BREAKING DEFENSE | eBRIEF



Expanding the counter-UAS envelope

An editorial eBRIEF sponsored by CACI

SITREP

The counter-UAS (c-UAS) challenge is increasingly one of scale, integration, and speed: detecting more threats across larger areas, giving commanders enough information to act, and trying to defend more locations against varied drone threats while integrating sensors, kinetic and non-kinetic effectors, directed energy, artificial intelligence (AI), and physical protection into architectures that can adapt as drones become more autonomous and adversaries change tactics.

That is driving the Pentagon toward layered defenses and open architectures that can incorporate new technologies as they emerge. It is also forcing a reassessment of long-standing assumptions about air and missile defense. Counter-UAS sensors, for example, may not always need the fire-control-quality fidelity required for traditional air defense, particularly when the immediate need is simply to know that something has crossed an installation boundary. Scaling those defenses presents another challenge. Military installations, airports, critical infrastructure, public gatherings, and other sites have different layouts, missions, personnel, and threat environments, making a single standardized counter-UAS package difficult to apply everywhere. The Army's Joint Interagency Task Force 401 (JIATF-401) is working to address that problem through a counter-UAS marketplace intended to broaden access to US-made systems while giving industry greater visibility into aggregate government demand.

The threat is also changing across regions. Ukraine and Russia continue to rapidly adapt drone tactics and defenses, while Russia's cooperation with Iran has spread lessons from the Ukraine conflict to the Middle East. In the Indo-Pacific, longer-range and lower-cost drones could give China another means of attacking US forces operating across the First and Second Island Chains. Across those theaters, the common requirement is a defense that can evolve as quickly as the threat.

This EBRIEF examines how JIATF-401 is approaching that problem, from sensing and defeat options to AI, acquisition, industrial capacity, and physical infrastructure. It also looks at how changing drone threats in Europe, the Middle East, and the Indo-Pacific are reinforcing the need for flexible, layered counter-UAS defenses rather than a single technological answer.

– Barry Rosenberg & Casey Laughman



Director of Joint Interagency Task Force 401 Brigadier General Matthew Ross tours Yuma Test Center at Yuma Proving Ground in Yuma, Ariz., Sept. 22, 2026, ahead of the Falcon Peak demonstration. (US Army photo by Ana Henderson)

ON THE COVER: Spc. Ian Zinsmeister, a first-person view strike drone operator assigned to D Company, 2nd Battalion, 5th Cavalry Regiment, 1st Cavalry Division, prepares to operate an FPV drone during a counter-unmanned aircraft system qualification event at Fort Hood, Texas, July 26, 2026. The qualification tested Soldiers' ability to detect, track and neutralize drone threats across multiple scenarios, reinforcing skills critical to surviving and fighting on the modern battlefield. (U.S. Army photo by Master Sgt. Luisito Brooks)

From directed energy to AI and hardening, JIATF-401 is widening counter-UAS options

The Pentagon's counter-UAS challenge is increasingly a problem of scale, integration, and speed: how to detect more threats across larger areas, give commanders enough information to act, field multiple defeat options, and adapt fast enough as drones swarm together and act with greater autonomy.

For the US Army's Joint Interagency Task Force 401 (JIATF-401), the Pentagon's lead for its c-UAS marketplace and related agreements with allies and partners, that means pushing industry beyond traditional assumptions about what a counter-UAS system should look like.



The U.S. Army, U.S. Air Force and Federal Aviation Administration conducted a joint test with a DJI Air 2 drone at Joint Base Andrews, Maryland, March 18, 2026. Unmanned aerial systems are an evolving threat, leading to the creation of groups like the Joint Interagency Task Force 401, focused on synchronizing c-UAS efforts across the Department of War and rapidly delivering state of the art c-UAS capabilities. (U.S. Air Force photo by Senior Airman Julia Lebens)

"More than anything, if industry heard nothing else, I would say don't self-limit what you provide in terms of solutions based off your understanding of our concept of employment," said JIATF-401 Director Brig. Gen. Matthew Ross.

