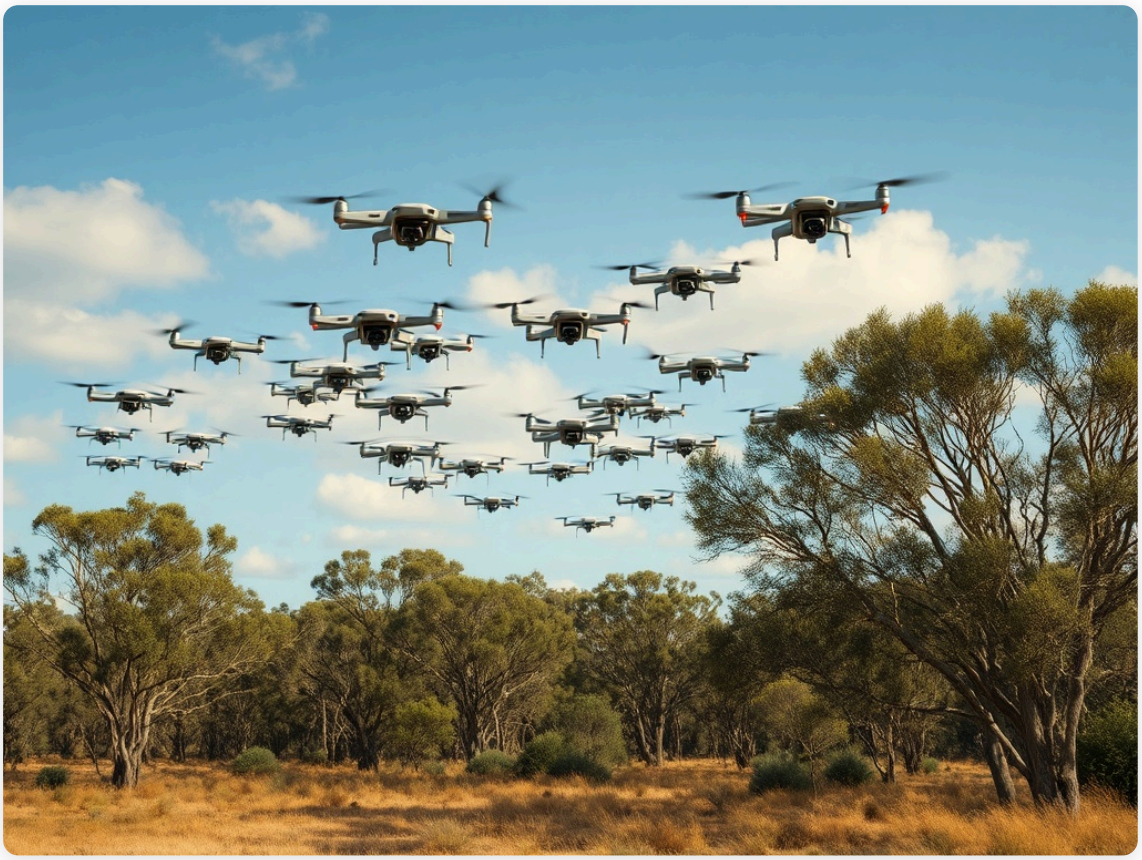
AI in defence for CUAS

A Strategic Whitepaper by Astute Systems

3 January 2026

AI in Defence for CUAS: A Strategic Imperative for Modern Security



Counter Unmanned Airborne Systems (C-UAS) are being enabled by AI

Executive Summary

The proliferation of Unmanned Aircraft Systems (UAS), commonly known as drones, has fundamentally reshaped the landscape of modern warfare and national security. From sophisticated military-grade platforms to readily available commercial quadcopters, these systems present diverse and evolving threats, ranging from intelligence, surveillance, and reconnaissance (ISR) to kinetic attacks and coordinated swarms. Traditional Counter-UAS (CUAS) methodologies, while effective against simpler threats, are increasingly overwhelmed by the speed, complexity, and sheer volume of contemporary drone operations.

