DRONESHIELD SRIGROUP

White Paper

Best Practices for Counter-Drone Deployment at Civil Airports

October 2025

BACKGROUND

Airports are a critical cornerstone of the global economy. In 2023, airports worldwide generated approximately US$146 billion in revenue, supporting millions of jobs and facilitating the movement of over 4 billion passengers. Passenger volumes are projected to reach 22.3 billion by 2053, nearly 2.4 times the expected traffic in 2024[1]. Airports not only enable tourism and trade but also serve as strategic infrastructure for national resilience and regional development. Their uninterrupted operation is essential to economic stability.

However, this vital infrastructure is increasingly vulnerable to disruption from Unmanned Aerial Systems (UAS), commonly known as drones. While most drone incursions near airports are accidental or nuisance-related, often involving hobbyists unaware of airspace restrictions, the threat spectrum is expanding.

Drones have increasingly been used for espionage, with documented incidents involving surveillance of critical infrastructure[2], and in some cases, to deliberately cause disruption or confusion in public settings[3]. In high-conflict regions, such as Ukraine and parts of the Middle East, drones have also been weaponised for payload delivery, ranging from explosives to contraband, posing direct threats to human life and military operations.

This evolving threat landscape underscores the importance of civil airports having the capability to first detect and understand the nature of a drone incursion, and then, where necessary, defeat the drone in a non-kinetic and proportionate manner. In civil aviation environments, where safety and public confidence are paramount, non-kinetic defeat methods, such as radio frequency (RF) disruption and RF cyber takeover, are preferred over physical interceptors.

In most nations, drones are regulated and typically operate using RF control links, making RF detection a highly effective first layer of defence. However, recent developments have seen drones navigating completely autonomously or using alternative communication protocols, such as LTE and 4G/5G cellular networks. This shift reinforces the need for a layered detection strategy at some airports, adding radar sensors where they would not interfere with operational communication protocols. In these circumstances, there is an opportunity to combine RF, radar and optical sensors to ensure comprehensive coverage and reduce the risk of false negatives.

Just as airports employ layered physical security measures, including perimeter fencing, surveillance cameras, and patrols, the same principle must apply to technological systems that respond to nefarious drones. A counter-drone system can be integrated into existing physical security systems to support the detection of drone threats.

[1] Airports Council International, “Press Releases - Airports Face Financial Challenges Despite Air Traffic Rebound, ACI World Economics Report Reveals”, 28 April 2025, https://aci.aero/2025/04/28/airports-face-financial-challenges-despite-air traffic-rebound-aci-world-economics-report-reveals

[2] EuroNews, “Russian spy drones over Germany: Why the Bundeswehr cannot shoot them down”, 5 September 2025, https://www.euronews.com/2025/09/05/russian-spy-drones-over-germany-why-bundeswehr-can-not-shoot-them-down

[3] The Wall Street Journal, “Drone Incursions Force Airport Closures in Copenhagen, Oslo”, 23 September 2025, https://www.wsj.com/world/europe/drone-incursions-force-airport-closures-in-copenhagen-oslo-ee49ba4d?

All signatory countries to the International Civil Aviation Organization's ICAO, Conventions must adhere to safety and security programs. Annex 17 (Security) to the Convention on International Civil Aviation set standards and recommended security practices for security at all airports. Unfortunately, current security operations are linear in approach and do not consider the air defence dimension that drones present. Defending the airspace over a civil airport should now be considered essential as the drone threat is increasing.

This White Paper explores the technologies and operational strategies most appropriate for civil airport environments. It focuses on cost-effective, scalable, and non-kinetic solutions, acknowledging that while kinetic effectors exist on the market, they are generally unsuitable for use in populated, high-traffic civilian settings. The goal is to provide airports, airport operators, regulators, and policymakers with a practical framework for deploying counter-drone systems that align with safety and operational requirements.

