BREAKING DEFENSE | COUNTER UAS eBRIEF

DRONES AN "IMMEDIATE THREAT":

DoD Plans Rapid Acquisition of Counter-UAS Systems

AN EDITORIAL BRIEF SPONSORED BY FLIR®


FLIR
INTEGRATED SOLUTIONS FOR C-UAS
Today's emerging threat is small, easily deployed, difficult to detect, and potentially lethal. FLIR provides a reliable countermeasure against drone threats to accurately detect, classify and track numerous drones simultaneously with man portable, fixed or mobile solutions to accommodate different missions, and can easily be integrated with defeat mechanisms.
LEARN MORE AT
FLIR.COM/SURVEILLANCE/INTEGRATED-SOLUTIONS

THE SITREP:

THE EMERGENCE OF DRONE WARFARE LEADS TO NEW ANTI-DRONE TECHNOLOGIES

The urgency to protect troops, bases, and installations from drone attacks changed forever on September 14, 2019. That's when a swarm of small, low-flying drones unleashed by Yemen's Iranian-backed Houthi rebels targeted Saudi Arabia's oil processing facilities at Abqaiq—causing hundreds of millions of dollars in damage, temporarily cutting the kingdom's oil production in half, and spiking global crude oil prices.

Even though the oil facility was protected by three Skyguard short-range air defense batteries from Germany, a U.S. Patriot surface-to-air missile defense system, and a French Shahine (Crotale) short-range anti-air missile system, none of the approximately 10 drones were destroyed before striking their target.

In essence, Saudi Arabia had prepared for a nation-state battle with ballistic missiles and was unprepared for guerilla warfare of the type launched by the Islamic, anti-U.S., anti-Israel Houthi movement. The attack was nothing less than a Pearl Harbor-type wake-up call for the need to counter unmanned aerial systems with defense technology commonly referred to as C-UAS.

That's the assessment that Under Secretary of Defense for Acquisition and Sustainment Ellen Lord heard in late 2019 when she met with military leaders in Iraq, Qatar, and Afghanistan. Her discussions centered around the need to identify and understand urgent C-UAS needs so they can be developed and acquired using the Pentagon's rapid acquisition authority.

"The one takeaway from all of my visits is that we need to continue to focus heavily on counter-UAS systems and strategies," said Lord during a press briefing in December. "This remains a top priority for the department, and I will continue to engage with Congress and the defense industry on ways ahead.

"We must balance the requirements to maintain our current platforms for the immediate threat, develop new technology to ensure we can dominate in a future fight, and change the way we do business to access the power and progress of the commercial sector. Counter-UAS is an excellent example of this balance."

– Barry Rosenberg
Contributing Editor, Breaking Defense

BRINGING ORDER TO C-UAS DEVELOPMENT & FIELDING

One of the first steps taken by the DoD to codify C-UAS efforts came earlier this year when it established a new 60-person team led by Army Maj. Gen. Sean Gainey, deputy director of force protection (J8) on the Joint Staff. The team's charge is to centralize policy and requirements, and field systems that will protect U.S. bases and installations in both the homeland and overseas. Development of portable and mobile C-UAS systems that can protect ground forces and vehicles are part of the team's charter. The team's first C-UAS proposals are expected in April.

"One of the threats seen in every AOR and CONUS is a variety of different drones coming toward our military installations," said Lord, referring to the acronyms for combatant commands' areas of responsibility (AOR) and the contiguous United States (CONUS). They are "often small (and) difficult to detect with typical sensor packages we have. We have had each of the services and a number of agencies over the last few years focused on trying to come up with systems to combat this."

Bagram Air Base in Afghanistan is one of many military bases around the world that the DoD wants to protect from enemy drones. Shown is a C-17 Globemaster III being loaded at Bagram.

It will be the job of the C-UAS team to coalesce those disparate service and agency efforts into one set of standards to help DoD qualify systems developed by industry, and then to identify those with both the sensor modalities to detect attacking drones and either kinetic or electronic warfare-type systems to neutralize the drone threat.

"My goal is to make sure we have three-to-five systems that are tailored to different types of threats, (for which) we can get economies of scale (with) a few best systems," said Lord. While much of industry's C-UAS development targets small hard-to-detect drones, the DoD effort will also extend to large Group 5 UAS that may be rough equivalents of the armed MG-9 Reaper and the high-flying surveillance RQ-4 Global Hawk.

