Unmanned Aviation

Building A Counter-UAS Market That Does Not Exist

Aviation Week & Space Technology Apr 09, 2019

Eric Tegler Washington

Onera

Six months ago, few outside the defense community in the UK and U.S. understood what the words “counter-unmanned aircraft systems” meant. But a succession of reported drone incursions at London’s Gatwick and Heathrow airports and Newark Liberty International Airport in New Jersey, which also serves New York City, changed that. Now the need to protect airports and other infrastructure from rogue unmanned aircraft systems (UAS) seems obvious. So, too, does a market for commercial counter-UAS (CUAS)

As of yet, however, there is no such market. In the U.S. and many other countries, shooting down, disabling or taking control of drones is illegal. There is no liability framework for such operations, no broadly reliable way to detect and identify drones and drone users, and the U.S. has yet to figure out exactly who will have authority to execute CUAS operations.

The FAA plans further evaluations of counter-UAS systems at airports

Potential CUAS buyers face a lack of information and viable solutions

Potential CUAS buyers lack information and viable solutions. There is no CUAS certification regime and thus no standard against which to measure the relative performance of the systems now offered. Despite a crowd of companies promoting potential products, there are few providers globally with systems ready to field. And outside sporadic battlefield experience, CUAS systems have no real-world track record.

From jamming and cybermanipulation to kinetics and even drone-capturing nets, the handful of active countermeasures now marketed all present potential negative side effects. Ironically, the mitigation portion of the CUAS puzzle requires its own mitigation.

“What this really is,” says Mark McKinnon, an attorney with Washington-based law firm LeClairRyan, “is a chicken-and-egg situation. But you need the chicken and the egg at the same time.”

Airports are not the only land users concerned about drones. Utilities, telecommunication providers, prisons, sports stadiums and even entire cities warily eye their threat potential. However, the safety implications of what airports do should put them at the forefront of counter-UAS advocacy. Or so you would think.

Related Content

Related Articles

Counter-UAS Special Report: The Countermeasures Options

Drone ‘Angst’ Extends Beyond Backyard Spying

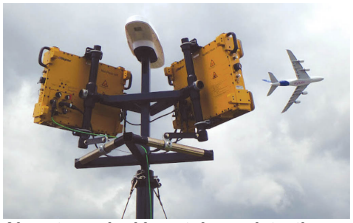
Boeing Warns Against Long Stealth Fighter Development

The Week In Technology, Sept. 19-23, 2016

The Week In Technology, Nov. 7-11, 2016

Aviation Week contacted the administration at Hartsfield-Jackson Atlanta International, the world's busiest airport. The airport's brief emailed response to a query about CUAS was that we would have to talk to the FAA. For Christopher Oswald, senior vice president for safety and regulatory affairs at the Airports Council International-North America (ACI-NA), Hartsfield-Jackson's response is not a complete surprise.

"Airports face significant hurdles in getting authorization to use [CUAS] systems. There isn't a legal framework in which U.S. airport operators would feel empowered to acquire and use them," he says.



Airports are looking at drone-detection systems that have already been deployed by the military, such as the UK-developed anti-UAV defense system. Credit: Liteye Systems

He adds that a July 2018 CUAS guidance letter from the FAA's Office of Airport Safety and Standards suggests even drone detection is a shaky near-term prospect, likely explaining airports' reluctance to comment. It repeated an admonishment from an earlier letter from 2016 which stated: "It is important that federally obligated airports understand that the FAA has not authorized any UAS detection or countermeasure assessments at any airports other than those participating in the FAA's UAS detection program . . . and airports allowing such evaluations could be in violation of their grant assurances."

The 2018 follow-up urged further caution based on the agency's own counter-drone study, stating: "The low technical readiness of [CUAS] systems, combined with a multitude of other factors, such as geography, interference, location of majority of reported UAS sightings, and cost of deployment and operation, demonstrate this technology is not ready for use in domestic civil airport environments."

Among the letter's assessments was that airport environments had numerous sources of potential radio-frequency interference—"more than anticipated." Their dense environments made drone detection difficult "and, in some instances, not possible."

A range of challenges was enumerated: a high level of manpower required to operate equipment and discern false positives, large numbers of sensors needed to achieve required coverage, communication/navigation interference, the deployment of CUAS assets in an environment owned by many entities, prohibitive costs and rapid technological obsolescence.

The FAA will gather more information this year, deploying CUAS systems at five airports to evaluate potential aviation safety risks and efficacy. An aviation rule-making committee is also being established to make recommendations for CUAS standards.

French research agency Onera is looking at ways to protect the country's nuclear power stations from drone threats. Credit: Onera

The challenges articulated largely leave aside broader legal questions that must be answered before a meaningful counter-UAS market can develop. Common approaches to detecting and mitigating unwanted UAS run afoul of the Communications Act of 1934, the U.S. Criminal Code and Federal Communications Commission and FAA regulations.