Sensor development is one area where industry shouldn't feel constrained by existing air-and-missile-defense (AMD) capabilities, he said. Traditional integrated AMD relies on highly precise sensors capable of producing fire-control-quality tracks. Applying that standard everywhere against small drones would require layers of expensive active and passive sensors spread across enormous areas.

Counter-UAS does not always need that level of fidelity. An installation commander may initially need to know only that something has crossed a boundary where it should not be. That warning could prompt a ground patrol, another drone, or a different response without first requiring a fire-control-quality track.

"From a counter-UAS perspective, I would accept a lower threshold in terms of fidelity," Ross told Breaking Defense at JIATF-401's recent interagency summit. "If we maintain that same standard for fire-control-quality data, (that) means we're going to go with a combination of active and passive sensors, just arrayed all over the place; we'll never be able to scale it. That is an active conversation that I've got ongoing with industry today."

The demand for flexibility applies to defeat, in particular. Rather than depend on a single effector or mechanism – whether that be kinetic or non-kinetic – the counter-UAS architecture has to give defenders options that can be matched to the threat, location, and circumstances of an engagement.

Expanding defeat options

One area of focus for JIATF-401 is developing high-energy lasers and microwaves as low-collateral defeat mechanisms around military bases and populated areas. These technologies have demonstrated that they can defeat drones, but still have to prove how effectively they can operate and be sustained at military installations without disrupting other base activities or airspace in surrounding communities.

"We've proven that the science works," noted Ross in his remarks during the interagency meeting. "You can defeat a drone with both a high-energy laser and high-power microwave, but we need to figure out how to use them successfully in an operational context."

That's the impetus for a year-long pilot at several US military installations, including a couple across the Southern border such as Fort Huachuca, AZ, and Fort Bliss, TX, as well as Naval Base Kitsap, WA; Grand Forks Air Force Base, ND; and Whiteman Air Force Base, MO.

Intended to measure more than whether the systems can hit a target, JIATF-401 wants the pilot to help it understand

power requirements, maintenance demands, mission-capable rates, and whether service members can operate and maintain the systems without relying on expensive field support representatives.

Another part of the cost calculation will allow the services to compare directed energy with both kinetic and non-kinetic approaches to defeating drones. Directed-energy systems are often discussed in terms of a very low cost per shot, but that does not necessarily capture the expense of buying, operating, and sustaining the system.



U.S. Air Force Master Sgt. Kevin Brown, Air Force Global Strike Command Security Forces manager of training and force development, speaks to U.S. Air Force Airmen during an X4 and SMASH 2000L Systems Firing Qualification at Camp Guernsey Joint Training Center's North Training Area, Wyoming, May 15, 2026. The qualification tested defenders' ability to employ emerging C-sUAS capabilities against simulated ground and aerial threats. Joint Interagency Task Force 401 hosted the qualification event to strengthen counter drone capabilities across multiple Department of War Services and components. (U.S. Air Force photo by Staff Sgt. Michael A. Richmond)

"If I procure that system and it costs me $6 million and I take one shot a year, you can't tell me that that shot only costs eight cents," Ross said. "We have to take a more holistic look at it."

That includes "kinetic defeat options at all of our defense critical infrastructure sites," Ross told Breaking Defense, describing kinetic defeat as another tool available to defenders rather than the basis for the entire counter-UAS architecture.

The same goes for counter-UAS systems that can operate farther left of the kill chain by not only detecting incoming AMD threats, but helping to locate their controller and origin.

Scaling c-UAS and the marketplace

The c-UAS challenge becomes more expansive as counter-UAS missions eventually extend beyond a handful of military installations to include critical infrastructure such as airports and public gatherings. JIATF-401 has been working to tailor defenses to individual sites rather than putting the same package everywhere, as different installations have varied layouts, assets, personnel, and security forces.

Building manufacturing scale for such a c-UAS architecture is also shaping acquisition. The JIATF-401-led counter-UAS marketplace is intended to give more government organizations, partners, and allies access to US-made systems while giving industry greater visibility into aggregate demand.

