DRONESHIELD

# CUAS FACTBOOK

8TH EDITION

# Contents





# Introduction

The rapid proliferation of unmanned aircraft systems (UAS), commonly known as drones, has revolutionized numerous sectors, including agriculture, logistics, infrastructure protection, surveillance, and military operations.

While UAS technologies offer significant advantages, their widespread availability and growing technical capabilities have introduced critical safety and security risks. Malicious actors can weaponize drones or use them for espionage, smuggling, or disruption of essential services – posing threats to national security, public safety, and critical infrastructure. Additionally, careless and clueless drone pilots pose serious risks to the national airspace, endanger the public, and disrupt vital operations.

In response to the evolving threat landscape, Counter-Unmanned Aircraft Systems (CUAS) have become an essential component of modern security frameworks. These systems are designed to detect, track, identify, and mitigate unauthorized or hostile UAS activities. Leveraging a combination of radio frequency (RF) sensors, radar, electro-optical/infrared (EO/IR) imaging, acoustic sensors, and electronic countermeasures, CUAS technologies operate across complex operational environments.

# Understanding UAS Types and Capabilities

UAS are categorized by the U.S. Department of Defense and other allied military organizations into five standardized groups. These classifications are based on a combination of weight, operating altitude, and airspeed, serving as a framework for determining UAS roles, performance expectations, and countermeasure strategies.

These groupings help military, law enforcement, and security stakeholders assess risk levels and tailor CUAS responses to the threat profile presented by each drone.

## Group 1

*Representative image*

**Common Examples**

DJI Mavic | Parrot Anafi | Skydio X2 | Hobbyist and commercial quadcopters

**Typical Chacteristics**

- Weight: <20lbs (9kg)
- Operating Altitude: < 1,200ft AGL
- Airspeed: < 100 knots
- Propulsion: Electric or small gas engines
- Launch/Recovery: Hand-launched or portable systems

**Operational Use**

- Typically used for short-range ISR, hobbyist activities, public safety support, or criminal and terrorist surveillance due to their small size and accessibility
- Despite limited endurance and payload, they can be difficult to detect
- Commonly used in urban environments

## Group 2

*Representative image*

**Common Examples**

ScanEagle | Flexrotor | SIC5 | PDW C100 | Puma LE | RQ-11 Raven

**Typical Chacteristics**

- Weight: 21-55lbs (9-25kg)
- Operating Altitude: < 3,500ft AGL
- Airspeed: < 250 knots
- Propulsion: Gasoline or diesel-powered
- Launch/Recovery: Portable catapults or runway-independent

**Operational Use**

- Often fielded by tactical military units for extended ISR missions
- Offer improved endurance and sensor capability compared to Group 1, while still retaining mobility and ease of use
- May also be used for border surveillance, perimeter monitoring, and environmental assessments





## Group 3

*Representative image*

**Common Examples**

RQ-7B Shadow | Tier II/STUAS

**Typical Chacteristics**

- Weight: < 1,320lbs (< 600kg)
- Operating Altitude: < 3,500ft AGL
- Airspeed: < 250 knots
- Propulsion: Gasoline or diesel-powered
- Launch/Recovery: Portable catapults or runway-independent

**Operational Use**

- Bridges the gap between tactical and strategic drone operations
- Capable of carrying sophisticated ISR payloads and often operate from fixed forward operating bases
- Due to their higher altitude and loiter time, they are used both in military operations and persistent border or infrastructure surveillance

## Group 4

*Representative image*

**Common Examples**

Fire Scout (MQ-8B, RQ-8B) | Predator (MQ-1A/B) | Sky Warrior ERMP (MQ-1C)

**Typical Chacteristics**

- Weight: > 1,320lbs (> 600kg)
- Operating Altitude: Typically, < 18,000 feet AGL
- Airspeed: Variable
- Propulsion: Turboprop or piston
- Launch/Recovery: Runway Required

**Operational Use**

- Long-endurance platforms used primarily by the military for ISR, target acquisition, and kinetic strike missions
- Can operate in controlled airspace and carry sensors and precision-guided munitions
- Their size and persistent capability make them high-priority targets for adversarial CUAS systems

## Group 5

*Representative image*

**Common Examples**

MQ-9 Reaper | RQ4 Global Hawk

**Typical Chacteristics**

- Weight: > 1,320lbs (> 600kg)
- Operating Altitude: > 18,000ft AGL
- Airspeed: Variable (typically high-subsonic)
- Propulsion: Turboprop or jet
- Launch/Recovery: Traditional runway

**Operational Use**

- Represents the most capable systems in terms of endurance, altitude, and payload capacity
- Used for deep ISR, electronic warfare, and long-range strike missions, often as part of joint or multi-domain operations
- Integrated into national and theater-level air operations and require extensive airspace coordination

INTRODUCTION

# Understanding Other Types of UxS and Capabilities

Unmanned Systems (UxS) are not limited to the air. Several types of vehicles, including Unmanned Underwater Vehicles (UUVs), Unmanned Ground Vehicles (UGVs), and Unmanned Surface Vehicles (USVs), are also used in a variety of operating environments.

## Unmanned Underwater Vehicles – Examples

### Iver3

**L3Harris OceanServer**


**Characteristics**

- Operational Use: Coastal surveys, research, defense
- Weight: 85lbs (38.5kg)
- Max. Depth: 328ft (100m)
- Max. Speed: 4 knots
- Endurance: 8-14hrs
- Sonar: Side-scan sonar, optional forward-looking sonar

### Bluefin-9

**Bluefin Robotics**


**Characteristics**

- Operational Use: Mine hunting, underwater surveys
- Weight: 154lbs (70kg)
- Max. Depth: 656ft (200m)
- Max. Speed: 6 knots
- Endurance: Up to 12hrs
- Sonar: Side-scan sonar, optional synthetic aperture sonar

### REMUS 100 AUV

**Hydroid (Kongsberg Maritime)**


**Characteristics**

- Operational Use: Mine countermeasures, hydrographic surveys
- Weight: 82lbs (37kg)
- Max. Depth: 328ft (100m)
- Max. Speed: 5 knots
- Endurance: Up to 12hrs
- Sonar: Side-scan sonar, optional forward-looking sonar

### Gavia

**Teledyne Marine**


**Characteristics**

- Operational Use: Geophysical surveys, environmental monitoring
- Weight: 110-154lbs (50-70kg)
- Max. Depth: 1640ft (500m)
- Max. Speed: 3 knots
- Endurance: 4-5hrs
- Sonar: Side-scan sonar, sub bottom profiler

## Unmanned Ground Vehicles – Examples

### TALON

**QinetiQ**


**Characteristics**

- Operational Use: EOD, Chemical, Biological, Radiological, Nuclear, and Explosives (CBRNE) detection, reconnaissance
- Weight: 115lbs (52kg)
- Max. Speed: 5.2mph
- Range: 1km

### PackBot 510

**Teledyne FLIR**

**Characteristics**

- Operational Use: EOD, DBRNE detection, reconnaissance
- Weight: 65lbs (29.5kg)
- Max. Speed: 5.8mph
- Range: 800m

### FirstLook

**Teledyne FLIR**

**Characteristics**

- Operational Use: Military combat support, rescue operations
- Weight: 5.2lbs (2.4kg)
- Max. Speed:3.4mph
- Range: 200m

### Axon Robotics Ripsaw

**Howe & Howe Technologies**

**Characteristics**

- Operational Use: Military combat support, search & rescue
- Weight: 9,000lbs (4,082kg)
- Max. Speed: 65mph
- Range: 300mi

## Unmanned Surface Vehicles – Examples

### MANTAS T12

**MARTAC Systems**

**Characteristics**

- Operational Use: Surveillance, mine countermeasures
- Length: 12ft (3.6m)
- Max. Speed:  25 knots
- Endurance: 20+ hrs

