Countering UAV threats

The need for integrated end-to-end solutions in an era of hybrid warfare

Digital Intelligence

BAE SYSTEMS

The rapid evolution of unmanned aerial vehicles (UAVs) and unmanned aerial systems (UAS) has **fundamentally reshaped the nature of modern conflict.** The use of commercially available drones is increasingly widespread and nations around the world are responding.

The US military, for example, is working overtime to accelerate its adoption and exploitation of drones. What's more, the UK's Strategic Defence Review makes multiple references to harnessing drones, AI-powered systems and autonomous capabilities alongside "the 'heavy metal' of tanks and artillery".

Within the context of hybrid warfare, UAVs act as low-cost, high-impact enablers across conventional, irregular, informational and cyber domains. Adversaries employ these platforms for a range of operations, often within legally ambiguous or technologically complex environments.

The role of UAVs in hybrid warfare

Hybrid warfare relies on merging traditional military tactics with irregular, informational and cyber operations to achieve strategic advantage. It is characterised by distributed and often autonomous operations, with small teams or agents exploiting legal, political and technical vulnerabilities.

The result is a highly dynamic and ambiguous operating environment to which UAVs are well suited – and which places considerable demands on defenders who must protect dispersed and critical infrastructure while maintaining operational tempo. It is therefore no surprise that, within this evolving landscape, UAVs – both military-grade and commercially available – have emerged as significant force multipliers across the dimensions of hybrid warfare.

Their accessibility, adaptability and affordability make them ideal for hybrid warfare applications. For example, they are frequently employed to conduct ISR (Intelligence, Surveillance and Reconnaissance) and targeting missions, providing near-real-time situational awareness. In many cases, UAVs are used in loitering and swarming operations, enabling adversaries to impose persistent psychological and operational pressure.

Such systems may be deployed by state or proxy actors, maintaining deniability while achieving significant operational effect. They can also be integrated with cyber and electronic attack campaigns, further amplifying disruption.

> "UAVs – both military-grade and commercially available – have emerged as significant force multipliers across the dimensions of hybrid warfare."

Responding to the hybrid UAV threat

There are several challenges associated with an effective response to the hybrid UAV threat, requiring several interconnected difficulties to be overcome.

For example, detecting small and inexpensive UAVs remains one of the most persistent operational challenges facing today's militaries. These platforms possess small radar cross-sections, produce minimal acoustic and thermal signatures, and often operate at low altitudes within ground clutter. Many are capable of autonomous flight with little or no radio frequency (RF) emission, making traditional detection methods unreliable.

Urban and vegetated terrain further complicate detection, as buildings and foliage create blind spots and signal reflections that mask UAV movement. Adverse weather, restricted lines of sight and interference from birds or civilian activity introduce additional uncertainty.

A connected challenge is distinguishing between hostile and civilian UAVs. Attribution and intent are major challenges, as it is often unclear who controls a UAV and for what purpose it is being used, particularly in grey-zone or proxy scenarios. The compressed decision timelines of UAV operations further complicate matters, as engagements frequently occur in seconds, leaving little room for deliberation.

Effective attribution therefore requires a layered approach that draws on multiple sources of corroborating information. No single sensor or data point can provide reliable classification. Instead, systems must combine data such as flight paths, geofencing and airspace authorisations, cooperative transponder signals, RF fingerprinting and command-link analysis.

Behavioural analysis, including loitering patterns and approach vectors, can indicate hostile intent, while comparison against intelligence databases of known operators provides additional assurance. Technological capability must be matched with legal and procedural safeguards to minimise the risk of misidentification and collateral damage. In hybrid or ambiguous environments, where attribution is uncertain, automation and well-defined legal frameworks are essential to ensuring both operational effectiveness and accountability.

Legal and rules of engagement (ROE) considerations introduce further complexity, particularly in civilian or contested airspace. Operations must balance the need for timely action with adherence to international and domestic law. Effective response also demands coordination across multiple services, agencies and jurisdictions, a process that can be slow and disjointed.