This whitepaper argues that Artificial intelligence (AI) is not merely an enhancement but a strategic imperative for the future of CUAS. AI offers unparalleled capabilities in real-time detection, classification, tracking, and autonomous response orchestration, significantly reducing operator cognitive load and improving decision-making speed. By leveraging AI, defence forces can move beyond reactive measures to proactive, adaptive, and predictive CUAS operations.

Astute Systems believes that successful AI integration requires a holistic approach, encompassing robust data infrastructure, advanced sensor fusion, edge computing, and modular, interoperable system architectures. While challenges such as data quality, ethical considerations, and adversarial AI

persist, the opportunities for enhanced security, operational efficiency, and strategic advantage are profound. This paper outlines the critical path for defence stakeholders to embrace AI in CUAS, positioning Astute Systems as a pivotal partner in delivering these advanced capabilities.

1. Introduction & Background

The global defence and security environment is undergoing a rapid transformation, driven in large part by the widespread adoption and technological advancement of Unmanned Aircraft Systems (UAS). Once the exclusive domain of state actors, drones are now accessible to a wide spectrum of users, including non-state actors, terrorist groups, and even individuals with malicious intent. These platforms offer significant advantages in terms of cost-effectiveness, persistence, and reduced risk to human life, making them attractive for a variety of missions, from intelligence gathering and target acquisition to direct kinetic engagement and the delivery of chemical or biological payloads.

The threat spectrum posed by UAS is multifaceted:

- **ISR and Reconnaissance:** Small, difficult-to-detect drones can provide real-time intelligence on troop movements, critical infrastructure, and high-value assets.
- **Direct Attacks:** Drones can be weaponized with explosives, chemical agents, or equipped for kamikaze-style attacks.
- **Swarm Attacks:** Coordinated groups of drones, often numbering in the dozens or hundreds, can overwhelm conventional air defence systems through sheer numerical superiority and complex, adaptive behaviours.
- **Disruption:** Even non-kinetic drones can disrupt critical operations, such as airport traffic or public events, causing significant economic and social impact.

Traditional CUAS systems, primarily relying on radar, electro-optical/infrared (EO/IR) sensors, and radio frequency (RF) jamming, face significant limitations when confronted with these evolving threats. The sheer volume of airspace data, the need to distinguish legitimate drones from environmental clutter (birds, balloons), and the imperative for rapid, precise responses against multiple, fast-moving targets necessitate a paradigm shift. This is where Artificial Intelligence (AI) emerges as a game-changer.

AI, encompassing machine learning, deep learning, computer vision, and expert systems, offers the capability to process vast amounts of sensor data, identify patterns, make informed decisions, and automate complex tasks at speeds far beyond human capacity. For CUAS, AI promises to transform detection accuracy, accelerate response times, optimize resource allocation, and ultimately, provide a decisive advantage against the growing drone threat.

2. Current State Analysis

The current CUAS landscape is a complex mosaic of technologies, each with its strengths and weaknesses. Early CUAS solutions primarily focused on point defence using a combination of detection and interdiction methods.

2.1 Traditional CUAS Technologies and Their Limitations

Detection Technologies:

- **Radar:** Effective for detecting larger drones at range but can struggle with smaller, low-RCS (Radar Cross Section) drones and suffers from false positives due to environmental clutter.
- **Electro-Optical/Infrared (EO/IR) Systems:** Provide high-resolution imagery for classification and tracking, especially in good visibility, but are range-limited and affected by weather conditions.

- **Acoustic Sensors:** Useful for detecting closer drones based on engine noise but highly susceptible to ambient noise and limited in range.
- **Radio Frequency (RF) Scanners:** Detect and classify drones based on their control signals, but ineffective against autonomous drones or those using encrypted/novel communication protocols.