### C-Worker 4

**L3Harris**

**Characteristics**

- Operational Use: Coastal surveys, environmental monitoring
- Length: 13.1ft (4m)
- Max. Speed: 5.5 knots
- Endurance: 48hrs

### SR-Endurance

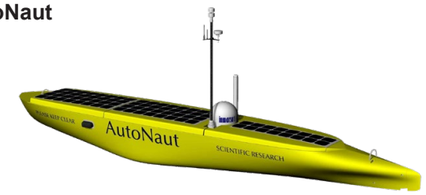
**SeaRobotics**

**Characteristics**

- Operational Use: Hydrographic surveys, water quality monitoring
- Length: 23ft (7m)
- Max. Speed: 6 knots
- Endurance: 30+ days

### AutoNaut

**AutoNaut**




**Characteristics**

- Operational Use: Ocean research, environmental monitoring
- Length: 16.4ft (5m)
- Max. Speed: 4 knots
- Endurance: Months

### Z-Boat 1800

**Teledyne Marine**

**Characteristics**

- Operational Use: Bathymetric surveys, inspection
- Length: 5.9ft (1.8m)
- Max. Speed: 5 knots
- Endurance: 3 hours

### Sea Baby

**Ukrainian Government**


**Characteristics**

- Operational Use: Kinetic attack with armaments including explosive warhead (up to 850kg) or 6x RPV-16 thermobaric grenade launch
- Length: 19.7ft (6m)
- Max. Speed: 90km/h
- Endurance: 1,000km range





# What is Counter-UAS?

CUAS encompasses a suite of technologies and strategies designed to detect, track, identify, and mitigate threats posed by UAS.

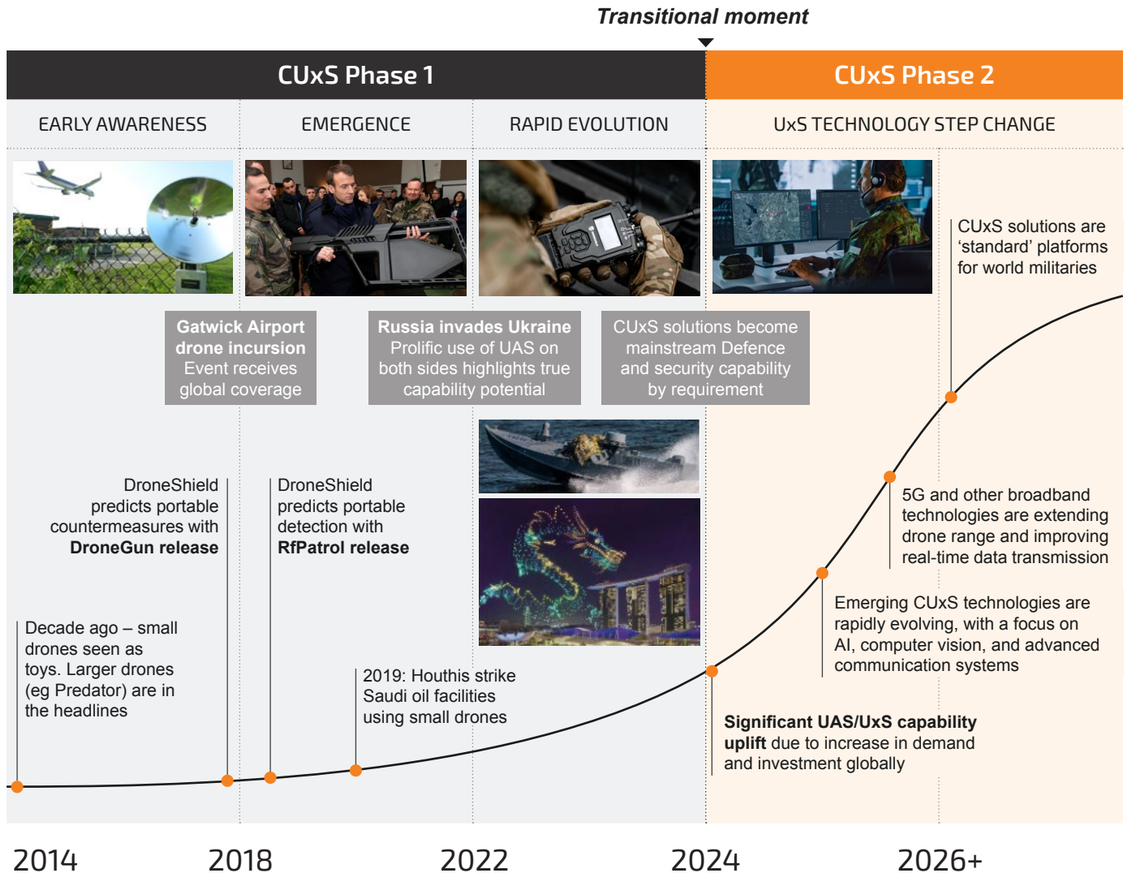
These solutions are critical for safeguarding airspace against unauthorized or malicious drone activities, which can range from surveillance and smuggling to direct attacks on infrastructure or civilians.

## Importance of CUAS in Modern Defense and Security

As drones become more prevalent, the need for CUAS solutions has grown. CUAS technologies are essential for protecting military, national security, and public safety. They provide a layered defense mechanism that can adapt to various threat levels and operational environments.

## The Future of UxS and CUxS Technology

The next few years will see even greater growth in the sophistication of drone technology, which in turn will eventuate in CUxS innovation to match.



# The Drone Threat Landscape

## Evolution of Commercial and Military UAS

Drones have evolved from simple hobbyist devices to sophisticated tools used in various sectors, including agriculture, logistics, surveillance, and warfare. Commercial drones have become more accessible, while military drones have advanced capabilities, leading to increased concerns about potential misuse.

## Common Threat Scenarios

### Intelligence, Surveillance, and Reconnaissance (ISR)

Drones can gather sensitive information, compromising security concerns

### Weaponized Drones

Equipped with explosives or firearms, drones can carry out targeted attacks

### Swarms

Coordinated groups of drones aimed at overwhelming defense systems

### Cyber Payloads

Drones can carry devices to disrupt communications or networks

### Smuggling and Contraband

Drones are used to transport illegal goods across borders or into prisons

### Airspace Interference

Unauthorized drones can disrupt airport operations

### Public Safety and Event Disruption

Drones can pose risks at public gatherings, including stadiums, VIP events, and parades

# Notable UAS Incidents

The dangers posed by drones are not confined to military theaters. Global headlines have documented drone incidents involving criminal activity, interference with emergency services, and attacks on critical infrastructure.