Airport contributions to the global aviation industry

Revenue generated by airports (2023)

~US$146 billion

Airports facilitated movement of **over 4 billion** passengers (2023)

9.8 billion passengers (forecast 2025)

22.3 billion passengers (projected by 2053)

Passengers forecast by region (2025)

• Asia-Pacific:	**3.6 billion**
• Europe:	**2.5 billion**
• North America:	**2.1 billion**
• Latin America-Caribbean:	**789 million**
• Middle East:	**466 million**
• Africa:	**273 million**

Source: Airports Council International

CASE STUDY:
Gatwick Airport, United Kingdom

In December 2018, Gatwick Airport was shut down for 33 hours due to suspected drone sightings. The incident occurred during the peak Christmas travel period, resulting in the cancellation or diversion of over 1,000 flights and a fecting 140,000 passengers. The estimated economic loss exceeded €55 million, primarily borne by airlines and service providers 1.

Despite a large-scale police operation and military support, no drone was conclusively identified. The incident exposed critical gaps in detection, verification, and response capabilities, prompting a nationwide review of counter-drone strategies.

FOUNDATIONAL AND COMPLEMENTARY COUNTER-DRONE TECHNOLOGIES

At a minimum, mitigating drone threats in a civil airport environment requires a detection strategy that begins with a reliable and scalable foundation. No single detection method is foolproof, as drones vary widely in size, flight characteristics, and communication protocols.

However, in most cases, radio frequency (RF) detection will provide an airport with sufficient drone defence, offering early situational awareness and actionable intelligence. RF sensors are highly effective at identifying the majority of commercially available drones which rely on remote control or telemetry links, and technologies provide a “dot on the map” for both the drone and its controller. This enables security teams to assess proximity, intent, and risk in real time.

Where appropriate, integrating RF sensors with radar and optical sensors means airports can build a more resilient and accurate detection network. This layered approach improves the likelihood of early threat identification, reduces fals positives, and enhances situational awareness. It enables security teams to visually verify threats before initiating countermeasures, ensuring that responses are proportionate, targeted, and safe for the surrounding environment.

In addition to detection, high-risk airports must also consider how to respond to drone incursions once identified. In civilian airport environments, defeat methods must not only be effective but also publicly acceptable, ensuring that mitigation actions are perceived as safe, proportionate, and aligned with community expectations around aviation safety and public risk. RF disruption is the preferred approach, allowing security teams to interrupt control signals and neutralise drones without physical interception.

This ensures that mitigation efforts are safe, targeted, and aligned with the operational realities of busy, populated airport environments.

To ensure that airports are getting the best counter-drone capability it is essential that they develop a risk-based approach to planning for any counter-drone system integration. Counter-drone planning should be conducted before engaging and buying technology. Elements of counter-drone planning that should be considered include physical evaluation of terrain; identification of likely avenues of approach; assessment of the RF spectral environment; airport command and control operations; airport crisis incident management structure; internal and external agency capabilities for counter-drone and local and national laws and regulations dealing with counter-drone use and response.

RF Detection and Disruption

Radio frequency (RF) detection is widely regarded as the foundational layer in counter-drone systems, particularly in civil aviation environments. This cost-effective method of drone detection involves passively monitoring the electromagnetic spectrum for signals emitted by drones and their controllers. RF sensors can identify the presence of drones by detecting control links, telemetry transmissions, or video feeds, often providing early warning before the drone becomes visible or enters restricted airspace.

There are two distinct levels of RF protection: detection-only systems, and detection-plus-defeat systems.

Detection-only technologies provide operators with situational awareness by identifying and geolocating both the drone and its controller. This information provides security personnel or law enforcement to take proportionate action, which may include direct engagement with the operator, such as issuing a verbal request to cease flying, without the need for electronic countermeasures. This approach is particularly relevant in civil airport environments, where most drone incursions are accidental or benign.

In higher-risk scenarios, RF-based drone defeat mechanisms may be employed to disrupt the drone's communication channels. These non-kinetic countermeasures such as jamming drone control frequencies, can force the drone to land or return to its operator, provided such protocols are built into the drone's design[4]. World-leading counter-drone systems can mitigate multiple drones operating on different frequencies simultaneously. This approach is especially suitable for airports, where safety and precision are paramount, and where physical interception methods may pose unacceptable risks to aircraft, personnel, or infrastructure.