Interdiction Technologies:

- **RF Jamming/Spoofing:** Disrupts drone control links or GPS signals, causing them to return home or land. Effective against most commercial drones but can cause collateral interference and is less effective against autonomous or hardened systems.
- **Kinetic Interceptors:** Shotgun rounds, nets, or even missile systems designed to physically destroy or capture drones. Highly effective but often costly, with potential for collateral damage (e.g., falling debris) and limited engagement capacity against swarms.
- **High-Energy Lasers (HEL) and High-Power Microwaves (HPM):** Emerging technologies offering precision, speed, and potentially low cost per shot. Still in development for widespread deployment, with challenges in power requirements and atmospheric attenuation.

While these technologies form the backbone of many existing CUAS deployments, their standalone effectiveness is increasingly challenged by:

- **Drone Miniaturisation and Stealth:** Smaller, quieter drones with advanced materials are harder to detect.
- **Autonomy:** Drones operating without continuous human control or RF links bypass jamming.
- **Swarm Tactics:** Coordinated attacks overwhelm single-sensor or single-effector systems.
- **Evolving Communications:** Frequency hopping, encrypted links, and satellite communications make RF detection and jamming more difficult.
- **Cost-Effectiveness:** The cost of intercepting a cheap commercial drone with an expensive missile is often prohibitive.

2.2 Emergence of AI in CUAS

AI is beginning to bridge these gaps by enhancing the capabilities of existing sensors and effectors, and by enabling entirely new operational paradigms. Early applications include:

- **Enhanced Detection and Classification:** Machine learning algorithms are trained on vast datasets of drone signatures (visual, acoustic, RF) to improve the accuracy of identifying drones versus non-threats, significantly reducing false alarms.
- **Automated Tracking:** AI-powered computer vision can maintain lock on fast-moving, erratic drone targets across multiple sensor feeds, even in challenging environments.
- **Sensor Fusion:** AI algorithms can intelligently combine data from disparate sensors (radar, EO/IR, RF, acoustic) to create a more comprehensive and accurate picture of the airspace, even when individual sensors are limited.
- **Threat Prioritisation:** Basic AI models can assign threat levels to detected drones based on their flight path, behaviour, and potential payload, helping operators focus resources.

For instance, the U.S. Army's counter-UAS strategy increasingly emphasizes integrated, multi-layered solutions where AI plays a central role in processing sensor data and recommending responses. Similarly, NATO's Joint UAS Exploitation Group (JUEG) is exploring AI-driven solutions for better threat assessment and interoperability.

> *"The sheer volume and sophistication of modern drone threats demand more than just incremental improvements to existing CUAS technologies," Ross Newman, CEO at Astute Systems notes. "AI is the critical enabler that allows us to move from simply reacting to threats to intelligently anticipating, classifying, and mitigating them with unprecedented speed and accuracy."*

Despite these advancements, the full potential of AI in CUAS is still largely untapped. The current state often involves AI assisting human operators rather than fully automating complex decision-making, setting the stage for future development.

3. Key Challenges & Opportunities

The integration of AI into CUAS presents a dichotomy of significant challenges and transformative opportunities. Navigating these will define the success of future defence strategies.

3.1 Challenges

- **Data Requirements:**
- **Volume and Quality:** AI models demand immense quantities of high-quality, labeled data for training. Acquiring diverse datasets covering various drone types, flight patterns, environmental conditions, and sensor modalities is challenging and costly.
- **Data Labelling:** Manual labelling of drone images, radar signatures, and RF patterns is time-consuming and prone to human error.
- **Synthetic Data Generation:** While promising, generating realistic synthetic data that accurately reflects real-world complexities remains an active area of research.
- **Computational Power and Edge Processing:**
- Real-time CUAS operations require AI models to process data and make decisions at the edge (i.e., on the sensor platform itself) with minimal latency. This demands powerful, energy-efficient processors that can operate in harsh environments.
- Bandwidth limitations often preclude sending all raw sensor data to a central cloud for processing.
- **Ethical, Legal, and Policy Frameworks:**
- **Autonomy and Responsibility:** As AI-enabled CUAS systems become more autonomous in decision-making (e.g., selecting countermeasures), questions of accountability, human oversight, and the 'human-in-the-loop' versus 'human-on-the-loop' debate become paramount.
- **Rules of Engagement:** Adapting existing rules of engagement to AI-driven systems requires careful consideration to ensure compliance with international humanitarian law and ethical principles.
- **Collateral Damage:** Minimizing unintended harm when autonomous systems deploy kinetic or non-kinetic countermeasures.
- **Adversarial AI and Robustness:**
- **Evasion Techniques:** Malicious actors will undoubtedly employ adversarial techniques to confuse or bypass AI-powered CUAS systems (e.g., disguising drones, spoofing sensor data, using novel communication protocols).
- **Model Robustness:** Ensuring AI models are resilient to noise, incomplete data, and deliberate adversarial attacks is crucial for military applications where failure is not an option.
- **Integration with Legacy Systems and Interoperability:**