Procurement and sustainment of countermeasures pose additional difficulties, as UAV technology continues to evolve rapidly within the commercial sector. Forces must constantly adapt their training, doctrine and systems to keep pace with this evolution. Only through automation, intelligence fusion and scalable systems can defenders hope to respond at the required speed and precision.

> "Technological capability must be matched with legal and procedural safeguards to minimise the risk of misidentification and collateral damage."

Limitations of Electronic Warfare

Electronic warfare (EW) of course offers a means of countering the UAV threat. However, EW presents limitations in dense or complex operational environments.

Multipath propagation and electromagnetic clutter reduce predictability, while the proximity of civilian systems creates difficulties in isolating targets without causing unintended interference. Legal restrictions on spectrum use in populated areas further constrain the employment of broad-spectrum jamming or denial measures.

Urban landscapes introduce physical barriers that create shadow zones where EW signals are ineffective. Meanwhile, many modern UAVs are equipped with anti-jamming technologies or can operate autonomously, rendering simple jamming measures inadequate.

For these reasons, EW must form only one component of a broader, integrated defensive system. A combined approach – incorporating kinetic, optical and cyber elements – is essential to maintaining resilience against adaptive and autonomous threats.

Effective Counter-UAV practices

With all these challenges in mind, the most effective counter-UAV systems adopt a layered defence approach that integrates detection, command and control (C2) fusion and a spectrum of defeat mechanisms.

Detection involves radar tuned to identify small UAS', supplemented by passive RF sensing, electro-optical and infrared (EO/IR) imaging and acoustic arrays as part of a unified multi-sensor system. These data streams are then fused within an AI-enabled C2 network that allows for rapid classification and prioritisation of threats – thereby greatly enhancing situational awareness.

Defeat mechanisms must include both non-kinetic and kinetic options. Non-kinetic methods such as RF and command-link disruption, global navigation satellite system (GNSS) spoofing or denial, and cyber interference can neutralise UAVs without physical destruction. Kinetic responses – such as interceptors, directed-energy weapons or automated gun systems – are used where non-kinetic options are insufficient or where collateral risk is acceptable.

Automation and integration are vital to success. By reducing human decision latency and providing robust control mechanisms, integrated systems ensure that operators can act with speed, confidence and precision while adhering to established rules of engagement.

> "Urban landscapes introduce physical barriers that create shadow zones where EW signals are ineffective."

BAE Systems Anti Threat System: End-to-end counter-UAS capability

The BAE Systems Anti-Threat System (BATS) developed by BAE Systems, offers a solution to the modern defence landscape. It provides an integrated, end-to-end capability to detect, classify and neutralise UAVs through both kinetic and non-kinetic effectors.

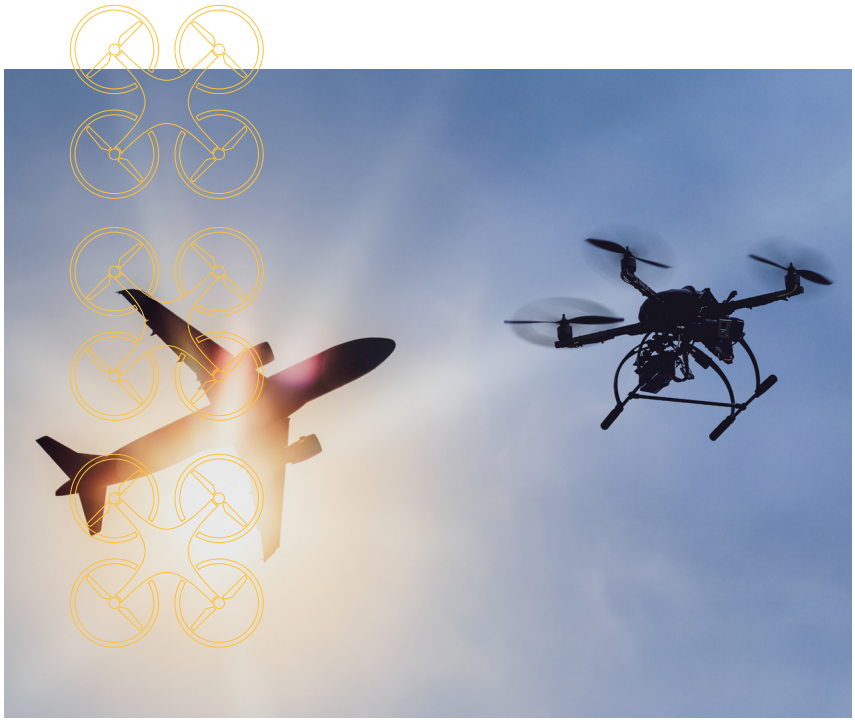
BATS is purpose-built to meet the demands of hybrid warfare and complex operational environments. It delivers a truly end-to-end counter-UAS (C-UAS) capability by integrating detection, analysis and engagement into a single, cohesive platform – combining multi-sensor detection, advanced artificial intelligence for classification, and both kinetic and non-kinetic defeat mechanisms within a single architecture.

