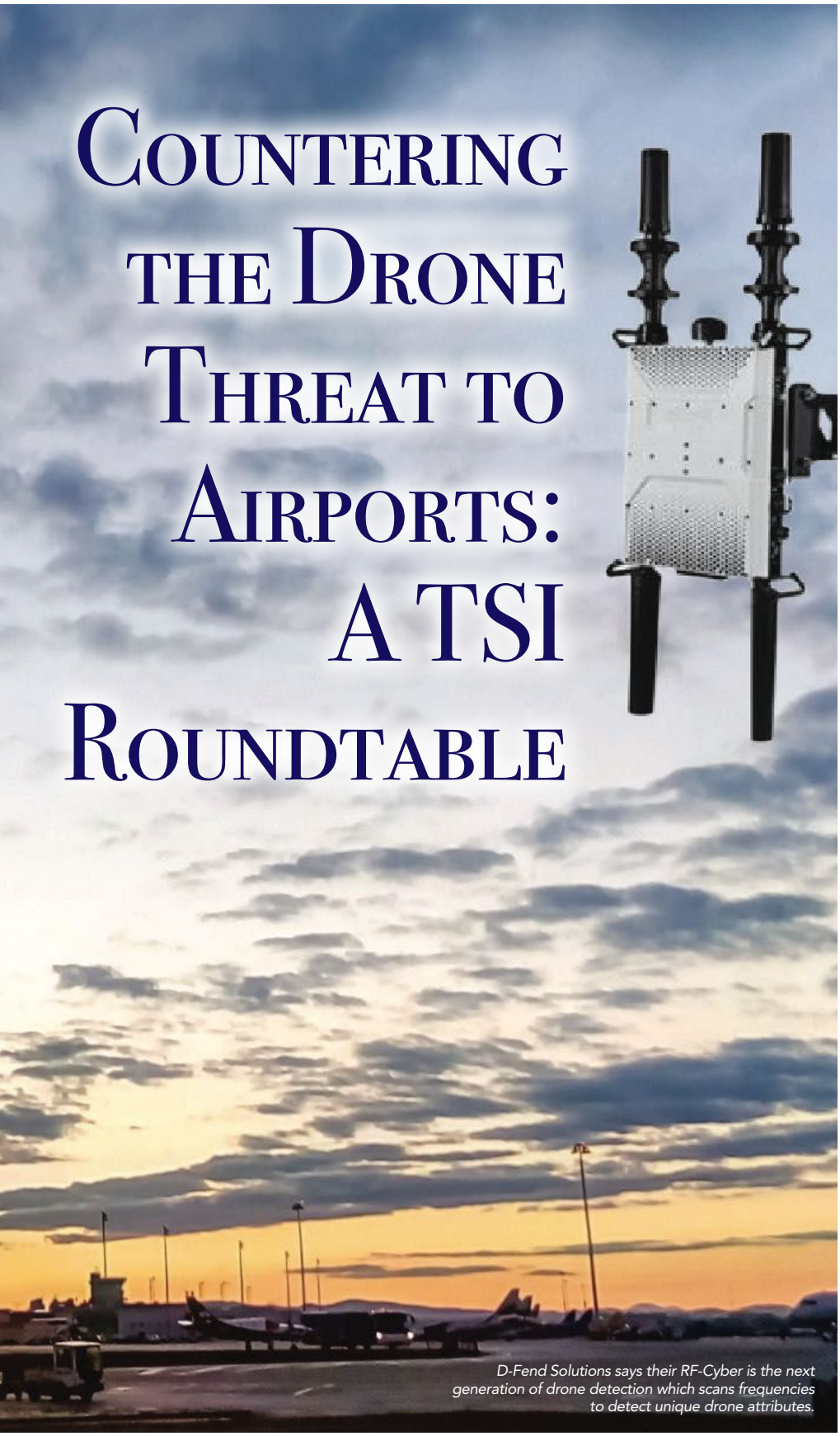
By James Careless

Countering the Drone Threat to Airports: A TSI Roundtable



D-Fend Solutions says their RF-Cyber is the next generation of drone detection which scans frequencies to detect unique drone attributes.

Drone incursions are becoming an increasingly serious problem for the world's airports. In the United States alone, "The FAA receives more than 100 such reports near airports each month,"said the FAA's Drone Sightings Near Airports webpage: www.faa.gov/uas/resources/public_records/uas_sightings_report.

Even in their most benign form, drone incursions represent a serious collision risk for aircraft using airports. This is why the push for "counter-drone" solutions is gaining traction in the aviation world — to neutralize (if possible) the threats posed by drones in these airspaces.