While RF detection may not capture every type of drone, particularly those operating autonomously or using unconventional communication protocols, it remains highly effective for the vast majority of real-world threats as the mainstream frequencies for consumer drones are RF-based[5]. RF detection systems are therefore a critical first layer in any counter-drone strateg .

Nonetheless, to ensure comprehensive coverage and reduce risk at airports with high volumes of passenger traffic, RF detection could be complemented by additional sensor types, such as radar and optical systems, which can detect drones that may not emit RF signals or are operating in complex environments.

[4] DJI, "What is the Return to Home (RTH) logic of DJI Inspire 3?", https://support.dji.com/help/content?customId=01700007759&spaceId=17

[5] Autel, "Understand the Frequency Bands of Drones", 22 April 2025, https://www.autelpilot.com/blogs/drone-technology/understand-the-frequency-bands-of-drones/

Cyber Takeover Capabilities

In addition to RF disruption, some advanced counter-drone systems offer the ability to assume control of a hostile drone mid-flight through cyber takeover techniques. This method involves exploiting vulnerabilities in the drone's communication protocols or onboard systems to override the original operator's commands. Once control is established, the drone can be safely redirected, landed, or neutralised in a controlled manner.

Cyber takeover offers a highly precise and low-risk mitigation option, particularly in environments where jamming may be restricted or where collateral disruption must be avoided. This capability may be valuable in high-density civilian environments like airports, where safety, precision, and public acceptability are paramount.

Radar and Optical Tracking

While RF detection remains the primary method for identifying drones, radar and optical systems provide valuable complementary capabilities. These technologies enhance the overall robustness of a counter-drone system by offering additional layers of verification and tracking

Radar systems are particularly effective in monitoring wide areas and detecting airborne objects based on movement and size. They perform well in various weather conditions and can help maintain situational awareness. Although radar may occasionally struggle to differentiate drones from birds or other small objects, its integration with other sensor types like RF sensors helps mitigate these potential false positives.

In airport environments, radar must be carefully selected to avoid interference with existing communication and navigation systems. When appropriately integrated, radar contributes to broader situational awareness and supports the detection of drones that may not emit RF signals. Such drones may be utilised by malicious actors or adversaries seeking to evade RF-based detection capabilities.

While these cases are less common, the associated risks are significantly highe , as malicious actors tend to be more calculated and deliberate in their methods.

Optical imaging systems add another layer of precision. These tools allow operators to visually confirm and classify drones based on shape and flight behaviou . When powered by artificial intelligence, automated hands-free visual tracking can support real-time threat assessment and prioritisation, enabling more informed decision-making.

Together, radar, optical, and RF systems form a cohesive, multi-modal detection network. This layered approach ensures that airports can detect, verify, and respond to drone incursions with greater accuracy and confidence, supportin both safety and operational continuity.

CASE STUDY:
Copenhagen Airport, Denmark

On the evening of 22 September 2025, Copenhagen Airport, Scandinavia's largest airport, was forced to suspend all take-offs and landings for nearly four hours due to sightings of two to three large, unidentified drones in its airspace. The disruption stranded tens of thousands of passengers and caused widespread delays and cancellations that rippled across the Nordic region.

The incident was described by Danish Prime Minister Mette Frederiksen as "the most serious attack on Danish critical infrastructure to date". Agencies reported that the drones demonstrated advanced capabilities: flying long distances, executing complex flight patterns, and appearing to operat from multiple directions. Investigators considered the possibility of launch from nearby vessels, highlighting the strategic vulnerability of coastal airports.

This event underscored the growing threat of hybrid attacks and the need for robust counter-drone systems. Although attribution remains uncertain, the calculated nature of the operation suggests a capable and deliberate actor. While such incidents are not yet commonplace, the risks are significantly higher, as malicious actors are increasingly strategic and sophisticated in their approach.