Lord also noted the need for C-UAS systems to more effectively use multiple means of detection, for example combining electro-optical and infrared sensors with radar systems, and by integrating multiple defeat systems such as jamming and spoofing. Doing so increases the probability that a C-UAS system accurately identifies a drone threat and can deter it. Along with the C-UAS systems themselves must also come the training and logistics tail to support them, Lord added .

As part of DoD's consolidation efforts, the Army was named earlier this year as the executive agent for all DoD-wide C-UAS efforts. Playing a key role will be the Army's Rapid Equipping Force (REF), the Ft. Belvoir-based organization responsible for turning current and emerging technologies into solutions that meet urgent challenges. The REF's program priorities are: expeditionary force protection to include C-UAS; development of persistent-duration UAS; subterranean operations; electronic warfare tactical vehicles; and squad intelligence, surveillance, and reconnaissance.

"REF's counter-UAS priorities are to find solutions that are capable of detecting, identifying, and defeating the UAS threat," LTC Christian Van Keuren, REF solution team chief, told Breaking Defense. "The REF seeks solutions that are rapidly deployable, easy and safe to operate, highly reliable and self-contained, and sustainable by soldiers and Army units.

"Of note, we are seeking solutions that will enhance a tactical unit's understanding of their environment in order to bolster force protection in challenging terrain and austere environments."

In addition, another objective of the DOD's C-UAS efforts is to address the interoperability of future C-UAS procurements. That is key to ensuring that new systems can work seamlessly with existing architecture and comply with host nation laws and regulations, as many countries ban signal jamming devices, for example. In doing so, the military hopes to avoid mistakes it made after 9/11 by acquiring new technologies that met urgent needs—such as communications and information systems—but had to be later scrapped because of interoperability issues with coalition forces.

The key to interoperability is of course standardization. Industry experts observe that more C-UAS systems

are being developed using standards from the National Institute of Standards and Technology and the International Society of Automation, both of which have published standards for cybersecurity and C-UAS technologies like night-vision systems.

THE MAIN ELEMENTS OF COUNTER UAS

Preventing drones from spying upon or attacking military installations (as well as commercial facilities such as power plants or oil fields) is a three-step process. The first is detecting the threat, the second is classifying the detection so you know what you're looking at, the third is defeating the drone by neutralizing it.

While technologies related to detection and defeat are constantly improving, the most significant advances in C-UAS systems are expected to come in the area of classification through the use of artificial intelligence (AI), which will also improve the speed at which the detect/classify/defeat process can take place.

"You want to automate the process as much as possible to take a human operator out of the loop to control the number of false positives and false negative you receive," explained Nick Lagadinos, FLIR Systems technical director for gimbal systems (stabilized EO/IR systems).

"The artificial intelligence piece is what's going to hit the sweet spot in classification by analyzing data in real time from various forms of detection like radar, EO/IR, acoustics—maybe even LIDAR (which develops 3D images of an object using laser light). It will tell the operators whether they need to pay attention to a potential target or not, significantly helping to reduce fatigue factor and loss of efficiency that people experience after viewing video and looking at radar dots over an 8-10-hour shift.

"And with AI-enabled neural networks, which are really good at understanding images, you can assign a probability of certainty to the classification so you can adjust your threshold to when it sets off an alarm that requires human attention. AI-enabled automation will make operators more accurate and fresher in their ability to solve problems, which the government has said repeatedly is a capability desperately needed."

THE HOWS AND WHYS OF C-UAS

With counter-UAS systems a global need for militaries, it's no surprise that there are hundreds of different systems being developed around the world that use multiple means for both detection and interdiction (defeat) of unmanned aerial systems.

A U.S. Marine programs a C-UAS system during training at Marine Corps Air Ground Combat Center, Twentynine Palms, CA.

Drones are typically detected and tracked through six different ways: radar, radio frequency (RF), electro-optical (EO), infrared (IR), acoustic, and through combined sensors.

RADAR: These systems emit radio-frequency pulses that bounce off unmanned aircraft to create radar signatures. Algorithms are then applied to the signatures to differentiate between actual UAS targets and other low-flying objects like birds. The DoD's focus has lately been on a variation of radar called moving target radar. Unlike standard radar it is able to ignore stationary objects, which is particularly valuable in urban environments so the system doesn't get echoes from buildings—only from moving targets. One drawback to all types of radar is that small drones flying at low altitudes can sometimes be hard to detect.

