NTS

CUxS CHRONICLE

17 JULY 2025

CUAS IN THE URBAN ENVIRONMENT

NAVIGATING COMPLEXITY

In recent years, the proliferation of small unmanned aerial systems (sUAS) has introduced a significant threat in urban environments. These threats range from criminal uses such as smuggling and surveillance, to terrorist applications involving improvised explosive devices (IEDs), and military intelligence, surveillance, and reconnaissance (ISR) missions. The relative affordability and accessibility of drones have enabled both state and non-state actors to exploit their capabilities, especially in the cluttered and densely populated urban terrain. Adding to this complexity, the increasing use of UAS by commercial entities such as Amazon for logistics and delivery services further congests the low-altitude airspace, complicating efforts to distinguish between legitimate and malicious drone activity.

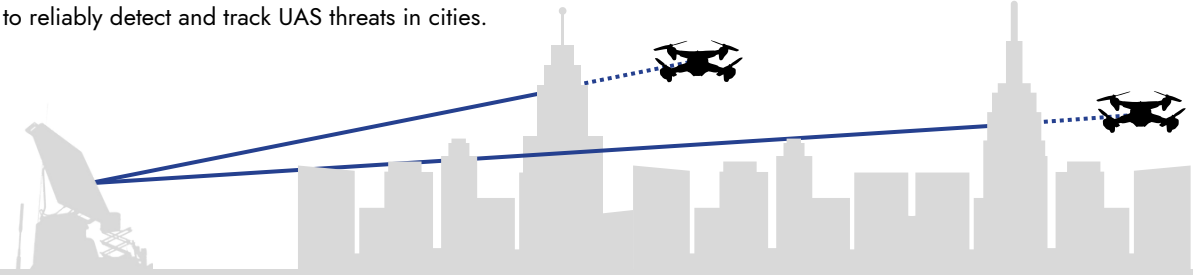
As a result, Counter-Unmanned Aircraft Systems (CUAS) have emerged as a critical capability for safeguarding military operations, ensuring the security of law enforcement missions, and protecting vital urban infrastructure such as airports, power plants, and government buildings. However, implementing CUAS in urban areas presents a multi-dimensional challenge. The dense physical and electromagnetic terrain, legal and ethical constraints, and risks of collateral damage require an integrated, nuanced approach to drone defense. The rise of commercial drone operations only heightens the need for advanced CUAS strategies that can differentiate between benign and hostile UAS in real time.

RADAR LIMITATIONS IN THE URBAN JUNGLE

Urban landscapes pose severe challenges to traditional radar systems used for drone detection. Buildings, bridges, power lines, and other infrastructure form an intricate three-dimensional maze that acts as terrain masking. These obstacles obstruct the line-of-sight paths essential for accurate radar detection and tracking.

Drones, particularly small, low-flying quadcopters, can maneuver through alleys, under bridges, and between buildings, exploiting the natural cover provided by urban architecture to avoid detection. Moreover, these structures contribute to multipath reflections, where radar signals bounce off surfaces unpredictably, creating a noisy environment filled with false echoes and ghost targets.

Additionally, the radar cross-section (RCS) of small drones is minimal, often comparable to that of birds or debris. This makes distinguishing them from background clutter difficult, leading to frequent false positives and reducing operator trust in automated systems. These radar limitations necessitate alternative or complementary sensor systems to reliably detect and track UAS threats in cities.



EW CHALLENGES IN AN RF-SATURATED ENVIRONMENT

Urban environments are not only visually and physically complex but are also saturated with electromagnetic (EM) emissions. With Wi-Fi routers, Bluetooth devices, 5G signals, cellular networks, and thousands of Internet-of-Things (IoT) devices operating simultaneously, the electromagnetic spectrum in cities is densely occupied.

Electronic warfare (EW) systems tasked with detecting and disrupting drone communications face significant obstacles in such RF-rich environments. Signal deconfliction becomes a primary challenge—EW systems must identify and target drone control or telemetry signals without inadvertently jamming or interfering with legitimate users. This is particularly difficult when drones operate using commercial frequency bands (e.g., 2.4 GHz, 5.8 GHz) that are also used by countless civilian devices.

