions. DroneShield's ability to collaborate with Defence aligns with two core DSR priorities: projecting area-denial beyond the Northern approaches and defending critical infrastructure. In addition, DroneShield's sovereign IP and supply chain enables the delivery of real capability within the most urgent three-year period.

Sovereign IP and Supply Chain. DroneShield's locally-developed C-UAS and sovereign supply chain serves as an enabler of national resilience, a concept heavily emphasised in the DSR. Trusted parties can collaborate and continuously enhance sovereign C-UAS capability. These solutions provide resilience against unexpected disruptions, keeping pace with the rapidly evolving strategic environment. Annex A details how DroneShield actively collaborates with a range of Australian partners.

Photo caption DroneShield RfOne passive far-range drone detection sensors on an Australian Light Armoured Vehicle.

CONCLUSION

UAS have emerged as an asymmetric and disruptive capability that pose significant challenges for protecting the ADF's people, platforms, and infrastructure. In order to bolster the ADF against this threat of asymmetric warfare, the DSR has recommended that Australia pursue a strategy of denial and improve national resilience. Whilst the DSR's recommendations are comprehensive, they have not addressed the significant gaps in the ADF's C-UAS capabilities. These gaps pose substantial risks to the delivery of DSR objectives and Australia's national and defence resilience.

To mitigate these risks, it is crucial for the ADF to adopt a forward-thinking and proactive approach that recognises the complexity and potential consequences of UAS threats. C-UAS offers a compelling pathway to mitigate this UAS threat. By integrating C-UAS capabilities across people, platform, and infrastructure projects, the ADF can strengthen its defence against the growing UAS threat, ensuring that the objectives of the DSR are not just aspirational but achievable.

DroneShield, an Australian-owned global leader in C-UAS, offers off-the-self solutions that can bridge the existing gaps in ADF capabilities. Waiting until the first UAS strike on Australian military systems to speed up capability acquisition risks a major scheduling gap between capability delivery, and integration and training for operators. This can be avoided by embracing proactive measures and leveraging the advanced technologies provided by DroneShield.

ANNEX A

DRONESHIELD **PARTNERSHIPS**

DroneShield's delivery of C-UAS outcomes and collaboration with a range of partners demonstrates its ability to deliver practical solutions to address Australia's C-UAS capability gap.

AUSTRALIAN PARTNERSHIPS

DroneShield has a strong background of partnering with Australian Government organisations and industry. This includes active involvement with the ADF during the 2021 Talisman Sabre military training exercise. Here, DroneShield's RfOne Mk2, a passive, high precision RF detection product was mounted on Australian Light Armoured Vehicles (ASLAVs), delivering long-range and highly accurate drone detection and tracking capabilities.

DroneShield's involvement has not been confined to military exercises. The company's technology was utilised as part of the comprehensive security measures implemented for the 2018 Gold Coast Commonwealth Games, the 2018 ASEAN-Australia Summit in Sydney, and 2023 Australian Formula 1 Grand Prix in Melbourne. During these events, DroneShield technology played a critical role in maintaining safety and operational integrity by providing reliable, effective counter-drone solutions.

In September 2021, a significant partnership with Trakka Systems marked a further milestone in DroneShield's Australian journey. The two firms joined their collective expertise in detection and situational awareness to create the Trakka Interceptor Package Solution (TIPS-C). Offering a covert solution to the growing UAS threat, the TIPS-C stands as a clear symbol of the productive, innovative collaboration shared between DroneShield and other industry leaders in Australia.

Photo caption A member of the Queensland Police Service utilising DroneGun Mk2 during the 2018 Gold Coast Commonwealth Games.

Photo caption DroneShield capability demonstration with the Australian Army.

AMERICAN PARTNERSHIPS

DroneShield has established a strong presence across the defence supply chain. In late 2022, it was selected by the Joint Counter-Small Unmanned Aircraft Systems Office (JCO) as part of SAIC consortium to provide RF-based drone detection and smart jamming based drone defeat for rollout across US DoD bases, following an extension evaluation over the course of the year.

DroneShield further solidified its American partnerships by initiating a Cooperative Research and Development Agreement (CRADA) with the US Department of Homeland Security Science and Technology Directorate (DHS S&T) in October 2021. By February 2022, DroneShield's Sensor and Command-and-Control platforms had fully complied with the US Government's Team Awareness Kit (TAK). This system, developed by the Air Force Research Laboratory (AFRL), is widely utilised by the US DoD and Allied forces.