SITUATIONAL AWARENESS AND MONITORING TOOLS

Effective counter-drone operations rely not only on detection technologies but also on the ability to coordinate and act on information in real time.

A centralised monitoring and decision-support platform is essential for integrating data from multiple sensors, visualising threats, and managing response protocols within the airport's operational framework with minimal operator cognitive burden.

Modern airport monitoring systems provide security and operations personnel with a unified interface that displays live drone activity, sensor status, and recommended response actions. Airport Operations Centers (AOC) are the likely location for counter-drone system integration. While AOCs are busy, it is imperative that counter-drone system integration is seamless and complements existing communication and command operations. The systems should become part of the Airport Security Program, ASP, mandated under ICAO and that the counter-drone system and its operations become part of the Airport Aviation Security Committee at that airport.

Furthermore, counter-drone operations should be integrated into the National Aviation Security Program to ensure national counter-drone integrity.

Beyond real-time oversight, these systems also support evidence logging and incident reporting, which are critical for regulatory compliance and post-event analysis. Integration with existing airport infrastructure, such as perimeter surveillance, air traffic control, and emergency services, ensures that counter-drone measures are coordinated and minimally disruptive to normal operations.

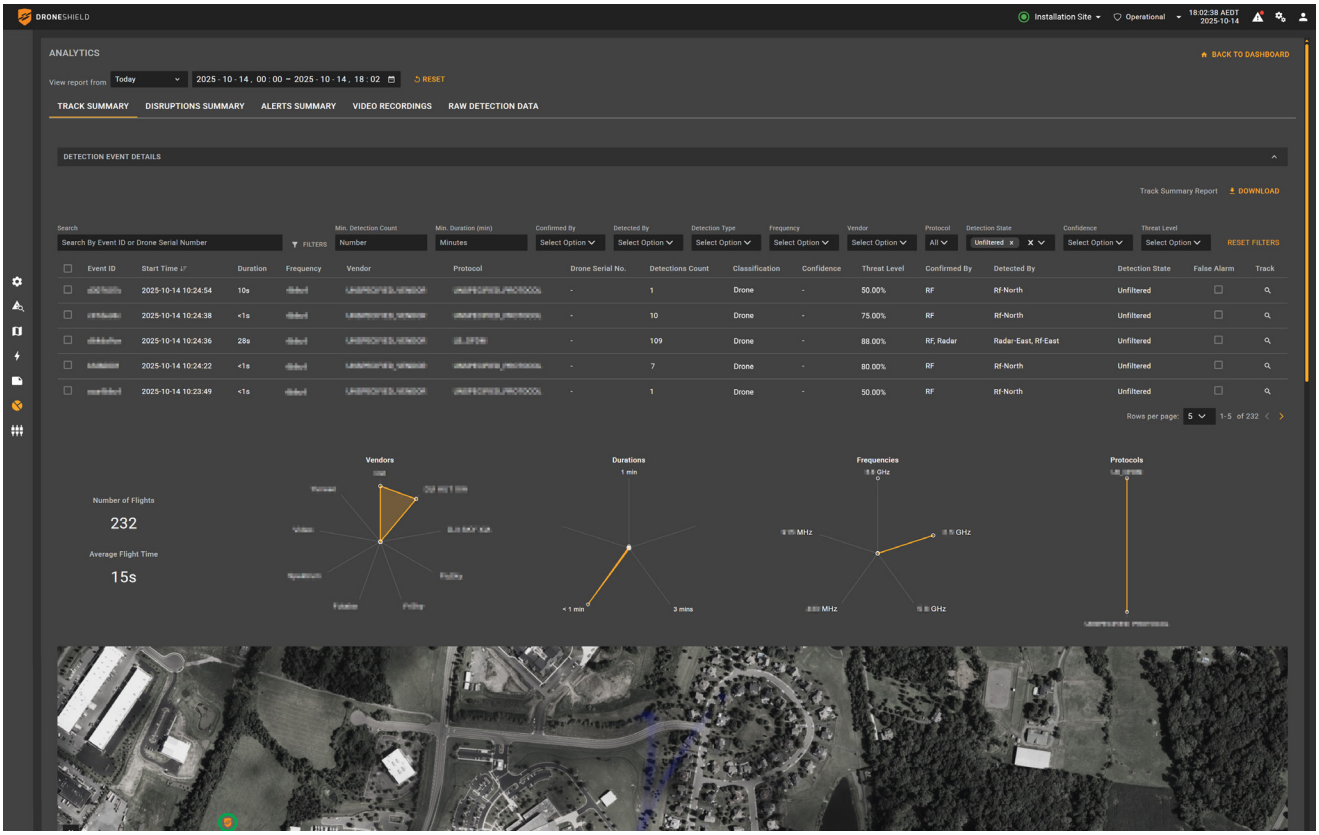
By consolidating situational awareness and decision-making into a single operational platform, airports can respond to drone threats with speed, precision, and accountability, while maintaining continuity of service and public safety.