*Ongoing*

### Russia-Ukraine Conflict

Ukrainian drones have been used to strike oil refineries, armored vehicles, and enemy positions with precise payload delivery. Psychological operations and cyber infiltration via drone proximity have emerged as key tactics

*Ongoing as of 2023 / Southern U.S. Border*

### Border Surveillance

Human smugglers are increasingly using drones as of 2023 to surveil U.S. Border Patrol agents along the southern border, enhancing their ability to avoid detection and coordinate illegal crossings

*2021-2023 / Georgia, U.S.*

### Contraband Delivery

Two individuals were indicted in 2023 for using drones between 2021 and 2023 to smuggle illegal drugs and contraband into federal and state correctional facilities across Georgia

*2020 / Middle East*

### U.S. Troops Attacks

National Guard units in the Middle East faced sustained drone attacks involving improvised explosive devices with 3D-printed components

*2018-2019 / UK*

### Gatwick Airport

Multiple UAS sightings disrupted airport operations, affecting over 140,000 passengers and canceling 1,000 flights. Additional drone activity months later caused renewed shutdowns and diversions

*2025 / California, U.S.*

### Aviation Incident

A Culver City man agreed to plead guilty for a 2025 incident in which he recklessly crashed a drone into a firefighting aircraft during the Palisades fire response operation

*2022 / Maryland, U.S.*

### Stadium Incident

A Maryland man faced federal felony charges for illegally operating a drone over M&T Bank Stadium during the 2022 Baltimore Ravens NFL season opener, violating restricted airspace

*2020 / Azerbaijan*

### Nagorno-Karabakh Conflict

Both Armenia and Azerbaijan employed loitering munitions and kamikaze drones. Turkish-supplied Bayraktar TB2 drones proved highly effective, including future drone warfare doctrine

*2019 / Saudi Arabia*

### Saudi Aramco Oil Field Attacks

UAS swarms struck the Abqaiq and Kurais oil processing facilities, temporarily halting production and cutting global supply by 5%

**Visit DroneShield's UAS incidents database to stay updated on drone-related news**





# Risks to National Security, Public Safety, and Critical Infrastructure

The proliferation of UAS presents a complex and evolving risk environment. These risks are not limited to physical attacks. They encompass a range of disruptive and asymmetric threats that challenge existing security doctrines, infrastructure resilience, and public safety protocols.

## National Security Risks

UAS platforms can exploit gaps in attribution and response mechanisms if they:

- Emit small radar signatures
- Are low cost and modular in design
- Operate autonomously or in swarms
- Perform reconnaissance missions prior to a planned attack

## Public Safety Concerns

Drones can be easily operated by bad actors to:

- Surveil or disrupt large public gatherings
  - Sporting events
  - Concerts
  - Political demonstrations
- Put urban environments at risk via harmful payload delivery
- Cause collateral damage
- Stress public resources or emergency response deployment
- Cause panic or the erosion of public trust in safety systems

Regarding the reported use of fiber-optic cables to control drones, there are significant limitations on their use, including entanglement of the lines to each other and trees, buildings, etc. (especially in adverse weather conditions), as well as the weight of the cables. AI drone deployments and counter-UAS responses are still the most prevalent and common forms of drone warfare.

## Risks to Critical Infrastructure

Critical infrastructure – including energy grids, airports, seaports, telecommunication networks, and correctional facilities – are highly vulnerable to aerial surveillance, disruption, and sabotage via UAS. These systems, often geographically dispersed and lightly guarded, are attractive targets due to the outsized impact a successful attack could generate.

Drones may be used to:

- Survey vulnerabilities through persistent overhead ISR
- Deliver payloads to damage infrastructure or equipment
- Interfere with communications and operational control systems
- Compromise data integrity through cyber-physical convergence

The low barrier to entry for using UAS to probe or impact critical systems adds urgency to the need for both regulatory and technical countermeasures.

# The Role of AI in Proliferating the Drone Threat

Artificial Intelligence (AI) is often used broadly when referring to autonomous or semi-autonomous drones. However, it can refer to various technical aspects:

- Machine Learning (ML) algorithms used for object or target recognition
- Computer Vision to enable situational awareness
- Path planning and navigation systems
- Swarm intelligence for coordinated drone operations
- Natural language processing to allow basic human-drone interaction
- Decision-making algorithms that support tactical choices

## Evolving Use Cases

AI's impact on drone capabilities is progressing into increasingly specialized use cases.

Key advancements include:

- Autonomous navigation and obstacle avoidance
- Target recognition and tracking
- Swarm technology
- Real-time decision making in combat environments
- Edge computing and real-time data processing

The evolution of consumer-grade technologies, into military applications illustrates the growing intersection between commercial and military sectors.





## Key Challenges: AI on the Battlefield

1. **Ethical Considerations:** Use of autonomous weapons raises serious moral questions about machines making life-or-death decisions without human oversight. Human-in-the-loop (or "human-armed") models are often preferred to retain oversight.

2. **Reliability and Robustness:** AI systems can behave unpredictably or fail in unexpected ways, which poses significant risks in high-stakes combat situations

3. **Adversarial Attacks:** AI systems may be vulnerable to jamming, spoofing or cyber attacks by enemy forces, potentially compromising drone operations

4. **Complex Decision-Making:** Battlefields are chaotic environments requiring nuanced judgments that current AI may struggle with

5. **Legal and Regulatory Ambiguity:** The use of AI-enabled drones in warfare faces unclear international laws and potential arms control agreements

## Drone AI in Ukraine

In current conflicts such as the war in Ukraine, the majority of drones are typically controlled by humans via First Person View (FPV) systems. These drones, while sometimes augmented with basic automation features, largely rely on direct human control rather than advanced AI for navigation and decision-making. Despite this, AI drones still play a role in the region.

**Saker Scout**

- Uses AI for target recognition
- Although its primary function isn't detailed as terrain tracking, its ability to identify targets likely involves terrain analysis as part of its operational functionality

**ST1 Drone**

- Designed primarily for landmine detection
- Equipped with sophisticated sensors and AI for detecting and mapping land mines–capabilities that could be adapted for terrain tracking

*Note: GNSS signals are often unreliable or unavailable in contested areas of Ukraine, limiting autonomous navigation and reinforcing reliance on manual control.*

# CUAS Operational Concepts

## The CUAS Kill Chain

### 01 | Detect

Identify the presence of a drone using various sensors

Depending on system configuration and capabilities, detection may report any object in view or may only alert the operator of objects deemed to be considered UAS.

### 02 | Locate / Track

Monitor the drone's movement to assess its trajectory and potential threat

- A ***location*** is a static estimated report or display of where a GCS or UAV is located at a given moment.
- A ***track*** is a compilation of location reports over a period of time. Tracks can be displayed for GCS and/or UAVs.

### 03 | Classify / Identify

Determine the type of drone and its intent

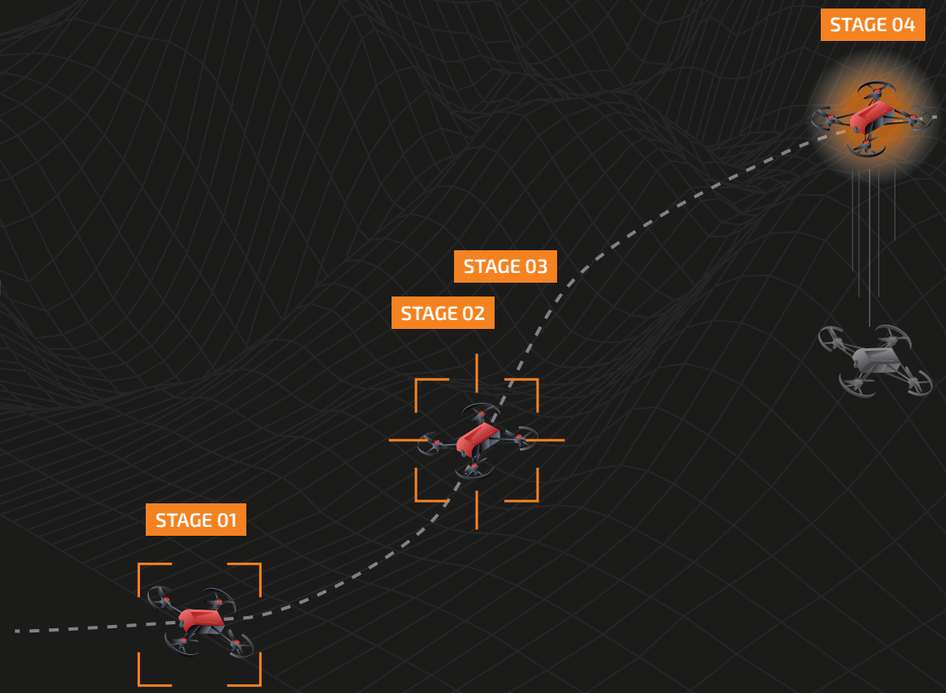
- ***Classification*** is the assignment based on high-level categories such as UAS type, group, manufacturer, and/or specific communication protocol.
- ***Identification*** is the assignment based on physical address of its modem, and exact make/model or UAS.