In October 2022, DroneShield secured a US$1.8m contract from the US DoD for its DroneGun MKIII handheld C-UAS, following on from multiple earlier sales to the US DoD of products deployed with the US military both to US and overseas bases. Subsequently, in November 2022, DroneShield formed a partnership with Epirus, Inc., a multi-billion US defence technology company specialising in software-defined High-Powered Microwave directed energy systems.

In April 2023, the Montgomery County Office of Homeland Security and Emergency Management (MCOHSEM) successfully utilised DroneShield's DroneSentry system during the 2023 IRONMAN Triathlon Championships in Woodlands, Texas.

Photo caption DroneShield capability utilised for event security at Ironman 2023, Texas.

Photo caption A security agent walks with DroneShield's DroneGun Tactical next to the presidential Rolls-Royce that was used by President-elect Luiz Inácio Lula da Silva at his inauguration ceremony in Brasilia, on January 1, 2023.

EUROPEAN PARTNERSHIPS

DroneShield has extensive partnerships across Europe. A noteworthy collaboration includes the integration of DroneShield's UAS detection and mitigation products with Bosch's video surveillance products as part of the Bosch Integration Partner Program (IPP). In 2019, DroneShield also joined forces with BT Group, a global leader in telecommunications, to provide solutions after several incidents of rogue UAS disruptions at London's Gatwick Airport.

In December 2020, DroneShield collaborated with Squarehead, a Norwegian-based acoustic array technology company. This partnership, which is currently undergoing test and evaluation with the US DoD, combines DroneShield's best-in-class C-UAS sensors and effectors with Squarehead's expertise in the acoustic domain.

In September 2022, DroneShield solidified its position in the European market, receiving a US$2m order for multiple DroneSentry fixed site detect and defeat systems from a European Government customer.

SOUTH AMERICAN PARTNERSHIPS

In 2021, DroneShield entered the South American market, selling several DroneGun Tactical units to the Brazilian Government. At the 2023 Presidential Inauguration, Droneshield's DroneGun Tactical neutralised four suspicious drones heading towards President Lula da Silva.

Photo caption DroneShield capability demonstration at Brussels Airport.

ANNEX B

C-UAS **CASE STUDIES**

Case Study 1

Maritime C-UAS Defence: Safeguarding Australia's Naval Assets against Drone Swarms

This case study explores a scenario where a UAS swarm, deployed from an unidentified fishing vessel, poses a threat to Australian naval vessels. It highlights the strategic importance of integrating robust C-UAS measures, like DroneShield's DroneSentry-X.

THREAT SCENARIO

A UAS swarm consisting of small, explosive carrying UAS is deployed and coordinated from an unidentified fishing vessel off the Northern coast of Australia. Littoral naval vessels are critical to ensuring both deterrence and practical defeat of any potential adversary north of Australia. These attacks would cause material damage and force the ADF to divert resources and personnel to counter this threat, resulting in the dispersal of resources needed to uphold area-denial in other areas.

STRATEGIC IMPORTANCE

The DSR seeks to develop the ADF so that any adversary seeking to coerce Australia through incursions in the north west shelf and exclusive economic zone or disruptions to sea lines of communication will be deterred from doing so. To achieve this, the DSR recommends a force posture which supports a strategy of denial, with the ability to hold forces at risk in northern maritime approaches. For this strategy to be sustainable, the ADF maritime surface capabilities must have comprehensive security and protection.

SOLUTION

DroneShield's DroneSentry-X can deny this threat by deploying a maritime-focused C-UAS capable of detecting and neutralising armed drones targeting naval assets. DroneSentry-X is a lightweight, portable C-UAS designed for maritime environments. It is resistant to shock, weather, and UV exposure. It can be installed on naval vessels to protect them from armed UAS threats, reducing the risk profile UAS pose to maritime platforms at a low operating cost. DroneSentry-X can optionally include DroneCannon countermeasures to defeat UAS automatically or manually once a threat has been identified. This provides end-to-end detection and response capability.
The effectiveness of DroneSentry-X was proven during sea trials aboard the US Navy's stealth experimentation prototype the M80 Stiletto. This solution contributes to critical maritime capacities for sea denial operations and localised sea control and would enhance existing Littoral Manoeuvre Vessel-Medium (LMV-M) programs.