Drone Identification

Accurate identification of drones is a critical component of any counter-UAS strategy. Identification and classification should b handled with Artificial Intelligence (AI) models sufficiently advanced to detect both known and novel drones, including those with non-standard characteristics or emerging technologies. Systems should be capable of identifying the communication protocol used by the drone and, where possible, determine its operating frequency. This information is essential for enabling targeted, non-kinetic neutralisation when required.

Event Logging and Post-Incident Analysis

Comprehensive event logging is essential for regulatory compliance, forensic analysis, and continuous improvement. Counter-drone systems should automatically record all detection events, threat classifications, video recordings, mitigation actions, and operator responses. These logs support post-incident reviews, legal investigations, and system tuning to improve threat response accuracy.



Operator Geolocation and Threat Attribution

Advanced counter-drone systems can geolocate the operator or pilot of the drone. This capability is critical for threat attribution, law enforcement coordination, and post-incident investigation. Technologies such as triangulated RF signal analysis and AI-assisted pattern recognition can help identify the source of control signals, enabling authorities to respond not only to the drone but also to the individual responsible for its operation.

CASE STUDY:
Dublin Airport, Ireland

In early 2023, Dublin Airport faced six drone-related disruptions in six weeks, forcing repeated suspensions of flight operations. These incidents caused delays, cancellations, and reputational damage. The economic ripple effects extended beyond aviation, impacting local businesses, logistics providers, and tourism operators.

The incidents prompted Irish authorities to explore advanced counter-drone solutions, with an emphasis on layered detection and AI-assisted threat classification. The goal was to move from reactive crisis management to proactive threat prevention.

AI-DRIVEN THREAT CLASSIFICATION AND DECISION SUPPORT

Artificial intelligence (AI) plays an increasingly important role in enabling real-time classification of drones based on their flight patterns, control signals, and visual characteristics.

AI-driven threat assessment tools can distinguish between recreational drones, commercial platforms, and potentially hostile devices, helping operators prioritise responses and avoid unnecessary disruptions.

Good threat detection systems rely on AI models that have been trained over many years using extensive datasets of drone activity, including both common and rare drone types. This long-term training enables the system to recognise not only standard commercial drones but also novel or modified platforms that may not conform to typical flight or signal patterns. As drone technology becomes more diverse, with variations in size, propulsion, control methods, and payloads, AI's ability to generalise from past data and identify anomalies becomes increasingly critical.

In the airport context, where the margin for error is extremely narrow, this capability is especially valuable. AI can detect subtle deviations in drone behaviour that may indicate a higher risk profile, such as erratic flight paths, hovering nea sensitive infrastructure, or approaching restricted zones. These insights allow airport security teams to respond with greater speed, precision and confidence, ensuring that interventions are targeted and proportionate to the actual threat.

