THE NEW BATTLESPACE

Ash Alexander-Cooper OBE, *shines the spotlight on the evolving world of drone warfare*

For more than a century, air superiority was defined as the side with the most advanced aircraft and the best-trained pilots. That dominance was built on hardware, skill and financial might. Today, the balance has shifted. One of the cheapest devices on the battlefield can inflict very costly damage, and airspace that was once secure now requires constant vigilance against low-cost threats.

Uncrewed aerial systems (UAS) are rewriting the rules of warfare. They require no onboard pilots and no runways. They can launch from civilian vehicles, fly hundreds of miles autonomously and often remain undetected by traditional defences until impact. Data from Dedrone by Axon's report 'State of Airspace defence Today and What's Next,' confirms that the shift has moved from theory to operational reality.

In 2025, operations such as Ukraine's Spider's Web and Israel's Rising Lion confirmed that drones could suppress traditional enemy air defences, evade detection and destroy strategic assets at scale. These examples marked a turning point, proving that uncrewed systems can deliver outcomes once reserved for nation-state air forces. Since then, the ripple effects have extended well beyond active warzones. Northern European nations including Poland, Finland and Denmark have reported repeated drone incursions across their borders, exposing how easily airspace can be penetrated without a single crewed aircraft crossing national lines. Additionally, Dedrone by Axon's reporting shows that 37.5 percent of detections across Europe, the Middle East and Asia now occur at night, suggesting operators are deliberately exploiting reduced visibility to bypass conventional surveillance.

These incidents and patterns underline that the challenge is no longer contained. It is systemic and it reaches into peacetime airspace, well beyond conflict zones. We can see how drones now define the accelerated pace and precision of modern conflict. They expose the vulnerability of traditional defences and reveal their decisive tactical advantage: the ability to strike at low human and monetary cost.

The economics of drone warfare have rewritten the rules of engagement

Drone warfare has collapsed the cost balance of defence. A single explosive FPV drone, costing less than $2,000 can destroy an F-35 fighter jet worth more than $80-million without any risk of life. Few other weapons create that level of asymmetry between price and impact. When defenders rely on multimillion-dollar interceptors to counter low-cost threats, the economics of deterrence start to break down.

That imbalance endures because the market for drones is built on accessibility. Data from the report shows that most drones detected across Europe, the Middle East and Asia still come from familiar commercial ecosystems. DJI, Autel and DIY builds accounted for almost 95 percent of all detections. These platforms are affordable, easy to modify and globally available, giving hostile actors near-limitless supply and flexibility. Every year, as components become cheaper and designs more modular, that imbalance widens.

The economics of drone warfare have rewritten the rules of engagement, but its true impact lies in speed. Each new design, tactic or code modification is tested and fielded faster than traditional defence systems can adapt. What once demanded years of development can now be produced in days using commercial components and open-source software. That acceleration has transformed drones from single-purpose tools into adaptable platforms. Early commercial models depended on GPS and radio frequency (RF) and were easily jammed. New variants navigate through visual or LiDAR mapping or operate on fibre-optic tethers. This evolution is constant, erasing the distinction between prototype and deployment.

Artificial intelligence (AI) has made that cycle more precise. Generative and adversarial AI models allow operators to design and refine tactics in simulated environments before real deployment. These systems learn how to evade detection, coordinate in swarms or re-route autonomously mid-mission. Additionally, open-source AI models mean these capabilities are no longer confined to advanced militaries. Non-state actors and criminal networks can now access technologies once restricted to defence laboratories.

The consequence is two-fold: Not only has this mismatch between cost and capability reshaped the economics of defence, but it results in a cycle of innovation that initially favours offense. Every new countermeasure is immediately met by an adaptation. This constant feedback loop creates pressure on defenders, but also drives them toward more adaptive, resilient solutions that can evolve as quickly as the threats themselves.

Defending against drones begins with detecting them, but that task is becoming harder. Over 80 percent of detections in 2025 were made using RF sensors, yet RF-silent drones are increasingly common. Operators are deliberately removing or spoofing emissions to bypass traditional drone detection systems.

Modern drones can be reconfigured to operate across multiple missions. A single type of airframe might serve as a decoy, a surveillance tool or a kinetic weapon. This modularity makes each encounter unpredictable. In the past, air defence relied on large radar signatures, predictable flight paths or clear electronic emissions. Drones have erased those assumptions. They fly low, move irregularly and often mimic the radar cross-section of birds.

As a result, the RF-first approach that has long underpinned counter-UAS operations is losing reliability. The answer must lie in a combination of AI-driven sensor fusion and wide-spread drone detection networks. These detection networks are made of integrated sensor modes including RF, radar, visual, acoustics and, looking forward, chemical/bio-sensors. These sensors cannot exist only at a border, they must also encompass both human and infrastructural assets deep inside nations where drones could be deployed. These networks will enable defenders detection and shared data across allies in real-time.