Photo caption DroneShield DroneSentry-X ship mounted direction-finding UAS sensor (using RF technology).

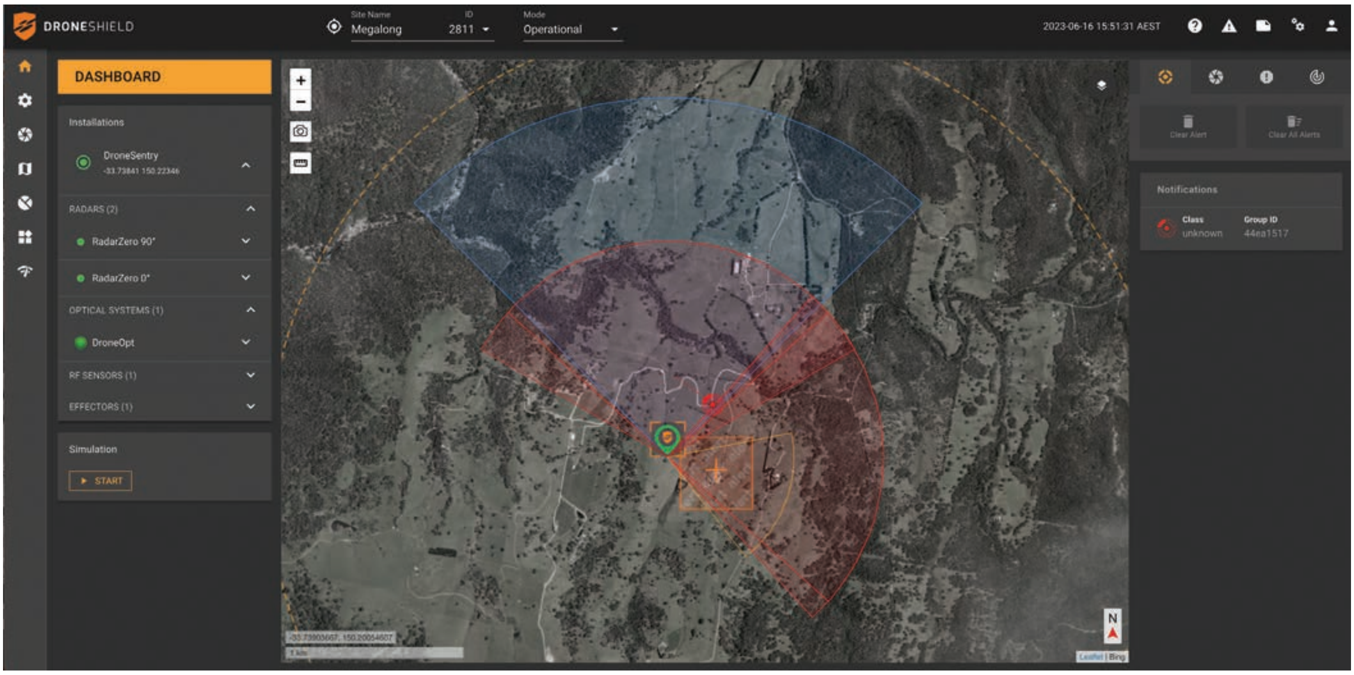
Case Study 2

C-UAS Defence for Strategic Infrastructure

This case study examines a scenario where an issue-motivated group seeks to disrupt the strategic operations of the Henderson Shipyard using a small UAS armed with chemical explosives. It underlines the necessity for an adaptive C-UAS solution such as DroneShield's DroneSentry to protect vital Defence installations.

Photo caption DroneShield capability demonstration at Sydney Airport.

Photo caption DroneShield DroneSentry-C2 Command-and-Control System.



THREAT SCENARIO

An issue-motivated group deploys a small UAS equipped with improvised chemical explosives from a hidden urban location East of the Henderson Shipyard, seeking to damage priority shipbuilding, shut-down critical berths for construction and maintenance and impact Australia's relationship with the United States.

STRATEGIC IMPORTANCE

The DSR identifies maritime nodes such as HMAS Stirling and Henderson Shipyard as being of strategic importance due to their contribution to priority capability development and hosting. These will require C-UAS to protect both Australian and allied platforms within three years. It highlights the need for hardening and dispersal, and securing critical inputs including fuel storage, mission planning nodes, and platform maintenance.