### 04 | Mitigate

Neutralize the threat through appropriate countermeasures

- ***Mitigate*** describes the methods used to remove or reduce the threat posed by a UAS. These methods include jamming, spoofing, or kinetic attacks.
- Mitigation may also include any capability of action associated with finding the sUAS operator and having that person safety land the sUAS, which would likely be permissible if the underlying detection system can be lawfully operated with law standards and requirements.

*Source: Department of Homeland Security, CUAS Tech Guide*





## Overview of Operational Layers

### Strategic

Long-term planning and policy development for CUAS deployment; this includes training, tabletop exercises, and collaboration with internal and external security stakeholders

### Operational

Coordination of CUAS resources and tactics across regions or sectors

### Tactical

Immediate response to drone threats in specific locations

## Threat Assessment and Rules of Engagement in CUAS

Assessing the threat level of a drone involves analyzing its behavior, payload, and proximity to sensitive areas. Rules of Engagement dictate the appropriate response, balancing the need for security with legal and ethical considerations.

# CUAS Technologies

## DETECTION SOLUTIONS

Image

*DroneShield's body-worn drone detection device, RfPatrol Mk2*

## Radio Frequency

Radio Frequency (RF) is considered the foundational layer of CUAS detection solutions.

RF passively scans and monitors the spectrum for known drone communication protocols and signals between drones and their controllers.

RF sensors are typically passive and do not broadcast or transmit. This allows RF counter-drone solutions to operate without causing any interference with other communications on the network or in the operational area.

RF-based solutionss offer other desirable features in addition to their passive advantage. Required features will depend on threat profile, and the following factors should be considered when evaluating RF solutions:

- A large, upgradeable RF signature library or detection engine to provide a high probability of detection and low false alarm ratios
- Ability to tag or filter false alarms to optimize and improve performance over time
- Ability to receive and decode Remote ID and/or Drone ID information broadcast by certain drones. In many cases, operators of RF detection technology may be able to determine the location of the drone and/or the drone pilot, as well as other important information for a thorough threat assessment
- Azimuth and vertical coverage angles optimized for UAS or UAS detection
- RF Direction Finding (RFDF) capability for UAS and controller can provide geolocation capability similar to radar.

RF-based detection technologies come in a wide range of form factors, such as handheld devices, vehicle mounted, and fixed-site solutions. Due to its versatility, passive and cost-effective nature, RF is often the first sensor deployed for CUAS.

Image

*DroneSentry multi-sensor detection solution example configuration*

## Radars

Radars track motion with applications beyond UAS tracking. Drone detection radars can utilize different technical approaches to detect and track drones based on movement and size.

Counter-drone radars use one of the following techniques:

1. **Active Radar-Pulse –**
   - Highly adaptable, from close-range urban operations to long-range situational awareness
   - Emits short, high-power pulses that measure reflected signals to detect, locate, and track objects
   - Performance is influenced by pulse data, ergonomics, FOV, number and placement of transmit and receive elements, refresh rates, and the software stack that interprets returns
   - Radars deliver high-quality, timely, accurate, and mission-relevant data for informed decision-making

2. **Active Radar-Continuous Wave –**
   - These radars continuously transmit an illumination signal and simultaneously receive echo reflections. A moving object's speed and trajectory can be determined by observing its frequency shift, as seen at the receiver, due to the Doppler effect
   - These systems cannot perform range measurements without including a timing reference in the transmitted signal

3. **Passive Radar –**
   - Makes use of existing environmental broadcast, communication or radio-navigation transmission signals to detect the presence of objects in the receiving monitoring area
   - The system transmitter and receiver are at separate locations, and the user only has control over the receivers.
   - Potential illumination signals that could be used for UAS detection include Frequency Modulation (FM), Digital Video Broadcasting (DVB), Global System for Mobile Communications (GSM), Global Navigation Satellite System (GNSS), or Wireless Fidelity (Wi-Fi). These radars do not emit a noticeable signature

## Cameras

Electro-Optical (EO) and Infrared (IR) cameras are widely used in UAS detection, often paired with other sensor types to create integrated multi-sensor solutions.

There is a performance trade-off between field of view (FOV) and detection range. Cameras with wide FOVs cover larger areas but struggle to detect drones at long distances, often only a few hundred meters. High-quality cameras with a 90° view still require initial cueing from radar or RF sensors to maximize effectiveness.

Recent advances in AI and computer vision have dramatically improved drone detection and classification algorithms. Cameras in multi-sensor solutions typically operate in a slew-to-cue mode, automatically pointing toward detected UAS, zooming in, tracking, and providing video analytics. These analytics enhance identification capabilities and may assess drone payloads and threat levels autonomously.



Image

*DroneSentry multi-sensor detection solution example configuration*

# Acoustic Sensors

Two primary types of acoustic hardware are used for UAS detection based on drones' unique sound signatures: arrays and single microphones.

Acoustic arrays offer more precise source localization but come with a larger form factor and higher cost compared to single microphones.

Acoustic detection software isolates noise generated by drone blades and motors, filtering out background clutter and matching sounds against a database of acoustic signatures. Like early RF detection, acoustic solutions rely on signature libraries that require regular updates to maintain accuracy. However, newer drones are significantly quieter, which challenges acoustic sensors' effectiveness.

While advancements in AI have strong potential to enhance acoustic detection, meaningful integration has yet to be realized. Acoustic sensors are increasingly seen as viable complementary layers in multi-sensor counter-UAS solutions.

Image

*DroneSentry multi-sensor detection solution example configuration*





# Multi-Sensor Solutions

Modern UAS detection solutions commonly combine RF, radar, acoustic, optical, and thermal sensors into integrated multi-layered solutions.

This multi-sensor approach mitigates the limitations of any single technology, providing more reliable detection across diverse UAS threats.

While multi-sensor solutions offer enhanced performance, they are more complex and typically more costly than single-method solutions. Emerging technologies such as LiDAR are under evaluation but have yet to demonstrate broad operational effectiveness.

No single counter-UAS technology fits all scenarios. Providers must continuously adapt to evolving commercial drone capabilities to stay effective.

# MITIGATION / DEFEAT METHODS

Mitigation technologies are employed when a drone has been assessed to pose a threat. The goal is to neutralize the threat while minimizing the risk to nearby assets, critical infrastructure, and personnel.

Mitigation tools are generally categorized into non-kinetic and kinetic solutions.




Image

*Epirus Leonidas HPM effector*

## NON-KINETIC SOLUTIONS

### Electronic Warfare

Electronic Warfare (EW) includes jamming and spoofing to disrupt drone operations. These soft-kill techniques disable drones without causing physical damage. Common methods include:

**RF Jamming –**

When a CUAS technology aims to neutralize or mitigate a UAS threat by disrupting the RF link (C2 and/or telemetry) between the GCS and UAV. UAS frequencies are emitted from an RF jamming antenna at greater power levels, flooding that frequency bandwidth and preventing actual UAS signals from being received. When a UAS C2 connection is severed or jammed, UAVs often respond according to their pre-programming by:

- Hovering in place
- Attempting to land in place
- Attempting to return home to their original launch location
- Moving to a user-specified location
- Unscheduled landing (crash)

**Global Navigation Satellite System (GNSS) Jamming** –

GNSS jammers disrupt the UAV's ability to receive spatial and temporal information from these satellite systems. UAVs that lose their satellite link often respond by:

- Hovering in place
- Landing in place at the moment of signal loss
- Attempting to return to their original launch location, if they have other means of orienting themselves in space

Both RF jammers and GNSS jammers can come in two variants: directional and omni-directional.