"If I could tell industry, 'globally, we're going to spend $3 billion on small-form-factor radars in 2027,' they would start making a bunch of radars," Ross said. "If instead they wait for DoW to offer a contract and then DHS to offer a contract, we're going to receive those radars in 2029."

The marketplace is also intended to make it easier to move technologies across traditional acquisition boundaries. Army equipment is being deployed at Air Force installations, while commercial technologies outside established programs of record can also reach operational formations.

"Just the fact that we can get our hands on the most current and effective technology solution and then get it in the hands of our formations without a prolonged, cumbersome process that makes that equipment late to need, that's a success," Ross said.

Not unique to the US

Scale is not the only factor complicating the counter-UAS problem. The threat itself varies considerably by region, while adversaries are learning from one another and changing their tactics as defenses improve. C-UAS requirements in the Middle East are different from those in the Indo-Pacific or Europe, while the US also has to account for domestic threats.

Adversaries are helping and learning from each other across regions, said Stacie Pettyjohn, director of the Defense Program at the Center for a New American Security.

"Russian and Iranian cooperation is not necessarily altruistic, but it is pretty deep and it is two-way now," said Pettyjohn. "The Iranians obviously first helped the Russians and provided

them with Shaheds, but now the Russians have improved upon those models significantly."

Russia has learned much from the move-countermove situation in drone warfare during its war on Ukraine. Russia had early success with its Shaheds, so Ukraine adapted mobile gun trucks to shoot them down. When Russia began flying the drones higher to avoid anti-aircraft fire, Ukraine responded with small quadcopters to ram Shaheds.

Now, Russia is turning to jet-powered drones such as the Geran-3 to outrun the quadcopters, with Pettyjohn noting that Russia sharing what it has learned with Iran could help the latter expand its tactics against the US and its allies in the Middle East.

"My fear is that in the future – and not really a very distant future – you're going to see Iran being able to launch raids or big attack packages that are more along the size of what Russia is doing today, where it's 800 drones, 15 to 20 cruise or ballistic missiles," she said. "It's nearly impossible to defeat every single incoming weapon."

In the Indo-Pacific, the concern has traditionally been China's stockpile of ballistic and cruise missiles, and now its efforts to develop and field hypersonics. There is a limit to how many of those weapons China can realistically build and store, and if they begin expending them quickly it will be difficult to produce them fast enough to keep pace with expenditures. Drones give China another option for projecting power.

The complicating factor for China is the area involved in the Pacific, as smaller drones don't have the range to reach across vast expanses of water or move from one island to another. But as drone range continues to rapidly grow with improved technology such as turbofan-powered engines, swarms in the Pacific are an increasing concern.

"If they had cheap drones with 1,000 or 2,000-mile range, that would give them the capacity to continually attack US bases and forces trying to operate in the First Island Chain and make that difficult," said Pettyjohn. "It could essentially undermine US distributed-operating concepts, whether that's the Joint Way Forward concept or the Air Force's ACE (Agile Combat Employment) concept or the Marine's EABO (Expeditionary Advanced Base Operations) concept."

The regional differences and the speed of adaptation put an additional premium on defenses that can change as quickly as the threats they are designed to defeat.

AI and c-UAS

Another major technology challenge is dealing with threats that are themselves becoming more automated. As drones begin sharing information and operating together, artificial intelligence and autonomy will also increasingly become part of the systems designed to counter them.

"Automation and AI is going to aid in kill chains or kill webs," Ross said, in response to a Breaking Defense question. "It's going to allow us to do things quickly, hopefully with more precision, certainly with more information."

He said that JIATF-401 is presently using AI to consolidate counter-UAS testing results into a common data lake. Rather than have different organizations repeatedly test the same system, the goal is to make those results accessible across the interagency and use AI to help filter the information.

Operational uses of AI and autonomy are being approached incrementally rather than by starting with an ambitious end state. The task force is working from technology that exists now and adding capability step by step.

