Playing Defense

Uncertain Regulations Stall the Implementation of Counter-UAS Technology in The U.S.

In early September 2019, a radical environmentalist group called "Heathrow Pause" threatened to shut down Heathrow Airport in the UK by flying drones within the airport's no-fly zone to call attention to climate change. Some Heathrow Pause members were arrested the day before their previously announced fly-date (9/13) and on the day itself their drones were unable to take off, electronically jammed by the authorities.

The protest represents a new wrinkle in the fast-moving world of unmanned aircraft systems (UAS) use and integration. As previous drone-induced airport disruptions at Heathrow and Gatwick in the UK and at Newark Airport, New Jersey in the U.S. demonstrate, society will need to prevent as well as facilitate drone use in daily life.

The recognition has kick-started a counter-UAS (CUAS) industry that's now trying to market itself to civilian

A rendering showing potential SkyDome AI protection of the city of Dubai, facilitated by Fortem's networked TrueView radar. (Fortem Technologies)

Cov ToC

clients. A raft of companies have emerged to provide CUAS services but their growth has been hampered by limited real-world experience and technical approaches constrained by civil oversight authority and U.S. laws.

Finding and Stopping Drones

Most experts agree that a layered drone defense is the best protection for critical infrastructure and other entities. That's an assessment embraced by firms like Utah-based Fortem Technologies. Formed in 2016 and backed by investment from Boeing's venture capital arm (Horizon X), Fortem offers complete detection and mitigation solutions to potential customers. The company refers to its integrated system approach as "Security Elevated", in essence taking site security above and beyond the fence line.

Preventing unwanted drone flight into an area – whether airport, football stadium, nuclear reactor or government building – is a two-part problem. First, the drone(s) must be de-

A head-on view of the Drone Hunter interceptor drone with its low power FMCW TrueView radar mounted above two net guns for capturing rogue drones. (Fortem Technologies)

tected and its location/flight path determined. Second, it must be stopped, diverted or destroyed. In the CUAS business these problems are called "detection" and "mitigation".

You can further break detection down into passive and active methods. The most basic approach is visual, using cameras, scopes and eyeballs to detect approaching drones. Visual detection is passive, generally avoiding interference with other systems or people.

But small drones are hard to see. That has led to development of other passive approaches including acoustic, infrared and RF monitoring systems. The latter effectively 'listen' for radio signals from a drone's pilot (via a controller) to the drone. They may also eventually take data from an FAA-approved database system called "Remote Identification" which could require small UAS to broadcast ID data from an onboard transponder or transmit in real-time to an internet network.

An artist's rendering of the protective AI-enabled SkyDome over a stadium in Jakarta, Indonesia. SkyDome offers 180-degree horizon-to-horizon detection around the entirety of the facility. (Fortem Technologies)

With Remote ID yet to be realized and physical limits on the effective range of many passive systems, there's a place for active methods too, principally radar. Though it can be affected by line-of-sight issues, radar can effectively spot small drones including those which may be partially autonomous or non-emitting – the sort malicious actors might use. However, distinguishing a small UAS from a bird with radar alone is difficult. That problem can be overcome by pairing radar with artificial intelligence (AI) enabled software.

Mitigation can be kinetic or non-kinetic. The former generally means shooting down the drone with a gun or laser, or capturing it with a net. Non-kinetic methods include jamming (breaking the link between controller and drone), cyber manipulation (breaking drone encryption and taking control) or geofencing (designating areas into which cooperative drones are programmed not to fly).

Kinetic and non-kinetic mitigation approaches come with undesirable side effects. Shooting a drone down may cause collateral damage as it falls, or from missing the target. Jamming drones can disable other nearby systems from mobile phones to radio communications and radar. Breaking control links may leave drones to fly uncontrolled. Defeating encryption puts the impetus (and responsibility) for drone control on the CUAS provider. Geofencing may restrict legitimate commercial or civil service activity. Legal limitations impact detection and mitigation systems as well.

Fortem's layered drone defense is brought together in its SkyDome system, an adaptable AI platform that fuses the company's TrueView® radar and other sensors (optical, thermal) to autonomously monitor an environment in three dimensions. The use of AI to classify objects and patterns in its airspace allows clients to dismiss many targets (including drones) which don't present a threat, reducing the false-positive problem common to CUAS systems.