RADIO-FREQUENCY: Unmanned systems are controlled over publicly known radio frequencies, and RF detectors scan for those frequencies. Algorithms then identify RF-emitting devices like drones and spot their location. These systems, however, need direct line of sight with the target in order to be effective. The same is true of EO and IR sensors.

ELECTRO-OPTICAL: Using cameras to detect drones, these systems identify targets through their visual signatures. Sometimes, though, EO systems have trouble distinguishing between unmanned systems, birds, and small aircraft. They're also limited to daytime use.

INFRARED (IR): Detection is made by zeroing in on heat signatures from the UAV structure itself, ss well as the engines and exhaust.

ACOUSTIC: Drone engines make noise and each one produces a recognizable sound. Identification is made by matching the sound of a motor with individual engine signatures stored in a database. The limiting factor of acoustic detection is that adversaries can develop heretofore unknown drones with never-recorded engine signatures, which means they won't be identified as potential threats. The same can be said of RF sensors, too, which also depend on a library of frequencies.

COMBINED SENSORS: Some systems use a combination of sensors to improve the accuracy of drone detection in order to reduce false alerts. For example, an acoustic sensor that detects engine sound can then cue an EO or IR detector to confirm an incoming drone.

There is an even greater variety of ways that C-UAS can interdict drones, including: RF jamming, disruption of the Global Navigation Satellite System (GNSS) satellite link, spoofing, laser, nets, and projectiles.

- **RF Jamming:** With this method, the radio frequency on which the drone operates is disrupting by flooding the area with RF output. When a UAS loses its signal it typically lands or is programmed to return home.
- **GNSS Jamming:** Here the drone's satellite link, typically Global Positioning System or Russia's Global Navigation Satellite System, is jammed. This also causes the drone to land or fly home.
- **Spoofing:** This interdiction method sends fake GNSS signals to the drone allowing the C-UAS system to take over control of the UAS.
- **Laser:** Aimed at the body of the drone, lasers and directed energy disable it and cause the drone to crash.
- **Nets:** With this method, a net is shot at the drone much like a rolled up t-shirt is shot into the crowd at a baseball game. The net entangles the drone and brings it to the ground.
- **Projectile:** Like lasers, this kinetic method is designed to bring down a drone by hitting it with a projectile.
- **Combined Elements:** Like combined detection methods, interdiction can include a variety of elements. Ones that typically work well together include RF and GNSS jamming.

Determining the right mix of detection and defeat technologies will depend on the specific operational environment and requirements.

Soldiers from Echo Battery, 6-52 Air and Missile Defense Battalion, established the first garrison counter-UAS defense capability in the Korean Theater of Operations in 2019. E/6-52 provides C-UAS protection in the garrison environment on Camp Carroll, South Korea, which includes the integration of new systems into normal Short Range Air Defense (SHORAD) operations.

"For example, if you're at a forward base, you might decide that moving target radar and electro-optical are your two best detection mechanisms because the amount of signal to noise in those spectrums would probably be to your advantage," explained FLIR's Lagadinos. "At the end of the day, the more spectrum you can analyze for detection classification the higher your accuracy is going to be.

"For an urban environment, if you were trying to protect an event like the Boston Marathon, for example, you might decide that RF and LIDAR (which is good at detecting size and shape) are more efficient. I'm not saying that they definitely are, but perhaps two different detection mechanisms are better in an urban environment, while two different ones are more effective for a deployed base where the kinds of motion you have are different."

Likewise on the defeat side, directed energy and projectiles wouldn't necessarily be the technology of choice for an urban environment because you don't want the drone crashing into buildings and populated areas. Better technologies in that situation would be jamming and spoofing.

C-UAS systems typically find themselves affixed to three types of platforms: (1) ground-based systems that are fixed or mobile (on a vehicle, for example); (2) hand-held systems like gun-shaped devices that shoot nets, as an example; and (3) and airborne systems designed for installation on other unmanned aerial vehicles that can intercept targets and deploy countermeasures like an explosive device.

Troopers from the 3rd Cavalry Regiment operate the Drone Defender during a C-UAS drill while deployed to Iraq in 2018.