So how serious is the current airport incursion situation, why is it happening, and what can be done to counter it? To find out, TSI magazine has brought together three experts in a virtual roundtable discussion.

Mark Freeman is the director of customer accounts at QinetiQ Target Systems Canada, a maker of defense and security solutions. "While our primary focus at QinetiQ Target Systems Canada is on maritime and aerial uncrewed platforms for test and evaluation, we work closely with QinetiQ Group's broader capabilities in counter-drone technologies," he told TSI. "These include advanced detection, tracking, and mitigation systems designed to protect critical infrastructure and operational environments from evolving drone threats."

Michael Hiatt is chief technology officer at Epirus. Its Leonidas high-power microwave platform is a software-defined, scalable counter-drone solution. "The platform delivers a weaponized electromagnetic interference effect to

Michael Hiatt, Epirus

Mark Freeman, QinetiQ

Jeffrey Starr, D-Fend Solutions

induce a full kill within a drone's critical onboard electronics rather than relying on kinetic destruction or RF disruption," said Hiatt. "This weaponized electromagnetic interference capability means Leonidas is effective where other counter-UAS solutions fall short — particularly against fiber-optic controlled UAS and large swarms."

Jeffrey Starr is chief marketing officer at D-Fend Solutions. It offers RF-cyber counter-drone solutions, specifically designed for sensitive and challenging environments. "Our flagship technology, EnforceAir, moves beyond the 'brute force' methods of the past," Starr said. "Instead of relying on jamming or kinetic projectiles, the technology utilizes radio frequency (RF) cyber technology to detect, locate, and identify rogue drones by analyzing their unique attributes. Crucially, the systems, when allowed by regulations and performed by authorized personnel, can take control of a hostile drone and guide it to a safe landing in a predetermined zone, ensuring continuity and safety." EnforceAir RF-cyber technology is already protecting critical infrastructure, airports, military facilities, and major events worldwide.

TSI: Just how serious a threat are drones to airports today?

Michael Hiatt: Incredibly serious. The drone threat is not hypothetical — UAS [uncrewed aerial systems] represent a real operational risk to airport security and operational continuity. A single small drone can halt departures, delay arrivals and cause delays that ripple across the entire airspace system.

It only takes one drone to disrupt an entire airport. In September 2025, Copenhagen Airport, the busiest in the Nordic region, halted all takeoffs and landings for nearly four hours after drones were spotted in controlled airspace, grounding flights and diverting traffic while authorities investigated. Frankly, I feel that we're lucky there hasn't been an accidental strike resulting in serious loss of life.

Mark Freeman: Drones pose a significant and growing risk to airport operations. Even small consumer drones can disrupt flight schedules, create safety hazards, and cause costly delays. A well-known example occurred at Gatwick Airport in 2018, where drone sightings led to the suspension of flights for over 36 hours, affecting 140,000 passengers and costing millions. This incident highlighted how even unsophisticated drone incursions can have outsized impacts on aviation security.

Jeffrey Starr: The threat is severe and has migrated from the battlefield directly to the homeland. Drones have become a new weapon of choice for bad actors due to their accessibility, low cost, and ability to carry heavy payloads over long distances. For airports, the risk is not just theoretical; it is operational and financial. A single unauthorized drone can cause cascading disruptions.

Just one representative example of many such airport incidents occurred at Luis Muñoz Marín International Airport in Puerto Rico. A drone intrusion there led to the diversion of an incoming flight to the Dominican Republic and caused cascading disruptions for flights across the entire Caribbean region. When a drone halts operations, the economic cost and the safety risks are immediate and serious.

TSI: Is the number of drone incidents at airports increasing?

Freeman: Yes. Global aviation authorities report a steady rise in drone-related incidents near airports. Factors include the proliferation of affordable drones, lack of operator awareness, and deliberate misuse. As drone technology becomes more accessible, the frequency and complexity of incursions are expected to increase.

Starr: Unquestionably. The industry is witnessing a constant and non-stop rise in drone incidents. Since the beginning of last year alone, numerous serious incursions have occurred at major transport hubs and critical sites. The proliferation of drones is driving a commensurate rise in dangerous incidents, and as these devices become cheaper

Epirus says their Leonidas system can defeat hundreds of rogue drones near an airport with targeted bursts of electromagnetic interference without disrupting airliners, air traffic control systems or other nearby infrastructure or personnel. Epirus image.

and more capable, the frequency of these disruptions is accelerating.