The system can deliver a complete spectrum of CUAS capability, reducing operator workload and decision-making time, while ensuring compliance with legal and safety requirements.

Key features include:

- **Sensor fusion:** The system combines radar, EO/IR, acoustic and passive RF sensors to provide comprehensive detection and tracking.
- **AI-driven command and control:** Artificial intelligence enables real-time classification, prioritisation and engagement recommendations.
- **Non-kinetic options:** The system offers precise RF and GNSS denial measures to neutralise UAVs without physical destruction.
- **Kinetic capability:** Where required, the system can deploy kinetic interceptors or directed-energy weapons for immediate neutralisation - all while maintaining a human in-the-loop.
- **Scalable deployment:** BATS can be configured for fixed-site, mobile or expeditionary operations, enabling flexibility across land, sea and urban domains.
- **Network integration:** The system can integrate with most air defence and command networks, supporting coordinated, multi-domain operations.

By uniting these capabilities, BATS can provide rapid, precise and legally compliant counter-UAS effects. Its modular and adaptive design help to maintain its effectiveness against both current and emerging UAV technologies.



Conclusion

The UAV threat environment is evolving rapidly, blurring the distinction between civilian and military technologies and demanding a new generation of countermeasures. Isolated or manually operated systems are no longer sufficient to cope with the speed, diversity and ambiguity of hybrid UAV operations.

The BAE Systems Anti-Threat System offers a fully integrated, sensor-to-effector solution that unites detection, decision and defeat within a single operational framework. By leveraging automation, artificial intelligence and multi-sensor fusion, BATS helps armed forces and security operators to act decisively, efficiently and within legal boundaries.

In an age where UAVs are redefining the tempo and transparency of conflict, BATS represents the next evolution in hybrid warfare defence: an adaptable, resilient and intelligent system built for the realities of the modern battlespace.

> "By leveraging automation, artificial intelligence and multi-sensor fusion, BATS helps armed forces and security operators to act decisively, efficiently and within legal boundaries."

We are Digital Intelligence

Digital Intelligence is home to over 4,500 digital, cyber and intelligence experts across 13 countries. We operate at the cutting edge of digital innovation and at the heart of organisations that keep vital infrastructure running, national security protected and armed forces prepared. Digital Intelligence is part of BAE Systems, which has a rich heritage in delivering technology today to protect our tomorrow. BAE Systems partners with governments, communities and companies large and small to design, build and maintain advanced defence and security solutions.

BAE Systems Digital Intelligence
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom
T: +44 (0) 330 158 3627

BAE Systems Digital Intelligence
Malta Office Park
ul. Abpa A. Baraniaka 88
Poznan
61-131
Poland
T: +44 (0) 330 158 3627

BAE Systems Digital Intelligence
Level 2
14 Childers St
Canberra
ACT 2601
Australia
T: +61 (0) 2 9053 9330

BAE Systems Digital Intelligence
Level 28, Menara Binjai
2 Jalan Binjai
Kuala Lumpur
50450
Malaysia
T: +60 327 309 390

BAE Systems, Surrey
Research Park, Guildford,
Surrey, GU2 7RQ, UK

E: learn@baesystems.com

W: baesystems.com/digital

linkedin.com/company/baesystemsdigital

@BAESystemsDigi

BAE SYSTEMS