For example, the Communications Act requires that radio transmitters including jammers be licensed. No CUAS jamming system has been licensed, nor has a licensing mechanism been established. Willfully destroying or disabling an aircraft is prohibited by the U.S. Criminal Code, as is intentional interference with satellite communications. "The FAA can't rewrite those laws," Oswald observes. "Congress has to rewrite them and recognize what would be lawful activity in a drone era."

With passage of the 2018 Federal Aviation Administration Reauthorization Act, Congress has rewritten some of those laws, giving 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. The provisions will likely face legal challenges, and they do little to clarify the commercial market for CUAS providers, McKinnon says.

"It's really tricky because the provisions are generally limited to operation by the federal government itself. This would not give [CUAS companies] broader authority to market the same technology to state or local governments or individuals," he says.

The new grants also imply a strictly federal approach to CUAS for the time being. Airports themselves differ on assuming drone-detection and mitigation responsibility, Oswald reports. Smaller operators tend to see local enforcement authorities (with proper resources) as better equipped to undertake CUAS. Larger airports, which have already incorporated anti-terror, active-shooter and portable anti-aircraft missile responsibility, may see CUAS as a logical extension of their own capabilities.

"They've had to be prepared to address those situations," Oswald affirms. "I think there's also a reality check on what level of federal resources there would be to respond in a tactical sense [to drone incursions]."

There has been no official confirmation of actual detection of UAVs at Gatwick, or Heathrow, nor at Newark or elsewhere in the U.S. Drone incursions have not drawn attention at other U.S. civilian facilities, and success on the battlefield is difficult for even the military to assess.

Vendors thus face the prospect of selling detection and mitigation systems without real-world examples of their efficacy. It is a thorny problem for CUAS manufacturers and potential customers, says Oleg Vornik, the CEO of Drone-Shield, a U.S.- and Australia-based company providing multisensor fixed/mobile drone detection and jamming. It says it operates in 50 countries and has recently sold equipment in Kuwait.

Vornik describes a global sales model in which airports run controlled trials of prospective CUAS systems, installing them for a few weeks at a time, operating them and assessing performance. The idea is contingent upon drones entering the relevant airspace, something airport operators would have to arrange themselves unless the CUAS provider offers to fly drones in. The latter is like having a car salesman test-drive the car for you, however.

“This is a nascent technology, and there’s no perfect answer,” says Vornik. “We would love to have a mandated set of requirements [against which competing systems are measured] and then airports or others choose from those [companies] that are certified. That doesn’t exist, but doing something is better than doing nothing.”

He estimates there are only about six CUAS providers capable of fielding potentially effective systems. “If you do a Google search, sure, you get a couple hundred firms that pop up, pretending they’re in the counter-drone space. But customers tend to be quite savvy, especially in the airport sector, and can tell the difference between two guys with an idea and an established company,” he says.

Among mitigation approaches, “smart” jamming seems to hold the most potential, says Grant Jordan, CEO of SkySafe, a San Diego-based company that has trialed ATV-mounted detection/jamming systems with the U.S. Naval Special Warfare Command.

“From our perspective, [radio-frequency] solutions get you 90% of the way there. They’re the best, most scalable solutions in the greatest number of real-world situations. But there will always be situations in which a kinetic system is required,” he says.

Anecdotal reporting from the battlefield suggests that kinetics (i.e., shooting down drones) is the only truly effective countermeasure. The Pentagon declines to confirm this, citing classification concerns and limited real-world metrics. Kinetic mitigation obviously creates significant safety and liability concerns in a civilian environment. Other approaches such as geofencing are less than optimal as well.

Actually taking control of rogue drones comes with a high degree of difficulty, he says. “We don’t love taking control of the drone because it’s so dependent on exploring vulnerabilities of the underlying protocol. You’re basically hacking into an encrypted connection. You’re fighting against the tide,” Vornik says. It is a perpetual cybercat-and-mouse game, which he says leads to a 50-50 chance of defeating a drone. And if a CUAS system assumes flight control of a UAV, it also potentially assumes liability for the aircraft.

“No system is a silver bullet,” ACI-NA’s Oswald agrees. Layered detection/mitigation solutions may be the only guarantor of sufficient success, an expensive proposition.

So what is an airport to do? Plan.

“Beefing up and enhancing UAS contingency planning is ongoing, especially since Gatwick,” says Oswald. “Even small airports are looking at drone contingency plans and tabletop exercises.”

The hope of airport operators is that FAA CUAS test sites can serve as proof-of-concept labs. Along with regulators and lawmakers, they will have to produce both chickens and eggs before a true commercial CUAS market emerges.

Editor's note: This article was updated to clarify the Pentagon view of effective counter-UAS.