SOLUTION

DroneShield's fixed site solutions mitigate this threat by deploying comprehensive C-UAS to identify and intercept a threat before harm is done. DroneSentry has the capability to detect, track, and neutralise UAS attempting to disrupt infrastructure. With its modularised long-range protection, DroneSentry can be deployed with a specific mix of sensor and effector modalities to adapt to the specific needs of a site; for example, Henderson Shipyard's large precinct area and proximity to urban centres increases the need for comprehensive C-UAS. In this way, DroneShield's systems can provide early warning of UAS intrusions to strategic nodes and critical infrastructure and disrupt hostile activity before damage is done.

Case Study 3

Enhancing Australian Special Forces' Capabilities

In the face of heightened regional threats and A2/AD strategies from potential adversaries, this case study explores the value of DroneShield's suite of C-UAS products in strengthening the capabilities of Australia's Special Forces.

THREAT SCENARIO

As threats in the Indo-Pacific region escalate, Australia's Special Forces face increasingly complex and dangerous missions. Their tasks vary, from supporting Unconventional Warfare (UW) with partner forces to neutralising A2/AD capabilities. These forces can operate independently or within larger forces on a spectrum of clandestine to overt missions. This would require the ability to detect and evade surveillance drones discreetly, and in the event of an incoming threat, neutralise it without compromising the mission's integrity and security.

STRATEGIC IMPORTANCE

The DSR stresses the importance of deterring acts of aggression and coercion in the Indo-Pacific region. Given the versatile capabilities and operational flexibility, Australian special forces play a pivotal role in Australia's deterrence capabilities. Their capacity to project impactful influence on their own or in collaboration with other ADF or partner forces greatly enhances the nation's resilience against emerging threats.

SOLUTION

The size, discretion, and duration of special operation missions can vary widely, requiring scalable and adaptable counter-drone capabilities. Whether it's a small patrol from the SAS Regiment (SASR) conducting discrete operations with 2-6 personnel or a larger Commando mission involving platoons to company groups with 12-20 vehicles on missions lasting up to 28 days, each scenario poses unique challenges for implementing C-UAS strategies. The chosen C-UAS solution must cater to a variety of mission types, from those operating out of discrete locations to larger military establishments, and from small discrete non-uniformed teams to larger uniformed groups.

Photo caption DroneShield body-worn RfPatrol.

Photo caption DroneShield DroneGun Mk4.

Force Size and Composition. DroneShield's solutions offer adaptability to support different mission profiles:

1. ***Small Forces (up to 30 personnel).*** The RfPatrol w/ MAK and DroneGun provide discrete, portable C-UAS capabilities.
2. ***Medium Forces (Platoon or Company Group).*** A combination of DroneSentry-X (DSX) and RfPatrol w/ MAK provide additional capability where weight and profile are not primary considerations.
3. ***Large Forces (Task Force or Joint Force Group).*** The comprehensive coverage of DroneSentry and DSX supplemented by RfPatrol units for added mobility and discretion would provide the flexibility and coverage required by larger groups.

Discreteness. Different missions require varying levels of discreteness. For non-uniformed groups or operations involving civilian vehicles, RfPatrol w/ MAK offers a discrete C-UAS solution. For uniformed groups or military vehicle operations, the DSX system is more suitable due to its comprehensive threat coverage. For static locations, single safehouse operations might best utilise the RfPatrol w/ MAK, whereas medium to large coalition bases would benefit from the broader coverage of DroneSentry and DSX.

Independent vs Larger Force. RfPatrol and DroneGun work effectively for independent small groups with limited support. In contrast, larger task forces can utilise DroneSentry or DSX, which can integrate with broader command and control (C2) systems, facilitate ATAK data sharing, and relay information via soldier radios.

Duration. For prolonged operations, power can be a significant factor. DroneShield's products come with interchangeable spare batteries compatible with other kits, allowing extended durations of operation. In situations requiring constant monitoring, larger batteries, backup generators, or local power supplies connected to vehicle power units may be employed.

Threat Responses. Depending on the nature of the threat, operators may choose between passive observation and active disruption. DroneShield's solutions offer capabilities to detect and direction-find the threats (RfPatrol w/ DF Kit or DSX) and take active measures to neutralise them (DroneGun). The systems can also provide "pattern of life" information about threats, facilitating early warning and response planning.

DRONESHIELD