- Many defence forces operate diverse, legacy CUAS and air defence systems. Integrating new AI capabilities seamlessly into these existing infrastructures is complex and requires open architectural standards.
- Achieving interoperability among different national CUAS systems, especially within alliances like NATO, is essential for coordinated defence but challenging due to varying standards and proprietary technologies.

3.2 Opportunities

- **Enhanced Detection, Classification, and Tracking (DCT):**
- **Superior Accuracy:** AI can significantly improve the probability of detection (Pd) and reduce false alarm rates (FAR) by discerning subtle patterns across multi-sensor data, distinguishing drones from birds, balloons, or other clutter.
- **All-Weather, All-Conditions Capability:** Advanced AI models can fuse data from radar, EO/IR, acoustic, and RF sensors to maintain robust detection and tracking even in adverse weather or complex electromagnetic environments.
- **Automated Threat Assessment and Prioritisation:**
- AI can rapidly analyze drone behaviour, flight paths, and potential payloads to assess intent and assign threat levels, allowing operators to focus on the most critical targets in multi-drone scenarios.
- This reduces cognitive load and accelerates decision cycles, critical against swarm attacks.
- **Optimised Countermeasure Selection and Resource Allocation:**
- Based on threat assessment, AI can recommend or autonomously deploy the most effective and least collateral-damaging countermeasure from available effectors (e.g., jamming, kinetic, directed energy), optimizing resource use.
- In swarm attacks, AI can orchestrate multiple effectors to engage numerous targets simultaneously and efficiently.
- **Adaptive and Predictive Capabilities:**
- Machine learning models can continuously learn from new threats and operational data, adapting their detection and response strategies over time.
- AI can perform predictive analysis on potential drone launch sites, flight corridors, and attack vectors based on intelligence and environmental factors.
- **Reduced Operator Cognitive Load and Increased Efficiency:**
- By automating routine tasks and providing highly curated information, AI frees human operators to focus on strategic decision-making and high-level oversight.
- This leads to more efficient operations with fewer personnel.
- **Swarm-on-Swarm Capabilities:**
- AI is essential for developing friendly drone swarms that can autonomously detect, track, and neutralize hostile swarms, creating a new layer of defence.

4. Detailed Analysis

4.1 AI-Powered Detection, Classification, and Tracking (DCT) through Sensor Fusion

The core challenge in CUAS is reliably detecting, classifying, and tracking small, fast-moving, and often evasive UAS in complex environments. No single sensor type provides a complete solution. This is where AI-driven sensor fusion becomes indispensable.

4.1.1 The Power of Multi-Sensor Integration AI algorithms excel at integrating and interpreting data from diverse sensor modalities:

- **Radar Data:** AI can filter out clutter, identify faint drone signatures, and predict trajectories. Deep learning models, particularly Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), can process raw radar returns to distinguish between drones, birds, and other objects with high accuracy.
- **Electro-Optical/Infrared (EO/IR) Imagery:** Computer vision techniques, powered by deep neural networks, enable real-time object detection and classification, even for small drones at significant ranges. AI can enhance image quality, track drones through occlusion, and perform behavioural analysis from visual data.
- **Acoustic Signatures:** Machine learning can identify specific drone acoustic profiles, separating them from background noise. This is particularly effective for close-range detection of smaller drones.
- **Radio Frequency (RF) Analysis:** AI can identify unique communication protocols, frequency hopping patterns, and command-and-control signals, even those attempting to evade detection. It can also differentiate between legitimate and malicious RF emissions.