CHARACTERIZING THE WORLD'S C-UAS SYSTEMS INTO THOSE THAT DETECT AND/OR DEFEAT

The majority of detection systems use only one sensor type, according to the 2018 Counter-Drone Systems report from the non-profit Center for the Study of the Drone at Bard College which examined all the world's known C-UAS systems. However, a significant number do rely on a combination of two or more sensors. The Bard report highlights several features as they relate to detection and interdiction:

THE DETECTION SIDE

- There are 235 C-UAS systems (including both detection systems and interdiction systems) sold by 155 organizations in 33 countries. This includes those in active development but yet to be deployed.
- Eighty eight systems are detection only, 80 are interdiction only, while 67 can do both.
- Of the total, 177 are ground-based systems. Thirty five are handheld and 18 are airborne mounted on a unmanned system.
- There are 155 systems that can detect drones, with 95 of them using only one sensor. Infrared is used by 53 systems, while 21 rely on an acoustic sensor. Sixty employ two or more sensors.

THE INTERDICTION SIDE

- Bard identified 147 systems designed to defeat drones. About half of them use only one technique to disrupt or destroy drones, with the other half rely on two or more.
- Jamming of RF and GNSS signals are the most prevalent means of interdiction, and 88 systems depend solely on jamming. Another eight systems use jamming plus a second technique.
- Spoofing is found on 12 systems.
- Lasers or projectiles are the primary interdiction means for 30 systems, and 5 others employ a combination of jamming and kinetics.

The greatest challenge for developers of C-UAS technology will be staying ahead of new drone designs that can evade detection, such as reducing radar signatures or dampening engine noise.

"Drone technology itself is not standing still," the Bard report states. "The C-UAS market will therefore have to constantly respond to new advances in unmanned aircraft technology. As the unmanned aircraft systems market expands, counter-drone systems will need to be flexible enough to detect and neutralize a growing variety of targets, ranging from large unmanned aircraft capable of carrying heavy payloads to low-flying micro surveillance drones that might only weigh a few grams."

VIEWPOINT FROM FLIR

ADDRESSING THE DOD'S C-UAS NEEDS WITH NEW CAPABILITIES, INTEROPERABILITY, AND IMPROVED SWAP

Nick Lagadinos, FLIR Systems technical director for gimbal systems (stabilized EO/IR systems)

1 Where is the U.S. need for C-UAS most urgent: military installations overseas? military installations in the U.S.? airports and utilities in the homeland? elsewhere? How do FLIR detection systems help to protect those urgent needs?

Currently the most urgent need for C-UAS is for our warfighters that are deployed at military installations OCONUS. However, we must be mindful that the threat exists inside the United States, as well. It is important for defense-solution providers to work together with DoD to bring forward meaningful capabilities to combat or neutralize these threats. FLIR is currently engaged with a number of government agencies developing, testing and deploying capabilities for all aspects of the C-UAS mission.

2 Tell us about your development efforts to make your sensors lighter with improved sensitivity and usability.

FLIR is integrating new vision processor capability embedded in our electronic architecture of our electro-optic and infrared (EO/IR) imaging systems. The vision processor provides built in computational resources to tie together many sensing and imaging technologies, including artificial intelligence, without adding additional components to the system, ultimately reducing the size, weight, power, and effectiveness of the solution.

3 Describe your prioritization of technology development as it relates to detection/ sensor technologies.

FLIR is engaged in many technologies for detection, sensing, and Identification of UAS threats and integrating them to provide more robust capabilities to carry out the C-UAS mission more effectively. Specifically, we currently have, and are continuing to refine, capabilities that provide 3D moving target radar detection to detect potential threats and provide cues to automatically point imaging sensors in the direction of the threat. Additionally, we offer EO/IR imaging systems that can automatically slew and provide positional information on the air vehicle, as well as custom versions of AI in the form of Convolution Neural Networks (CNN) that are being trained to classify potential threats. All of these capabilities are tightly integrated and have connectivity to defeat mechanisms, providing an enhanced, integrated C-UAS solution.

4 After 9/11, the DoD acquired many urgent-need technologies that later ended up being interoperable. How is interoperability (with classification and defeat systems, for example) being addressed for the C-UAS systems that FLIR develops?

The government is looking for industry to provide Modular Opens System Architecture (MOSA) along with Integrated Sensor Architecture (ISA) for solutions that are being developed. These requirements provide the flexibility to support interoperability and functionality for connectivity and security while maintaining lightweight deployment.

FLIR®

Breaking Defense thanks FLIR for supporting this editorial E-Brief. Sponsorship does not influence the editorial content of the E-Brief.