These systems are particularly valuable in environments like airports, where rapid decision-making is essential but must be balanced with safety and regulatory compliance. AI can support both automated and human-in-the-loop workflows, allowing operators to verify threats before initiating countermeasures. This approach ensures that responses are proportionate and informed, reducing the risk of false positives and enhancing operational confidence

By continuously learning from new data, AI-based classification systems improve over t me, adapting to emerging drone models and tactics. This dynamic capability is essential for maintaining resilience in the face of a rapidly changing threat landscape.

OPERATIONAL CONSIDERATIONS FOR AIRPORT COUNTER-DRONE PROGRAMS

While technology forms the backbone of any counter-UAS strategy, successful implementation depends equally on operational planning, stakeholder engagement, and policy development. The following considerations provide a practical framework for airports seeking to build resilient, coordinated, and legally compliant counter-drone programs.

Counter-drone systems and programs should be fully integrated into the airport ASP and that counter-drone operations are regularly briefed at the quarterly Airport Security Committee meetings. In this way counter-drone operations will be transparent and part of a successful response. Counter-drone operations can ensure visibility to the threat by using data and analytics of drone threat incidents regularly briefed to the Security Committee.

Continuous Improvement and Threat Intelligence

As drone technology continues to evolve, so too must the systems designed to detect and assess potential threats. Airports should implement continuous improvement processes that incorporate threat intelligence, system performance data, and stakeholder feedback. This includes updating detection algorithms, refining classification models, and adapting to new drone types and tactics. A proactive approach ensures long-term resilience and operational confidence

Integration with Physical Security Measures

RF detection is the most suitable and effective first layer for addressing nefarious drone operations in civil airport environments, particularly given that most commercially available drones rely on RF-based control links. To maximise the effectiveness of security responses, RF sensors should be integrated with the airport's existing physical security infrastructure, such as perimeter fencing, surveillance cameras, and patrol systems. This layered approach ensures that drone threats are detected in context, enhances situational awareness, and allows security teams to respond with greater precision and coordination.

Coverage Must Extend Beyond Flight Paths

While approach and departure corridors are the most obvious zones for counter-drone coverage, limiting detection to these areas leaves airports exposed to significant risk. Drones can enter airspace from any direction—over terminals, fuel depots, maintenance zones, or even adjacent public property. Each of these areas presents unique vulnerabilities that must be factored into a comprehensive counter-drone strategy.

Expanding coverage beyond flight paths ensures that threats are detected regardless of their point of origin. This includes passive monitoring surrounding land, water, and infrastructure that may serve as launch sites for malicious or careless drone operators. A well-designed sensor network should provide a 'bubble' or 360-degree coverage, enabling early detection and coordinated response across all airport zones.

Clear Policies and Procedures Are Critical

Technology alone cannot guarantee effective counter-drone operations. Airports must establish clear policies and procedures that define roles, responsibilities, and response protocols for drone incidents. Without these frameworks, even the most advanced systems can fall short,

leading to confusion, delays, or inconsistent decision-making during critical moments.

Strong policies ensure that all stakeholders, from security teams to air traffic control, understand their duties and can act decisively. These procedures should be regularly reviewed as part of regular business planning processes and updated to reflect evolving threats, regulatory changes, and lessons learned from real-world incidents. A well-documented response plan also supports legal compliance and public accountability, reinforcing trust in airport operations.

Engage Internal Stakeholders Early

Counter-drone programs affect multiple layers of airport operations and must be developed in close coordination with internal stakeholders. Law enforcement and security teams bring expertise in threat response and enforcement authority. Operations and facilities teams ensure that detection and mitigation technologies integrate smoothly with existing infrastructure and workflows. Air traffic control plays a vital role in coordinating airspace management and ensuring that drone-mitigation actions do not interfere with manned aviation.

Airlines must also be engaged to address concerns around flight disruptions, passenger safet , and reputational impact. Early and ongoing collaboration across these groups ensures that counter-drone systems are not only technically sound but also operationally viable and legally compliant.

Coordinate with External Security Partners

Drone threats often originate from outside airport boundaries, making coordination with external stakeholders essential. These may include neighbouring precincts, local law enforcement, local government authorities, and national security agencies. Without their involvement, airports may struggle to respond effectively to threats launched from adjacent land or water.