SOFTWARE-DRIVEN, OPEN ARCHITECTURES ALLOW UPDATES TO BE DEPLOYED IN DAYS, NOT YEARS

The future of drone warfare will not be defined by individual drones, but by coordinated, multi-domain operations. Drones will act alongside uncrewed surface and underwater vehicles, synchronising attacks across air, sea and land. The battlefield is expanding vertically and horizontally at once.

There are four broad categories where the threat is advancing. The first is saturation and scale. Large 'mothership' drones capable of releasing dozens of microdrones mid-flight are transforming swarm warfare. Once deployed, these microdrones can operate independently or as coordinated units, overwhelming defences by volume rather than complexity.

The second is stealth and evasion. Drones built with radar-absorbing materials, low-heat propulsion and near-silent electric systems can loiter undetected for extended periods. Some navigate entirely without GPS, relying instead on visual or inertial mapping. Experimental 'cybugs' now demonstrate how miniaturised drones can infiltrate secure facilities, conducting surveillance or sabotage beyond current detection limits.

The third is miniaturization and bio-integration. Insect-sized 'cybugs' represent a new frontier in drone technology, small enough to infiltrate secure facilities through ventilation systems or open windows. Bio-hybrid drones – platforms that integrate living tissue with mechanical systems – are advancing from laboratory concept to field prototype, potentially combining biological stealth with mechanical precision. These systems can conduct surveillance or sabotage operations beyond current detection limits, exploiting their scale and biological characteristics to evade traditional countermeasures.

The fourth is cross-domain expansion. Maritime and ground-based uncrewed systems are already

being adapted for reconnaissance, sabotage and logistics support. These platforms exploit blind spots in radar and sonar coverage, using the same modular principles that make aerial drones so adaptable. These developments mark a strategic turning point. defences built for single-vector threats will fail against interconnected ones. The next wave of conflict will be shaped by integration – of sensors, command systems and mitigation tools – rather than by hardware superiority alone.

37.5% OF DETECTIONS ACROSS EUROPE, THE MIDDLE EAST AND ASIA NOW OCCUR AT NIGHT

Static systems cannot keep pace with dynamic threats. The future of airspace defence depends on flexibility. Specifically, the ability to adapt software, share information across networks, and adjust tactics as rapidly as adversaries iterate their designs. The data from 2025 shows that the forces driving this change are automation, scale, and AI-driven adaptability. Each demands a corresponding shift in how defences are built and deployed.

Software-driven, open architectures allow detection and response capabilities to evolve without replacing entire systems. Updates can be deployed in days, not years, allowing defenders to recognise new flight patterns and signal profiles before they become standard.

Networked systems at scale create shared situational awareness across units, borders and alliances. When one system detects a new threat type, that intelligence will immediately inform others. This form of distributed learning is essential to counter tactics that cross multiple domains and jurisdictions.

Finally, adaptability driven by AI closes the reaction gap. Machine-speed analysis enables systems to prioritise threats and select the appropriate countermeasure in real time. The side that automates faster will control the tempo of engagement. The future battlespace will reward agility and network scale over individual platform size. The question is no longer who owns the most advanced aircraft, but who can deploy the largest distributed networks while sensing, deciding and acting the fastest.

The evidence is conclusive. The modern threat environment is evolving faster than most defence programmes can respond. Legacy air defences were built for state-launched attacks, not decentralised actors deploying low-cost, high-impact drones. Today's battlefield is defined by autonomy, speed and saturation.

Governments and defence ministries face a stark choice. They can continue investing in closed, hardware-heavy systems that will degrade within years or they can pivot to open, networked and adaptive platforms that evolve in sync with the threat. The nations that treat this transformation as a technology race, rather than a procurement cycle, will maintain airspace control. Those that hesitate will face adversaries who can outmanoeuvre them through scale and through speed.

The next conflict won't begin with a missile. It will begin with a drone, launched cheaply, flown remotely and armed with intelligence far greater than its size suggests. The decisive factor will not be firepower – it will be the ability to adapt in real time. Defenders that grasp this reality can shift from reactive to predictive operations, building the resilience needed to secure national airspace against both present and future threats. The future of defence will belong to those who integrate intelligence, connectivity and adaptability into every layer of their security infrastructure. Drones have changed the rules of warfare. The task now is to change how we defend against them ●

Ash Alexander-Cooper OBE is VP of APAC and EMEA, Dedrone by Axon.

The future of airspace defence depends on flexibility to adapt software, share information and adjust tactics

Picture credit: Axon