- Directional jammers radiate RF signals in a more focused manner such that the operator can point the jammer in the direction of their intended target
- Omnidirectional jammers are less discriminatatory, and radiate RF signals in all directions

**High-Powered Microwaves (HPM)** –

HPMs are non-kinetic, low-collateral CUAS solutions.

- These solutions are a subset of directed energy that emit a powerful, focused beam of electromagnetic energy to critically disrupt the internal electronics of an intended target. This includes fiber optic drones.





## KINETIC SOLUTIONS

### Hard-Kill Solutions

Hard-kill methods physically neutralize drones through kinetic means such as counter-drones, net guns, directed energy weapons (lasers), or ammunition.

These solutions are typically reserved for military and federal applications due to the risk of collateral damage and operational complexity:

- Directed Energy Weapons
- Low and High Powered Lasers

**Autonomous Kinetic Defeat UAS** –

Commonly referred to as "kamikaze drones", and UAS-seeking drones that physically intercept targets using nets or projectiles. While effective in specific scenarios, these methods face scalability issues against drone swarms and pose an increased risk of collateral damage or injury.

**Lasers** –

CUAS lasers can be low powered or high powered. The benefits of low powered lasers are their relatively lesser price point and smaller form factor.

Both varieties need to be trained on a drone target for at least several seconds to achieve a desired effect, while aiming at the connection between the body of the drone and its propellers (the weak point). This can be particularly difficult if a drone is moving at extremely high speeds.

## CYBER AND HYBRID APPROACHES

### Cyber Techniques

Cyber techniques exploit software vulnerabilities in drone control systems or associated mobile applications to hack control or disable functionality.

Hybrid approaches often combine cyber, EW, and kinetic methods, integrating them into a single platform or command interface to offer multi-layered mitigation strategies.

Weaknesses of cyber techniques may include:

- A reliance on decrypting protocols for both detection and disruption. With a large and ever-growing number of protocols used, as well as improvements to communication bandwidths between drones and their controllers, this has never been more difficult
- The prolonged time it takes to decrypt a single drone (at times, approximately 30 seconds per drone). In comparison, smart jamming works on a set area, regardless of the number of drones

# Types of CUAS Solutions

Depending on the threat environment, mission objectives, and operating conditions, CUAS technologies are packaged into various form factors – from wearable units for individual operators to large-scale solutions integrated into existing air defense infrastructure. Each type of solution brings distinct operational advantages and limitations.

Image

*DroneShield's DroneGun Mk4 counter-drone effector and DroneShield's body-worn drone detection device, RfPatrol Mk2*

## Mobile Units

Mobile CUAS units are designed for portability and rapid deployment. These systems are typically small, lightweight, and operated by a single person or small team.

**Wearable / Man-Portable Solutions**

These solutions are intended for frontline personnel and first responders who require immediate threat detection and mitigation capabilities.

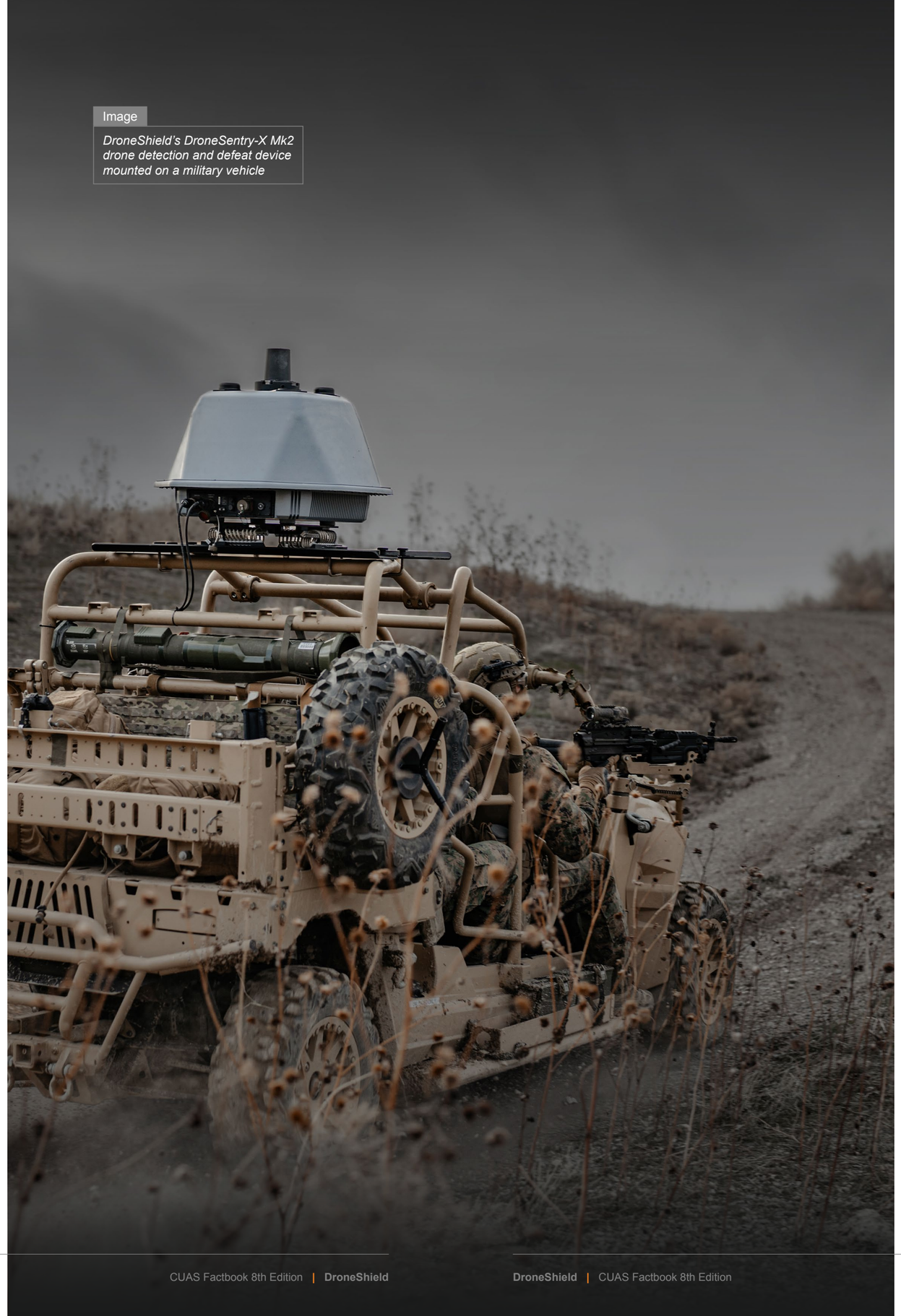
Wearable CUAS solutions may include:

- **Handheld Drone Jammers –**
  Handheld jammers provide dismounted operators with a simple point-and-shoot capability to disrupt or disable rogue UAS. These portable devices offer frontline personnel agile and immediate defense during ground operations.

## Transportable Solutions

Transportable CUAS platforms are modular solutions designed to be quickly moved and set up in new locations. They typically require vehicle transport and a team for deployment, and can be operational within hours.

- Usually combine multiple sensor modalities such as RF detection, radar, and EO/IR, and are capable of longer-range surveillance and engagement
- Transportable units are ideal for temporary facilities, border outposts, expeditionary bases, and events where airspace control is needed for limited durations
- Mitigation capabilities may include RF jamming, GNSS spoofing, or even kinetic countermeasures, depending on legal and operational constraints



Image

*DroneShield's DroneSentry-X Mk2 drone detection and defeat device mounted on a military vehicle*

## Vehicle-Mounted Platforms

Vehicle mounted CUAS solutions are integrated directly onto land vehicles, enabling mobile operations with high-capacity detection and mitigation tools.