Establishing formal partnerships and communication channels with external entities enables faster response times, clearer jurisdictional authority, and more comprehensive threat coverage. Joint planning and shared situational awareness help ensure that drone-mitigation efforts extend beyond the fence line and into the broader security ecosystem.

Regular Tabletop Exercises

Drone incursions should be treated as a core scenario in regular airport training exercises and response simulations. Tabletop exercises provide a structured environment for internal and external stakeholders to rehearse coordinated responses to drone threats, evaluate decision-making processes, and identify operational gaps. By incorporating drone-related incidents into broader emergency preparedness programs, airports ensure that counter-UAS protocols are not siloed but integrated into the overall security framework.

These exercises help build familiarity with detection systems, clarify roles and responsibilities, and strengthen communication across teams. They also support continuous improvement by generating insights that inform updates to response plans, stakeholder coordination, and technology deployment. Regular inclusion of drone scenarios ensures that all parties are prepared to act swiftly and effectively when a real-world incident occurs.

Promote Public Awareness

Not all drone threats are malicious. Many stem from uninformed operators who are unaware of airspace restrictions. Simple, low-tech measures can significantly reduce these risks. Posting “No Drone Zone” signage around the airport and near likely launch sites (determined through drone detection data) serves as a visible deterrent. Social media campaigns, community outreach, and engagement with drone clubs help educate the public on the dangers of flying near airports

These proactive steps foster a culture of compliance and awareness, reducing the likelihood of accidental incursions and reinforcing the airport’s commitment to safety. By building relationships with the community, airport operators can turn potential risks into opportunities for collaboration and prevention.

IMPLEMENTATION RECOMMENDATIONS

Deploying a counter-drone system at a civil airport requires a structured and strategic approach to ensure effectiveness, safety, and operational continuity.

The following steps outline key considerations for successful implementation:

- Site Assessment: Begin with a thorough evaluation of the airport's layout, flight paths, and surrounding environment to identify high-risk zones such as runways, approach corridors, fuel depots, and passenger terminals. Planning tools can assist in modeling sensor placement and coverage to optimise detection capabilities.
- Layered Sensor Network: Establish a multi-modal detection system that integrates radio frequency (RF) sensors, radar, and optical and/or thermal imaging. This layered approach enhances reliability by compensating for the limitations of individual sensor types and provides redundancy in complex or cluttered environments.
- System Integration: Ensure that the counter-drone system interfaces smoothly with existing airport infrastructure, including perimeter security, air traffic control, emergency response protocols, and digital incident management platforms. Seamless integration supports coordinated responses and minimizes disruption to normal operations.
- Training and Simulation: Regular training exercises and scenario-based simulations are essential for maintaining operational readiness. These should involve both technical staff and decision-makers to ensure familiarity with system capabilities, response procedures, and regulatory constraints.
- Ongoing Maintenance and Support: Counter-drone systems should be regularly updated to reflect evolving drone technologies and threat profiles. This includes software updates and performance audits to ensure continued effectiveness and compliance with aviation safety standards.

CASE STUDY:
Civil Aviation Regulator

A national civil aviation regulator proactively engaged DroneShield in mid-2025 to address the emerging risks posed by drones to airport operations. Recognising the growing complexity of drone threats and the need for a coordinated national response, the regulator sought to establish a forward-looking framework before any major incidents occurred. Rather than taking a reactive approach, they turned to industry experts with a proven track record in delivering counter-drone technology.

DroneShield was brought in early to provide strategic guidance on the development of a national counter-drone regulation for the protection of regional airports. This included advising on the technical architecture of detection and mitigation systems, defining mini um performance standards, and outlining operational requirements tailored to the civil aviation environment. DroneShield's experience in deploying systems across both civilian and defence sectors enabled it to offer practical, scalable recommendations that balanced safety, legal compliance, and operational feasibility.