Sometimes the answer is not another system

Even with an emphasis on sensors, effectors, AI, and open architectures, some of the most useful counter-UAS measures may be far less technologically complex. JIATF-401 has made three visits to Ukraine in a recent six-month period to examine how unmanned systems are being employed, including how air bases, airports, national capitals, and other rear areas are protected. One lesson has been the value of physical infrastructure.

"Physical infrastructure improvements are extremely effective against unmanned systems," Ross said. "It's not where everybody starts when they start talking about counter-UAS."

For a command post in the field, that can mean dispersion, moving into a basement, or using existing buildings to help ensure the mission can continue despite a drone threat.

The same analysis applies to fixed infrastructure. JIATF-401 looks at the mission that has to continue, the asset being defended, opportunities for redundancy or hardening, available manpower and authorities, and the most likely and most dangerous threats.

"What that led us to in some cases is that the right answer actually was not additional autonomous warfare capabilities or



Civilian contractors with CACI work from the operations center staged during the SkyValor Operational Demonstration at Cannon Air Defense Complex in Yuma, Arizona, May 13, 2026. This exercise is coordinated by Joint Interagency Task Force 401 showcasing the ability to counter small unmanned aerial systems from CACI. The SkyValor Operational Demonstration is in support of Joint Task Force - Southern Border to enhance air domain awareness along the southern border. (U.S. Marine Corps photo by Lance Cpl. Sarah E. Foster)

technology," Ross said. "In some cases, relying on the improvements to infrastructure was just as effective, if not more so."

Regardless of whether the threat is in Europe, the Middle East, or a potential future conflict in the Indo-Pacific, there is no universal model for defending against UAS because of differences in drone size, range, and capability. That makes flexible, adaptable defenses a requirement rather than a single technological choice.

"You need layered defenses," said Pettyjohn. "You're going to find that ships that can move around or aircraft provide you with those flexible and more responsive types of defensive systems, but often are still fairly expensive or have expensive interceptors for certain locations that you feel like you need to defend. You're going to want point defenses, too, and it's not just going to be having some guns, having counter-drone, drone interceptors. The reason is that if you just have one type of defensive system, they can easily find a way to circumvent it."

The result is a counter-UAS effort built around multiple layers rather than one answer: sensing that can cover more territory, directed-energy along with other kinetic- and non-kinetic defeat options, interoperable systems, automation, physical protection, and an industrial base able to keep changing as the threat changes.

"We want breadth and depth in the industrial base," Ross said. "We want the ability not only to produce known systems today and produce them at scale, but to be able to rapidly iterate with those systems and take advantage of the organic industrial base inside the United States to be able to support our warfighters."

VIEWPOINT FROM CACI

LONG-RANGE DETECTION CAPABILITIES EXTEND DECISION TIME FOR COUNTER-UAS ACTIONS



CACI

CACI Chief Technology Officer Jason Bales

Drone threats give defenders less time to determine intent and select the appropriate response to protect borders, military installations, and critical infrastructure with no/low collateral damage.

CACI International's SkyValor next generation drone defense system is designed to expand that decision space through long-range detection and a layered architecture that combines radio frequency (RF) sensing, radar, electronic warfare, cellular detection, and electro-optical and infrared sensors. Breaking Defense talked about SkyValor with CACI's CTO Jason Bales.

Breaking Defense: Before we get into the details of SkyValor, what threat scenarios is it designed to address, and why are these concerns more urgent now?

Bales: SkyValor builds on more than two decades of designing and deploying counter-UAS systems worldwide. Over 300 fielded systems have informed our understanding of how drone threats evolve across national security missions, homeland defense, and critical infrastructure protection. We've taken that day-to-day operational insight and transformed it into a commercial offering purpose-built for homeland and national security missions. Border defense is a major focus—tracking drones operating near or across national boundaries, as well as protecting critical infrastructure from incursions. Our long-range detection gives operators the decision space to determine intent and escalate force appropriately across a rapidly shifting threat landscape.