Moreover, direction finding (DF) capabilities, which rely on measuring the angle of arrival of RF signals, become unreliable in urban areas. RF signals reflect and refract off surfaces, causing significant distortion and making it nearly impossible to localize a source accurately. These issues contribute to high false-positive rates and reduce the effectiveness of RF-based CUAS systems in cities.

THE RISKY BUSINESS OF DEFEAT MECHANISMS

Defeating a rogue drone in an urban area is not as straightforward as it might be in an open environment. Non-kinetic options like RF jamming are attractive due to their relatively low risk of physical damage, but they are fraught with unintended consequences. Jamming can interfere with GPS signals, disrupt Wi-Fi networks, and even affect emergency communications systems—posing risks to public safety and potentially violating regulatory constraints.

The legal and ethical landscape further complicates the use of jamming technologies. In many jurisdictions, the use of RF jamming is strictly regulated or outright prohibited outside of military operations. Thus, deploying these tools in populated areas requires careful coordination and often special legal authority.

Kinetic defeat mechanisms—such as net guns, shotgun shells, or interceptor drones—introduce their own set of risks. A disabled drone falling from the sky can injure civilians or damage property. Even if precision is achieved, any misfire or secondary damage could have serious legal and reputational consequences. The use of force in civilian areas also invites scrutiny under national and international laws, making the selection and employment of defeat mechanisms a high-stakes decision.

OPERATIONAL IMPLICATIONS AND BALANCING

Given the layered complexity of CUAS operations in urban areas, a one-size-fits-all solution is not viable. Success demands the use of precision tools operated by highly trained personnel who understand the technical, legal, and tactical nuances of urban CUAS missions.

A key operational approach is the fusion of multiple sensor modalities—optical cameras, acoustic arrays, RF detectors, and radar systems. Each sensor type has its limitations, but when combined, they can provide a more comprehensive and accurate detection picture, reducing the likelihood of false alarms and missed threats.

Furthermore, the development and enforcement of clear policy frameworks are essential. These should delineate authority, define rules of engagement, and set boundaries for the use of defeat mechanisms in urban areas. Public education and awareness campaigns can also help reduce panic and build trust when CUAS operations are visible or impactful to civilians.

FAA & CUAS

The Federal Aviation Administration (FAA) continues to face significant hurdles in implementing Remote Identification (Remote ID) for Unmanned Aircraft Systems (UAS), a foundational capability intended to support safe and accountable drone operations in the national airspace. While Remote ID is critical for enabling law enforcement, regulators, and the public to identify and track drones operating in shared airspace, compliance delays, technological limitations, and legal challenges have slowed its rollout. These issues complicate both the legislative framework and enforcement mechanisms surrounding UAS use in the public domain. Although the FAA is the lead agency, effective implementation of Remote ID inherently overlaps with the Federal Communications Commission (FCC), given the reliance on spectrum management, data transmission standards, and interference mitigation—making this a joint regulatory challenge that mirrors the dual-agency responsibility.

A similar cross-domain overlap exists within the Department of Defense (DoD), where Counter-UAS (CUAS) operations are recognized as both an Air and Missile Defense issue and a Signal/Electronic Warfare (EW) challenge. In dense urban environments—where the airspace is shared among commercial drones, manned aircraft, and critical infrastructure such as airports—this multidimensional problem becomes even more pronounced. Major metropolitan areas are often co-located with large airports, elevating the urgency for robust CUAS solutions capable of discriminating between benign and hostile UAS while avoiding disruption to civilian aviation and communications. This operational complexity reinforces the need for harmonized policies and interoperable technical frameworks across civil and defense agencies to ensure UAS accountability and public safety.

CONCLUSION

Counter-drone operations in urban settings are more than a technical challenge; they represent a confluence of tactical, legal, and ethical complexities. As drones become increasingly integrated into both benign and malicious activities, urban CUAS operations must evolve in both sophistication and responsibility.

Looking ahead, the integration of AI and machine learning for adaptive threat detection and classification will be vital. These tools can help filter noise, reduce false positives, and enhance real-time decision-making. Low-collateral defeat mechanisms—such as high-precision directed energy weapons or geo-fencing protocols—will also play a critical role.

Ultimately, effective CUAS operations in urban environments will hinge on collaboration across government agencies, industry innovators, and academic institutions to ensure safety, legality, and public trust in the systems designed to protect them.