The collaboration extended beyond technical specifications. Dro eShield collaborated closely with the regulator to ensure the proposed framework aligned with international best practices, supported seamless integration with existing airport infrastructure, and addressed the unique challenges of operating in densely populated, high-traffic environments. The regulator valued DroneShield's ability to translate complex technical capabilities into actionable policy language, helping to bridge the gap between technology providers and government stakeholders.

Following this engagement, the regulator formally issued a national counter-drone regulation, mandating best practice deployment across all international airports. By setting sensible and realistic guidance, airports were able to adopt a standardised approach to ensure compliance and enhance their ability to detect, assess, and respond to drone incursions.

This case study demonstrates how early collaboration between regulators and trusted industry partners can accelerate the development of effective, real-world frameworks.

CONCLUSION

Drone incursions, whether accidental or deliberate, pose a growing threat to this infrastructure.

High-profile incidents at airports internationally have demonstrated how even short-term disruptions can result in millions of dollars in losses, ripple effects across supply chains, and erosion of public confidence. These events are no longer isolated anomalies, but are part of a broader trend that demands coordinated, strategic responses.

Governments, aviation regulators, and airport operators must treat counter-drone capability as a core component of national critical infrastructure protection. This includes investing in detection systems, establishing clear operational protocols, and ensuring legal frameworks empower timely and proportionate responses.

The economic stakes are too high to rely on reactive measures alone.

Proactive investment in drone detection and defeat is not just a matter of aviation safety; it is a matter of economic security and public trust. As drone technology continues to evolve, so too must the systems and policies designed to manage it.

ABOUT DRONESHIELD

Founded in 2014, DroneShield (ASX:DRO) has continually focused on developing cutting-edge counter-drone technologies that protect people, assets, and infrastructure from the rapidly evolving threat of drone-based attacks. Today, the company employs around 400 people globally, including almost 300 engineers.

DroneShield's technology is trusted by Tier 1 military, law enforcement, intelligence, and border security customers around the world, and has a presence in 70+ countries. Over 1,000 DroneShield units are currently deployed in Ukraine, where the equipment is actively saving lives in one of the world's most challenging conflict zones

As a company that excels in AI technology, including the continuous development of its proprietary SensorFusionAI, ThreatAI and DroneOptID, DroneShield is committed to evolving its hardware and software systems to stay ahead of emerging drone threats. Its global footprint and advanced AI-driven solutions enable the delivery of highly adaptive and effective counter-drone capabilities to military, law enforcement, and critical infrastructure customers worldwide.

ABOUT SRI GROUP LLC

The SRI Group LLC is a security consulting company that focuses on transportation, immigration and intelligence/security operations.

The SRI Group uses security experts with decades of experience working with aviation, port and critical infrastructure security as well as experience with ICAO, IMO, TSA, ECAC and other security organizations.

Our Counter-Drone experts have worked in UAV and Counter UAV from the governmental, commercial and academic world providing key assistance on the growing challenges of counter-drone operations. Our approach to Counter-drone operations centers on a risk-based planning and integration as well as CD training development and standardization. The SRI Group clients range from governments to Fortune 500 companies and security technology manufacturers. The SRI Group is particularly adept at integrating new security technologies into operational capability.

APPENDIX A

List of DroneShield Products:

SentryCiv 	SentryCiv is a passive, compact, fixed-site drone detection system that delivers 360° radio frequency (RF) situational awareness using DroneShield's proprietary RFAI™ engine.
DroneSentry-X Mk2 	DroneSentry-X Mk2 is a software-defined detection and adaptive disruption system, designed for mobile, field expedient pop-up, and fixed site protection. Engineered for seamless integration across land, sea, and air platforms, it provides real-time drone detection and mitigation in complex operational environments.
DroneSentry 	DroneSentry is a modular installation that can be configured with a variety of optical, radar, and radio frequency (RF) sensors, edge computing systems, and software. With various deployment options available, DroneSentry provides operators with a comprehensive CUxS solution that meets their mission requirements.

info@droneshield.com | droneshield.com