Hiatt: Absolutely. In the U.S. and Europe, what were once rare drone sightings are now routine reports that pose increased risks to airport operations. In Europe, high-profile cases like the temporary shutdowns of Copenhagen Airport and Aalborg Airport due to drone incursions highlight a recent spike in disruptive drone activity. In the United States, officials have reported thousands of drone events near major airports since 2021, including hundreds of sightings that forced evasive action by aircraft or contributed to flight delays — and data suggests these events are increasing year-over-year.

TSI: What kinds of drone intrusions are occurring at airports?

Freeman: Intrusions range from accidental incursions by hobbyists unaware of restricted airspace to deliberate disruptions by activists or criminals. More concerning are coordinated attempts to interfere with airport operations or smuggle contraband. The spectrum of threats spans from nuisance-level disruptions to sophisticated attacks targeting critical infrastructure.

QinetiQ Drone Detect and Defeat systems leverages multi-sensor fusion and electronic disruption to neutralize threats safely. QinetiQ image.

Starr: The range of intrusions is dangerously broad. Incidents at sensitive sites broadly may include everything from attacks and collisions to smuggling and espionage. In the airport environment, incidents may manifest as harassment and nuisance disruptions that freeze operations, but the potential for more malicious intent such as surveillance of sensitive areas or even direct targeting of infrastructure, is real. Even clueless operators flying commercially available drones into protected airspace pose risks to aircraft and airports.

TSI: What kinds of actors are flying drones into airport areas, and what are their motivations?

Freeman: Actors include:

- Recreational users unaware of regulations.
- Commercial operators conducting unauthorized filming or inspections.
- Activists seeking publicity through disruption.
- Criminal organizations using drones for smuggling or surveillance.
- State or non-state adversaries testing vulnerabilities or planning attacks.

Motivations range from negligence to deliberate interference with economic or security objectives.

Starr: The actor profile is diverse, which complicates the defense. On one end, there are clueless hobbyists or careless operators who simply don't understand airspace regulations. On the other end, security teams face hostile groups, criminals, and lone opportunists.

Their motivations vary from simple curiosity to smuggling contraband, conducting hostile surveillance, or attempting terror attacks. There is also the weaponization of build or buy DIY drones, effectively transforming them into flying improvised explosive devices (IEDs). Whether the actor is malicious or just negligent, the outcome for an airport, a stopped runway or a collision, is unacceptable.

Hiatt: Actors range from unaware hobbyists to reckless thrill-seekers to deliberate disruptors and perhaps state or non-state aggressors. Findings of investigations aren't always shared with the public, so it's difficult to pinpoint definitive bad actors. That said, the possibility of America's adversaries leveraging drone technology to disrupt airport operations is incredibly real — and likely already happening in my opinion. With major drone manufacturers removing the restrictions on flying in designated No-Drone zones, I think we're likely to see more and more accidental incursions.

TSI: What options exist for countering drone intrusions, including products made by your company?

Hiatt: There's a slew of counter-UAS technologies out there.

The most common is simple EW systems that disrupt the control link or send a "go-home" command to a drone. These basic systems are good against NDAA-compliant drones but minor modifications to the drone's programming or using fiber-optic control will render those C-UAS solutions all but useless.

Kinetic interceptors (think using a missile to intercept a drone) are perhaps most common in military scenarios, but, for obvious reasons, aren't well-suited to protect airports from drone incursions.

Lasers offer dazzling precision but also demand perfect conditions — clear skies, uninterrupted line of sight and sustained tracking. They are costly, difficult to maintain and hamstrung by significant maintenance and power burdens.

Then you have what Epirus develops, high-power microwave, which unlocks a number of advantages: software definition allows for incredibly precise target defeat and makes Epirus HPM a safe and low-to-no collateral capability that's ideally suited for airport security missions. Epirus HPM is also the only effective one-to-many counter-swarm solution. With our Leonidas systems, we could defeat (God forbid) hundreds of rogue drones near an airport with targeted bursts of electromagnetic interference — and without disrupting airliners, air traffic control systems or other nearby infrastructure or personnel.

Freeman: Effective counter-drone strategies combine detection, tracking, identification, and mitigation. Technologies include radar, RF sensors, electro-optical systems, and electronic countermeasures. QinetiQ offers integrated solutions such as Drone Detect and Defeat systems, which leverage multi-sensor fusion and electronic disruption to neutralize threats safely. These systems are designed for deployment at airports and other sensitive sites.

Starr: Legacy technologies like radar, optical sensors, and jammers are often unsuitable for dense airport environments. Radar can be confused by birds; optical sensors need a clear line of sight; and jamming can disrupt critical communications.