- Platforms may be fitted on armored or utility vehicles, capable of moving with convoys or securing perimeters while in motion
- The integration of radar, RF sensors, and kinetic interceptors provides comprehensive protection in mobile or semi-permissive environments
- Commonly used by military forces and border security teams, particularly in areas with limited infrastructure
- They often feature stabilized mounts and automatic tracking to remain effective while in motion





## Maritime CUAS Solutions

The maritime domain introduces unique challenges for CUAS operations, including movement from sea swells, corrosion, and electromagnetic interference from shipboard systems.

Maritime CUAS solutions are engineered to function effectively in this environment.

- These solutions are deployed on naval vessels, coast guard ships, and offshore platforms
- They provide surveillance and defense against drone incursions near maritime assets, which may be used for surveillance, targeting, or disruption of ship operations
- Often feature ruggedized radar and EO/IR components, stabilized mounts, and electromagnetic shielding
- Mitigation techniques may include non-kinetic and kinetic options adapted for use at sea

## Fixed-Site Installations

Fixed CUAS solutions are permanently installed to protect high-value infrastructure, such as airports, stadiums, government facilities, military bases, power plants, or correctional institutions.

- These solutions are typically networked, providing continuous 360° surveillance with integrated detection and, when authorized, mitigation capabilities
- Due to their stationary nature, fixed solutions can support larger and more sophisticated sensor arrays, longer detection ranges, and more powerful defeat methods
- Often integrated with command-and-control (C2) systems, allowing for real-time threat visualization and coordination with broader security infrastructure
- Fixed site solutions are designed for long-term reliability and may include redundancy to ensure uninterrupted operation

Image

*DroneShield's DroneSentry-X Mk2 transportable installation*





## Integrated Air Defense and CUAS Hybrids

In advanced military environments, CUAS capabilities are increasingly being integrated into broader air defense ecosystems. These hybrid platforms treat UAS as one of the many airborne threats and apply similar detection and engagement protocols.

- Integrated solutions may be connected by ground-based air defense radars, missile systems, and manned aviation to provide unified situational awareness and coordinated response. This allows for seamless tracking and engagement of threats across altitude and size spectrums from microdrones to cruise missiles
- These hybrids are particularly effective in contested airspace where adversaries may employ mixed tactics, including the simultaneous use of manned aircraft, drones, and electronic warfare

Each of these CUAS solution types plays a specific role in the layered defense against aerial threats. Selecting the appropriate platform depends on the operational environment, available infrastructure, and legal regulations.

# Applications and Operational Contexts

CUAS is being integrated into various operational contexts to safeguard national security, protect critical infrastructure, and ensure public safety.

While the fundamental principles of CUAS remain consistent, their application and execution vary significantly based on the mission, environment, and threat profile.

## Military and Battlefield Use

UAS have become a fixture in modern warfare, used extensively for intelligence gathering, target acquisition, and direct attacks. Adversaries, including non-state actors, increasingly deploy small and inexpensive drones to conduct surveillance, deliver improvised explosive devices (IEDs), or overwhelm forces using swarms.

CUAS operates in military settings at all levels-strategic, operational, and tactical. Solutions must detect and defeat threats ranging from long-range fixed-wing UAS to small quadcopters flying at low altitudes. On the battlefield, CUAS technologies are employed to protect:

- Forward operating bases and logistics hubs
- Armored columns and infantry formations
- Strategic command and communication nodes

The challenge lies in neutralizing threats without interfering with friendly forces, civilian populations, or critical communications–a delicate balance in complex, dynamic combat zones.

# Critical Infrastructure Protection

Drones present a clear threat to critical infrastructure, including energy facilities, nuclear sites, data centers, and transportation hubs.

A single drone can carry out physical attacks, conduct surveillance for future operational threats, or interfere with sensitive systems through cyber payloads.

CUAS solutions are deployed to protect these vital assets by:

- Monitoring low-altitude airspace for unauthorized drone activity
- Provide key information to counter-UAS operators to enable an efficient and thorough threat assessment
- Mitigating threats through controlled and legally compliant countermeasures

Fixed installations with persistent monitoring capabilities are favored in these contexts, often integrated into broader physical and cyber security frameworks.


Image

*DroneShield's DroneSentry-X Mk2 CUAS detect solution at an airfield*





# Law Enforcement

Domestic law enforcement agencies face increasing challenges from drones used in criminal activity.

These include surveillance of police activity, smuggling, espionage, and disruption of operations. Drones have also been used during civil unrest to monitor or interfere with law enforcement units.

CUAS applications in law enforcement emphasize:

- Rapid detection and threat assessment in populated areas
- Minimal collateral impact on civilians and communications
- Adaptability to tactical deployments such as SWAT, bomb squad, crime scene, and emergency response operations

For many law enforcement agencies, laws and regulations limit the use of drone defeat technologies, making drone detection technologies especially valuable.

Image

*DroneShield's DroneGun Mk4 (top) and DroneSentry-C2 Tactical (bottom)*

## Border Security and Maritime Domains

Drones are increasingly used to transport contraband, conduct surveillance or patrol routes, or facilitate human trafficking operations across national borders. In the maritime domain, drones may be launched from vessels to bypass conventional radar detection or compromise shipboard systems.

CUAS in these environments face unique challenges:

- Vast and often remote terrain (e.g. desert borders, coastal regions)
- High mobility requirements
- Integration with existing surveillance assets like ground sensors, ships, and aircraft

Mobile and vehicle-mounted solutions are particularly valuable in border and maritime security, where fixed infrastructure may be limited.





## Event and VIP Protection

Large public gatherings such as sporting events, political rallies, festivals, and VIP visits are potential soft targets for drone-based disruptions or attacks. Drones can be used for:

- Dropping hazardous materials or propaganda
- Gathering intelligence on security layouts
- Causing panic and disrupting public order

CUAS at public events must be unobtrusive yet highly effective. This often entails deploying portable or dismounted solutions capable of rapid response, short-range mitigation, and clear rules of engagement. In VIP protection, CUAS may be synchronized with motorcades or venue security to maintain continuous airspace awareness.

CUAS is no longer reserved for the battlefield. It has become a critical component of layered defense strategies across military, civilian, and law enforcement domains. As the drone threat becomes increasingly democratized and sophisticated, the demand for tailored CUAS applications will only grow.

# Challenges in CUAS Implementation

Beyond technical performance, a successful CUAS strategy must navigate regulatory, logistical, environmental, and strategic hurdles.

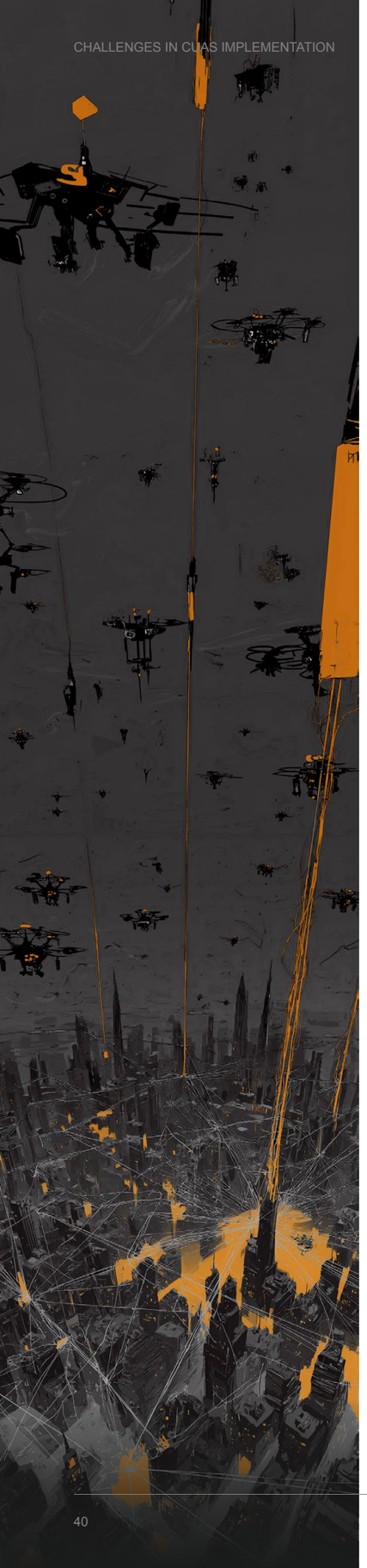
These challenges are often overlooked in favor of technological discussions, yet they are essential in determining the real-world effectiveness of CUAS deployments.