When the system detects and anticipates a threat, it can alert personnel or launch one of the company's DroneHunter® interceptors to neutralize dangerous or malicious drones. Fortem can configure DroneHunter on a variety of drone platforms depending on the interceptor performance the customer requires. When launched, the interceptor leverages Fortem's TrueView radar to autonomously detect, pursue and capture the offending drone(s) with its onboard net-capture effector. Firing a net, rather than destroying or diverting the malicious drone, allows for forensic analysis of the craft.

Though other CUAS providers offer radar-based detection, Fortem's networked radar departs from typical single location radar arrays. TrueView is a miniaturized, low power FM continuous wave radar in a small package that can be placed on a drone or at ground locations around a protected site (potentially even a city). Networked together, the small radars can provide airspace awareness both at the perimeter and in a complete arc, or "dome", above the site. Combined with other sensor input and AI, the company says TrueView offers awareness beyond simple drone detection.

"That's why SkyDome was created, to maintain a persistent view of what's happening in an airspace for all kinds of drones," says Fortem CEO, Timothy Bean. He adds that non-emitting drones are detected as well. "In a criminal situation, there's often no RF to detect. Our system uses physics to detect everything in the airspace."

The Authority Bottleneck

Measuring the effectiveness of layered systems like SkyDome is difficult in the U.S. aside from test scenarios because as of late 2019, only the federal government is permitted to employ CUAS systems. The 2018 Federal Aviation Administration Reauthorization Act gave the Department of Homeland Security and Justice Department the right to "disrupt," "exercise control of" or "seize or otherwise confiscate" drones deemed a "credible threat" without a warrant. Those provisions will likely face legal challenges and they do little to clarify the commercial market where shooting down or disabling drones remains illegal. There is no liability framework for such operations. Likewise, there is no CUAS certification regime and thus no standard against which to measure the relative performance of the systems now offered.

"The biggest thing we need is regulatory clarity," Fortem CTO, Adam Robertson affirms. "What are the issues with collateral damage? If you light up an RF countermeasure in an airport environment for example, are you going to do more harm than good? Does a government guy have to press the button? Could a contractor operate [a CUAS system] in a proxy situation? Could we have counter UAS-as-a-service?"

Even passive detection systems could run afoul of American law. The federal

Wiretap Act prevents law enforcement departments from intercepting "wire, oral or electronic" communications without a court order. The pen register law prevents the use of pen register or "trap and trace" devices that trace telephone calls, including cellular and, putatively, drone communications. The restrictions apply to law enforcement, but the code is silent on private CUAS operators, creating confusion and potential liability.

"That's still in the legal court of debate," Phil Pitsky, VP of US Federal Operations for Virginia-based CUAS provider, Dedrone acknowledges. Dedrone differs from Fortem in that it principally provides detection solutions, leaving mitigation to its partners. The company also sticks primarily to passive detection, pairing AI with RF detection. Pitsky emphasizes that Dedrone monitors the RF environment at the "unclassified level", scooping signal data but not personal identifiable information (PII).

With the Department of Justice yet to clarify what RF information commercial CUAS detection firms may gather, the company is being careful.

"We aren't going inside the [RF] links and de-crypting," Pitsky explains. "There are other [commercial] systems that do that which is a more overt violation of the [pen register laws] than just capturing back addresses transmitted in the clear."

Dedrone's VP agrees with Fortem's CTO that the delay in crafting clear CUAS regulations has the industry on pause. That pause affects potential collateral revenue as well. The detection technologies and forensics touted by CUAS providers could be rich sources of business intelligence.

"We expect this data to be extremely valuable," Fortem's Adam Robertson allows. Robertson points to extant open source business intelligence gathering like hedge funds using satellite imagery to detect corporate employment levels, traffic, and more as precedent.

Fortem also offers the tantalizing prospect of using its networked TrueView radars in cities to facilitate the air traffic management necessary for unmanned urban air mobility (UAM). While that's a longer term possibility, the threat from the seven million drones the FAA predicts will be in the air by 2020 cannot be ignored – a lesson that Gatwick airport operators learned in 2018.

"They hadn't digitized the airspace directly overhead to have a persistent view of a drone," Timothy Bean asserts. "You really need that, especially if it's going to be replaced by another in 20 minutes."

Counter UAS regulations may be on hold but there will be no pause in the threat from drones.

This article was written by Eric Tegler, Freelance Technical Writer, Fortem Technologies (Pleasant Grove, UT). For more information, visit ***http://info.hotims.com/76503-500.***