The "next generation" option is

RF-Cyber, which is where D-Fend Solutions leads. This technology quietly scans frequencies to detect unique drone attributes. Once a threat is verified, the system can disconnect the rogue drone pilot from the drone, and take control, guiding the drone to a safe landing. This allows for a surgical, non-kinetic mitigation that doesn't disrupt nearby communications and navigation. It is important to note that RF-cyber technology is meant to be used in a way that is performed by authorized personnel and as allowed by local laws and regulations.

TSI: How effective are today's counter-drone tactics, and which airports are using them?

Freeman: Current counter-drone systems are effective against most commercial drones, but challenges remain with swarm tactics and autonomous platforms. Several major international airports have deployed layered counter-drone solutions, often combining radar, RF detection, and jamming technologies. Effectiveness depends on integration with existing air traffic management and rapid response protocols.

Starr: Legacy tactics are increasingly insufficient as a standalone solution. Jamming is risky because it creates interference, and kinetic methods (shooting drones down) are dangerous in a crowded terminal area due to falling debris.

In contrast, RF-Cyber is highly effective because it focuses on control and continuity. It distinguishes between authorized and unauthorized drones, allowing friendly drones to continue working while mitigating the threat. RF-yber technology is currently deployed at sensitive environments across the world, operating alongside radar and other sensors to provide a "surgical tool" for these areas.

TSI: Given the growing complexity and scale of drone attacks, what do makers of counter-drone systems have to do to keep up with them?

Freeman: Manufacturers must innovate continuously to address evolving threats. This includes:

- AI-driven detection and classification to identify drones quickly and accurately.
- Scalable solutions for swarm scenarios.
- Non-kinetic defeat options that minimize collateral risk.
- Integration with airport security and ATC systems for real-time decision-making.
- Cyber resilience and compliance with aviation safety standards are also critical.

Starr: Operators and providers must shift from a hardware-centric to a software-centric mindset. The threat evolves faster than hardware can be replaced. Drones are becoming smarter, using AI mission planning, complex protocols, and swarm behaviors.

To keep up, systems must foresee the drone future and always stay one step ahead. This means utilizing software-driven solutions that allow for rapid, modular updates to counter new drone models and protocols as they appear. Open architecture is also essential, ensuring systems can integrate seamlessly with existing command-and-control layers to form a robust, multi-layered defense.

Hiatt: I think what's most important is for counter-drone tactics to evolve as fast as drone threats themselves. Drone manufacturers are moving to encrypted links and more sophisticated antenna systems that are harder to jam or take over with protocol attacks. Custom-built drones are moving to fiber-optic control so there are no control signals to detect or jam. While not on the battlefield today, fully autonomous drones are currently being tested and will likely be available soon.

Counter-UAS systems must be scalable, adaptable and software-driven to enable rapid updates via field software updates. Static solutions can't keep pace with evolving drone types, autonomy or swarm tactics. Continuous updates and flexible architectures are essential. These are all core capabilities of Epirus' Leonidas HPM platform.

TSI: What do you see as the future of counter-drone systems for airports, including any new advances that your company is working on?

Hiatt: In my mind, the future of counter-UAS is integrated, layered and non-kinetic. Systems that can address single drones and complex swarm scenarios while remaining safe for people, aircraft and infrastructure should be prioritized by airport security decision-makers and lawmakers alike. Epirus is focused on developing systems that meet all these requirements and I'm confident our technology will prove integral to airport drone defense across the globe.

Freeman: The future lies in networked, autonomous counter-drone ecosystems that combine AI, sensor fusion, and automated response. Advances will include predictive analytics to anticipate incursions and cloud-based coordination across multiple sites. QinetiQ is investing in next-generation detection and defeat technologies, including low-collateral RF disruption and AI-enhanced tracking, to ensure airports remain secure against increasingly sophisticated threats.

Starr: The future is defined by integration and intelligence. There will be a doctrinal shift where RF-Cyber is the forefront of a layered defense, supported by legacy sensors when necessary.

Advanced capabilities will not just stop the drone, but, when permitted, capture intelligence. By recovering rogue drones intact via a controlled landing, security agencies are provided with the drone and forensics that can lead to the apprehension of the rogue drone pilot and the prevention of future attacks. Focus is also being placed on automation and AI, enabling systems to either autonomously or manually identify, track, and mitigate threats with even greater speed and precision. The goal is simple: airspace safety with zero disruption to the passengers and planes that rely on it.