## Rapidly Evolving Threats

The drone threat landscape is characterized by its adaptability and speed of innovation. Commercial drones are updated regularly with new capabilities – greater range, autonomy, encrypted communications, or stealth features – while adversaries develop custom platforms to evade detection and defeat systems.

- **Adversarial Adaptation –**
  Malicious actors study CUAS capabilities and evolve tactics to bypass them, including low-profile flights, terrain masking, swarm coordination, and decoy use
- **Technology Turnover –**
  The pace of drone innovation frequently outpaces CUAS upgrade cycles, creating persistent capability gaps

To remain effective, CUAS platforms must be modular and designed for rapid adaptation, both in terms of software and hardware, without requiring a full system overhaul for every new threat.



## Detection Accuracy and False Positives

Effective CUAS depends heavily on the ability to detect and correctly identify UAS threats in real time. However, the detection environment is often cluttered and dynamic.

- **Sensor Limitations –**
  RF sensors may be limited by signal saturation in urban areas. Radar may have difficulty distinguishing small drones from birds or other airborne clutter. EO/IR systems are affected by weather and line-of-sight
- **False Positive Rates –**
  Inaccurate detection can lead to unnecessary security responses, desensitization to detection alerts, and loss of trust in the system

Advanced sensor fusion, machine learning, and context-aware decision systems are designed to reduce error rates and enhance classification confidence.

## Dense Urban Environments

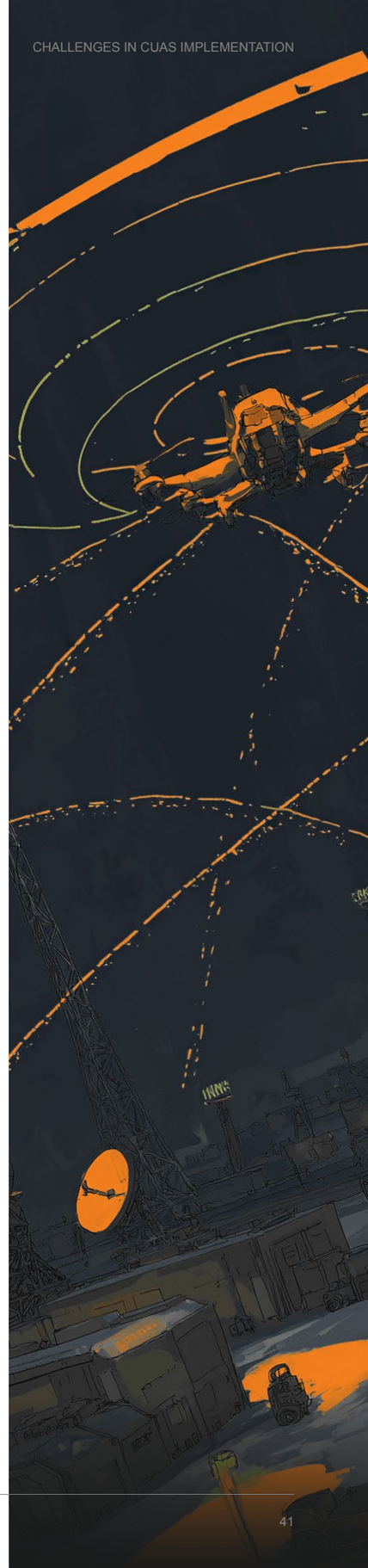
Urban environments present unique operational and technical challenges to CUAS implementation.

- **RF Congestion and Reflection –**
  Dense RF environments complicate detection and tracking. Signals may bounce off buildings or be drowned out by other sources
- **Restricted Fields of View –**
  Buildings, terrain, and infrastructure can obstruct line-of-sight for optical sensors and radars, creating blind spots
- **High-Civilian Presence –**
  Any countermeasures used in a city must minimize the risk to uninvolved parties. This greatly limits the use of kinetic defeat options and increases legal scrutiny

Successful CUAS in urban settings requires layered, multi-modal sensing with emphasis on precise localization and low-collateral mitigation.







## Jamming and Electromagnetic Interference Risks

Many CUAS solutions rely on electronic warfare techniques for mitigation. These methods can carry significant risks.

- **Collateral Interference –**
  Jamming may disrupt legitimate RF systems, including public safety radios, cellular networks, and navigation services, especially in densely populated areas
- **Adversary Countermeasures –**
  Advanced drones may operate autonomously or use hardened communication links, making them resistant to jamming or spoofing
- **Regulatory Constraints –**
  The use of RF jamming is tightly controlled in many countries, limiting its deployment to military or specialized federal agencies. Operators must weigh the operational necessity of jamming against potential risks and often require legal or procedural frameworks to govern its use.

## Cost, Scalability, and Logistics

While technological innovation dominates CUAS conversations, the practical aspects of fielding, scaling, and sustaining CUAS are equally critical and often underappreciated.

- **Resource Constraints –**
  CUAS solutions can be expensive to procure, maintain, and operate. For smaller agencies or private sector entities, costs may be prohibitive
- **Coverage Limitations –**
  Protecting a single facility may be manageable, but scaling to protect entire urban areas, border regions, or infrastructure networks introduces logistical hurdles
- **Operational Readiness –**
  Solutions must be deployed with trained personnel, maintenance support, and integration into existing security architecture.
  A technically advanced system with poor operational planning can be rendered ineffective

Moreover, because drone threats can appear suddenly and move rapidly, solutions must be designed for high availability, quick deployment, and seamless interoperability.

# The Future of CUAS

The future of CUAS will be shaped by emerging technologies, new operational paradigms, and an increasing need for integrated airspace awareness.

## Emerging Technologies

The CUAS landscape is rapidly expanding beyond traditional sensors and kinetic solutions. Several emerging technologies are beginning to reshape how threats are detected, classified, and defeated.

**Drone Autonomy –**
Autonomous drone technology is not quite at the stage where it can unilaterally replace “human in the loop” operations. The current trend of First Person View (FPV) drones has proven that RF-based technology is unlikely to disappear.

When conducting surveillance, timely information is critical. Autonomous drones have historically performed poorly in this area, given that they will first need to return to their pilots for them to download and view the footage.