4.1.2 AI for Enhanced Accuracy and Reduced False Positives Traditional rule-based systems often struggle with the variability of drone threats and environmental conditions, leading to high false alarm rates. AI-powered systems learn from data, continuously improving their ability to:

- **Discriminate:** Distinguish between a DJI Mavic drone and a large bird, or between a legitimate commercial drone and a suspicious one, based on nuanced patterns across multiple sensor inputs.
- **Adapt:** Adjust detection thresholds and classification parameters based on real-time environmental data (weather, urban clutter, electromagnetic interference).
- **Predict:** Utilize historical data and current trajectories to predict future drone movements, enhancing tracking continuity and enabling proactive countermeasure deployment.

4.1.3 Edge AI for Real-time Processing For CUAS, latency is critical. Decisions must be made in milliseconds, not seconds. This necessitates **Edge AI**, where processing occurs directly on the sensor platforms or local CUAS nodes, rather than relying on centralized cloud infrastructure.

- **Reduced Latency:** Eliminates data transmission delays to a central server.
- **Improved Resilience:** Operates effectively even in disconnected or bandwidth-limited environments.
- **Enhanced Privacy/Security:** Raw data is processed locally, reducing the need for extensive data exfiltration.

> *"The ability of AI to fuse disparate sensor data – radar, EO/IR, acoustic, and RF – into a coherent, real-time threat picture is foundational," states Ross Newman, CEO at Astute Systems. "This multi-modal approach, coupled with intelligent algorithms operating at the edge, provides the robust detection and classification accuracy that traditional systems simply cannot match against the evolving drone threat."*

4.2 Autonomous Decision Support and Countermeasure Orchestration

Beyond detection, AI profoundly impacts the decision-making process and the orchestration of countermeasures against drone threats. This moves CUAS from a human-intensive, reactive system to an intelligent, proactive one.

4.2.1 Intelligent Threat Assessment and Prioritisation Once a drone is detected and classified, AI can rapidly assess its threat level:

- **Behavioral Analysis:** AI algorithms can analyze flight patterns, speed, altitude, and proximity to critical assets to infer intent (e.g., hovering over a sensitive area versus transiting).
- **Payload Estimation:** Using visual or other sensor data, AI can make educated guesses about potential payloads, elevating the threat level for weaponized or hazardous drones.
- **Origin and Destination Prediction:** Advanced AI can integrate with intelligence feeds and geographical data to predict potential launch points and intended targets, informing pre-emptive actions.

In a swarm attack, where dozens or hundreds of drones might be simultaneously engaged, AI is indispensable for:

- **Dynamic Prioritisation:** Continuously re-evaluating the most immediate and dangerous threats based on real-time data, ensuring high-value targets are addressed first.
- **Resource Allocation:** Intelligently assigning available countermeasures (jammers, kinetic effectors, lasers) to specific drones or groups of drones to maximize effectiveness and minimize collateral damage, while conserving limited resources.

4.2.2 Automated Countermeasure Selection and Orchestration AI can move beyond mere recommendation to autonomously selecting and deploying the optimal countermeasure:

- **Soft-Kill vs. Hard-Kill:** AI determines whether RF jamming, GPS spoofing (soft-kill) is sufficient or if a kinetic intercept (hard-kill) is necessary, considering factors like drone type, location, and potential collateral effects.
- **Multi-Effector Coordination:** In complex environments with multiple CUAS effectors (e.g., jammers, lasers, kinetic systems), AI can orchestrate their simultaneous or sequential deployment to achieve the desired outcome. For example, jamming a drone's control link while a laser prepares to engage a different target.
- **Adaptive Response:** If an initial countermeasure fails, AI can quickly analyze the failure and deploy an alternative, learning from the engagement to improve future responses.

4.2.3 Human-on-the-Loop vs. Human-in-the-Loop While full autonomy in lethal decision-making remains a subject of intense ethical debate, AI in CUAS can operate effectively within a "human-on-the-loop" framework.