In Ukraine, development in FPV drone autonomy is going at pace, and is already in operational use in the war by both Russian and Ukrainian forces

- Last-mile-technology is already a feature that can be selected by most of the FPV manufacturers providing drones to Ukraine (the same technology is presumably valid on the enemy side)
- The current level of development requires in most cases the operator to select “lock on target” before the vision based auto targeting module takes over control (there are also modules that are doing automatic target recognition and able to select target, lock and attack autonomously)
- Once “locked”, the video link is still maintained for the operator to do battle damage assessment. If the control link is not cut due to EW jamming, the operator can take over control to more accurately hit the weakest spot of an enemy vehicle – or abort the mission
- RF detection is still relevant in these cases, but disruption is constantly playing catch up with greater distances (exceeding the current average of about 500-1,000m) and more sophisticated solutions required
- Since power amplifiers (such as Alientech) combined with directional high gain antennas are standard, the power required for a jammer to be effective at 1,000m is significant and requires an intelligent EW approach to be feasible across a wide frequency range (unless it is a truck-sized solution)

Autonomous precision strike operations tend to involve two flights by two different drones:

- The first flight, usually equipped with a camera, radar, or LiDAR, is for reconnaissance to map the target and flight paths
- The captured data is then used for the direct strike mission using a visually guided drone as opposed to a GPS-guided drone. Thus, the ability to detect, track, and defeat UxS using RF technologies is still the most effective CUAS approach

**GPS-Guided Drones –**
Drones using way-point navigation (GPS-guided drones), do not appear to provide sufficiently accurate and precise satellite navigation in warzones such as Ukraine, where GNSS jamming and spoofing are common across wide areas. Outside warzones, GNSS suppression is able to disrupt way-point navigation of drones (where lawful for the customer to deploy).

Remote Weapon Stations have a narrower market applicability, generally to war zones, and are subject to technical export control and collateral damage limitations.

**Fiber-Optic Drones –**
Drones controlled by fiber-optic cables have significant limitations on their use, including entanglement of the lines to each other, trees, buildings, the drone being tangled onto itself (especially in adverse weather conditions), as well as the weight of the cables.

Use of multi-sensor solutions, including AI-powered sensor fusion with other modalities for detection (radar, acoustic, camera, etc.) and defeat (high-powered microwaves), is the best approach for such drones.

## Swarm Defense and Counter-AI Solutions

Drone swarms represent a significant leap in adversarial capability. Enabled by AI and decentralized control algorithms, swarms can conduct complex operations autonomously, such as:

- Saturating a CUAS system's detection and targeting capacity
- Engaging in coordinated attacks on multiple targets
- Adapting in real-time to defense countermeasures

Future CUAS will require automated response strategies to match the speed and complexity of AI-driven swarms. This includes:

- **Swarm Behavior Modeling –**
  Understanding how drone swarms communicate, and coordinate can inform detection and disruption strategies
- **Autonomous Counter-Swarming –**
  AI-enabled CUAS solution must be able to analyze, prioritize, and respond to multiple threats simultaneously without requiring continuous human intervention

Robust sensor fusion, distributed processing, and machine-speed decision-making will be foundational to defeating swarm threats.

## Airspace Awareness for Advanced UAS Operations

The emergence of complex UAS use cases – such as Beyond Visual Line of Sight (BVLOS) flights, drone delivery, and Drone as First Responder (DFR) programs – necessitates new approaches to low-altitude airspace management.

- **Persistent Surveillance –**
  CUAS technologies are being adapted to provide persistent airspace awareness in the low-altitude layer, enabling safe operations of both friendly and commercial drones
- **UAS Traffic Management (UTM) –**
  Integration with UTM systems will allow CUAS solutions to distinguish between cooperative and non-cooperative drones in real-time
- **Sensor-Integrated Air Picture –**
  Combining RF, radar, and optical data into a common operational picture will enable better decision-making for both defensive and commercial operations

By enabling greater airspace situational awareness, CUAS solutions are poised to play a dual role-defending against threats while also enabling the safe integration of drones into national airspace.





## CUAS and Space-Based Threat Monitoring

The increasing use of satellites for surveillance and communications has prompted interest in using space-based assets to augment CUAS capabilities.

- **Global Surveillance –**
  Satellites can provide persistent observation over wide geographical areas, supporting early warning for mass UAS launches or tracking long-range drone activity
- **Signal Intelligence –**
  Space-based platforms can detect and geolocate RF emissions from drones, enabling detection over remote or denied areas
- **Sensor Fusion Across Domains –**
  The fusion of terrestrial, airborne, and space-based data streams offers the potential for a truly layered defense architecture

Though still in its infancy, space-based CUAS integration will become more important as drone threats grow in range and sophistication.

## Forecasting the Next Generation of Threats and Solutions

The drone threat is not static – it is dynamic, inexpensive to scale, and creatively employed by both state and non-state actors.

- **Biologically Inspired Drones –**
  Small drones mimicking birds or insects are harder to detect and may bypass current sensor capabilities
- **Cyber-Autonomous UAS –**
  Drones that operate entirely disconnected from external command-and-control (C2) links, making them resilient to jamming or spoofing
- **Drone-Launched Countermeasures –**
  UAS that carry and deploy their own mitigation systems to evade CUAS efforts

In response, CUAS solutions must become smarter, faster, more agile, and more deeply integrated into defense and public safety ecosystems. Open architecture frameworks, AI-powered automation, and scalable C2 solutions will define the systems of the future.

## Drones have fundamentally altered the threat landscape, enabling state and non-state actors to conduct surveillance, disrupt infrastructure, and inflict harm with speed, precision, and deniability.

CUAS is not a singular technology, but an evolving discipline – an ecosystem of detection, tracking, identification, and mitigation tools that must work in concert to safeguard airspace, assets, and lives. From military operations and critical infrastructure protection to event security and urban defense, the demands placed on CUAS solutions are complex, dynamic, and constantly shifting.

As threats grow more autonomous, networked, and evasive, the future of CUAS will depend on layered, scalable approaches – grounded in sound operational concepts and supported by continuous innovation. Technologies like AI-enabled sensor fusion, swarm defense protocols, airspace awareness systems, and space-based surveillance will define the next era of aerial security.

At the core of this evolving mission is one truth: effective CUAS solutions must be tailored to the environment, the threat, and the mission. There is no one-size-fits-all approach. Success lies in designing systems that are not only technically capable, but operationally relevant – deployable where needed, when needed, with clear rules of engagement.





| | | |
|---|---|---|
| **A** | AGL | Above Ground Level |
| | AI | Artificial Intelligence |
| **B** | BVLOS | Beyond Visual Line of Sight |
| **C** | C2 | Command-and-Control |
| | CUAS | Counter-Unmanned Aerial System |
| | CUxS | Counter-Unmanned System |
| **D** | DF | Direction Finding |
| | DFR | Drone as First Responder |
| | DVB | Digital Video Broadcasting |
| **E** | EO | Electro-Optical |
| | ERMP | Extended-Range Multi-Purpose |
| | EW | Electronic Warfare |
| **F** | FM | Frequency Modulation |
| | FOV | Field of View |
| | FPV | First Person View |
| **G** | GCS | Ground Control Station |
| | GNSS | Global Navigation Satellite System |
| | GPU | Graphics Processing Unit |
| | GSM | Global System for Mobile Communications |
| **H** | HPM | High Powered Microwave |
| **I** | ID | Identification |
| | IR | Infrared |
| | ISR | Intelligence, Surveillance, and Reconnaissance |
| **L** | LE | Long Endurance |
| | LiDAR | Light Detection and Ranging |
| **M** | ML | Machine Learning |
| | MQ | M = Multi-Mission \| Q = Unmanned Aerial Vehicle (UAV) |
| **P** | PDW | Performance Drone Works |
| **R** | RF | Radio Frequency |
| | RQ | R = Reconnaissance \| Q = Unmanned Aerial Vehicle (UAV) |
| **S** | sUAS | Small Unmanned Aerial System |
| | STUAS | Small Tactical Unmanned Aerial System |
| **U** | UAS | Unmanned Aerial System |
| | UGV | Unmanned Ground Vehicle |
| | USV | Unmanned Surface Vehicle |
| | UUV | Unmanned Underwater Vehicle |
| | UxS | Unmanned System |
| **V** | VIP | Very Important Person |
| **W** | Wi-Fi | Wireless Fidelity |

DRONESHIELD

To explore tailored CUAS solutions aligned with specific mission needs, contact our team of specialists.

We are committed to advancing airspace security through informed collaboration, operational insight, and continuous cutting-edge capability development.

**Connect with us**