- **Human-in-the-Loop:** Requires human approval for every decision, which can be too slow for rapid-fire swarm attacks.
- **Human-on-the-Loop:** AI systems operate autonomously but under continuous human supervision, with the ability for human operators to intervene, override, or halt operations if necessary. This balances speed with accountability.

> *"The strategic advantage of AI in CUAS lies not just in its ability to detect drones, but in its capacity to intelligently orchestrate a multi-layered defence," Ross Newman, CEO at Astute Systems, comments. "From assessing the nuanced threat of a single drone to coordinating a symphony of countermeasures against a complex swarm, AI elevates our defensive capabilities to an entirely new level of precision and responsiveness."*

4.3 Future Trends: Swarm CUAS, Adaptive Learning, and System of Systems Integration

The future of AI in CUAS is characterized by increasing autonomy, collective intelligence, and deeper integration into broader defence architectures.

4.3.1 Swarm-on-Swarm Capabilities As adversaries increasingly deploy drone swarms, the most effective countermeasure will often be an intelligent, autonomous CUAS swarm.

- **Collective Intelligence:** AI-powered CUAS swarms can coordinate their actions (detection, tracking, engagement) without central control, exhibiting emergent behaviours that are highly resilient to attack.
- **Distributed Sensing and Effects:** Each drone in a CUAS swarm can act as a sensor and an effector, providing a highly distributed and redundant defence.
- **Adaptive Tactics:** Machine learning, particularly reinforcement learning, can enable CUAS swarms to learn and adapt their engagement tactics in real-time based on the adversary's swarm behaviour.

4.3.2 Adaptive Learning and Predictive Maintenance AI models are not static; they continuously evolve.

- **Continuous Learning:** CUAS systems can be designed to continuously ingest new data from real-world engagements, simulations, and intelligence feeds to refine their detection models, threat assessment algorithms, and countermeasure strategies. This ensures they remain effective against emerging drone technologies and tactics.
- **Predictive Maintenance:** AI can monitor the performance of CUAS hardware (sensors, effectors, processing units) to predict potential failures, enabling proactive maintenance and maximizing system uptime.

4.3.3 Explainable AI (XAI) in Defence For military applications, understanding *why* an AI system made a particular decision is crucial for trust, accountability, and post-incident analysis.

- **Transparency:** XAI techniques aim to provide human-understandable explanations for AI decisions, enhancing operator confidence and facilitating regulatory compliance.
- **Validation and Verification:** XAI aids in the rigorous testing and validation of AI models, ensuring they operate as intended and do not exhibit unexpected or undesirable behaviours.

4.3.4 Modular, Open Architectures and NATO Standardisation The pace of technological change demands flexible and upgradeable CUAS systems.

- **Open Architectures:** Adopting open, modular architectures allows for easier integration of new AI capabilities, sensors, and effectors from various vendors, preventing vendor lock-in and fostering innovation.
- **API-driven Integration:** Standardized Application Programming Interfaces (APIs) facilitate seamless communication between different CUAS components and broader C2 systems.
- **NATO Standardisation:** For alliance operations, achieving common standards for AI-enabled CUAS data exchange, threat classification, and operational protocols is vital for interoperability and coordinated defence across member states. This allows for a "system of systems" approach where national CUAS assets can seamlessly collaborate.

5. Recommendations

To fully harness the potential of AI in CUAS and establish a robust defence against evolving drone threats, Astute Systems recommends the following strategic actions for defence organizations and stakeholders:

- **Prioritise Data Infrastructure and Management:**
- **Invest in Data Collection and Annotation:** Establish robust programs for collecting, curating, and accurately labeling diverse datasets of drone signatures across all sensor modalities (RF, EO/IR, acoustic, radar). This includes real-world data and high-fidelity synthetic data generation capabilities.
- **Secure Data Pipelines:** Implement secure, resilient data pipelines for the continuous ingestion, storage, and processing of CUAS operational data to feed AI models.
- **Embrace Modular, Open-Architecture CUAS Systems:**
- **Adopt Open Standards:** Mandate the use of open standards and APIs for all new CUAS procurements to ensure interoperability between different sensors, effectors, and C2 systems, facilitating seamless AI integration and future upgrades.
- **Avoid Vendor Lock-in:** Promote competition and innovation by encouraging solutions that allow for easy integration of components from multiple suppliers.
- **Invest in Edge AI and High-Performance Computing:**
- **Develop Edge Processing Capabilities:** Prioritise research, development, and procurement of CUAS systems with integrated edge AI processors capable of real-time, low-latency data analysis and decision-making in contested environments.
- **Optimise AI Models:** Focus on developing compact, efficient AI models suitable for deployment on resource-constrained edge devices without compromising performance.
- **Foster Collaboration and Knowledge Exchange:**
- **Industry-Academia-Defence Partnerships:** Establish strong collaborative frameworks between defence organizations, technology companies (like Astute Systems), and academic institutions to accelerate AI research, development, and deployment in CUAS.
- **International Cooperation:** Actively participate in international forums (e.g., NATO) to share best practices, develop common standards, and collaborate on multinational AI-enabled CUAS development programs.
- **Develop Ethical and Regulatory Frameworks for AI in CUAS:**
- **Establish Clear Guidelines:** Proactively develop national and international ethical guidelines and rules of engagement for AI-enabled autonomous CUAS systems, ensuring human oversight and accountability remain paramount.
- **Legal Scrutiny:** Conduct thorough legal reviews to ensure AI-driven CUAS operations comply with international humanitarian law and national legislation.
- **Invest in Workforce Development and Training:**
- **Upskill Personnel:** Implement comprehensive training programs for military personnel and defence contractors to develop expertise in AI concepts, data science, and the operation and maintenance of AI-enabled CUAS systems.
- **AI Literacy:** Foster a culture of AI literacy across defence organizations to ensure informed decision-making regarding AI adoption and deployment.
- **Prioritise Robustness and Adversarial AI Research:**
- **Resilient AI:** Fund research into making AI models more robust and resilient to adversarial attacks, spoofing, and evasion techniques.
- **Continuous Testing:** Implement rigorous testing and validation protocols, including red-teaming exercises, to evaluate the performance and vulnerabilities of AI-powered CUAS systems against sophisticated threats.

6. Conclusion

The proliferation of Unmanned Aircraft Systems represents one of the most pressing and rapidly evolving threats to national security and military operations worldwide. The traditional approaches to Counter-UAS, while foundational, are increasingly insufficient to contend with the sophistication, autonomy, and swarm capabilities of modern drone threats.

Artificial Intelligence is not merely an evolutionary step in CUAS technology; it is a revolutionary one. By enabling real-time, multi-sensor data fusion, highly accurate detection and classification, intelligent threat assessment, and autonomous orchestration of countermeasures, AI transforms CUAS from a reactive, human-intensive process into a proactive, adaptive, and highly efficient defensive system. The ability of AI to reduce cognitive load on operators, accelerate decision cycles, and optimize resource allocation provides a decisive strategic advantage in a rapidly changing threat landscape.

> *"The future of effective CUAS is inextricably linked to AI," Ross Newman, CEO at Astute Systems, concludes. "Those who embrace AI responsibly and strategically will gain a significant edge in protecting critical assets and personnel. Astute Systems is committed to leading the charge in developing and deploying these advanced, AI-powered solutions, ensuring our defence forces are always one step ahead of the threat."*

Astute Systems, with its deep expertise in defence technology and enterprise solutions, is ideally positioned to partner with defence organizations in navigating this complex but essential transformation. By focusing on modular, secure, and intelligent AI-driven solutions, we aim to deliver the next generation of CUAS capabilities, ensuring enhanced security and operational superiority in the face of persistent and evolving drone threats. The time to act on AI in CUAS is now; the security of tomorrow depends on it.

Get In Touch

astutesys.com

enquiries@astutesys.com

Suite 2.08, The Precinct, Brunswick Street, Fortitude Valley,
QLD 4006