Range is one of SkyValor's attributes. Tell us about this.

SkyValor doesn't just extend the detection envelope, it transforms the entire decision space. While most Group 1–3 systems spot a drone only one to five kilometers out, giving operators a frantic 10-second window to react, SkyValor reaches an impressive 75 kilometers. That jump in range turns split-second choices into a deliberate, 18- to 20-minute tactical advantage, giving operators the breathing room to read intent, weigh options, and apply precisely the right level of force.

Describe SkyValor and its components, and where it fits within a broader counter-UAS architecture.

It's a multi-layered architecture built for a fast-moving threat. Our RF heritage enables long-range detection, signal analysis, and the ability to break into a drone's communications and create cyber effects—and to apply those effects to steer or take over the platform. The system can also jam broadly when confronting swarms. Our RF and EW capabilities are built in-house, and we integrate commercial radar for added range and precision. A key differentiator is our cellular-network technology, which detects and mitigates drones using cellular links, alongside EO/IR sensors and integration with kinetic interceptors.

Tell us about your non-kinetic defeat options.

Non-kinetic effects allow us to neutralize a drone with almost surgical precision. Instead of relying on expensive interceptors that may require multiple shots, we use software-driven energy effects that deliver low or no collateral damage and provide an essentially unlimited magazine. It's the difference between having to physically remove a threat and being able to outthink it by using the system's intelligence to quietly and efficiently disable or redirect a platform long before it becomes a problem. Kinetic tools certainly have their place, but SkyValor's long-range detection lets

operators be deliberate rather than reactive. When you have minutes instead of seconds, you can choose the right level of force instead of defaulting to the most aggressive one. That measured escalation preserves valuable interceptors for situations where they're truly needed.

How does being software-defined change the equation?

Being software-defined changes the entire equation. It means our non-kinetic effects aren't fixed - they evolve. At a recent event, a drone operator tried to slip past us by altering their waveform. In half an hour, we pushed a new update across the system and reasserted control. That agility is a hallmark of SkyValor: rather than chasing the threat, we stay ahead of it. The platform adapts in real time, letting operators counter new behaviors as soon as they appear.

What did the recent testing of SkyValor at Yuma and the southern border demonstrate?

Our recent work with JIATF-401 at Yuma and along the southern border was a real proving ground. It combined controlled test runs with unpredictable, real-world encounters—short-range pop-ups, long-range crossings, low-altitude skimmers, and drones using a mix of communication links. Every time the environment changed, SkyValor kept pace. Those trials didn't just validate performance metrics; they demonstrated the system's ability to adapt to a living, evolving threat landscape.

What does CACI uniquely contribute in detection, tracking, processing, and non-kinetic defeat?

We designed SkyValor to operate autonomously from day one. That means it can collect, detect, track, and relay information without waiting for human intervention—all while feeding curated, AI-filtered insights back to operators. The autonomy isn't about removing humans from the equation; it's about giving them cleaner, more actionable intelligence. When the system is doing the heavy lifting behind the scenes, operators can focus on making confident, well-timed decisions in a compressed battlespace.

What real-world scenarios best illustrate where SkyValor adds the most value?

Border protection is a prime example. You want to know when a drone is approaching long before it crosses the line, and SkyValor gives you that early warning, turning a few frantic seconds into a structured decision window. In high-density conflict zones, where threats evolve nightly and new drone behaviors emerge constantly, the system's software-defined nature gives operators an advantage: real-time updates, remote adjustability, and layered sensing that keeps pace with the fight. And when it comes to critical infrastructure like power plants, data centers, and other assets central to national resilience, SkyValor provides the persistent coverage needed to keep mission-critical sites secure.

What should readers take away about SkyValor?

SkyValor is the culmination of two decades spent tackling the drone problem in the real world. It's field-proven, adaptable, and built for missions where speed, scale, and flexibility matter most. Because of our extensive C-UAS knowledge, we successfully moved from concept to deployment in 12 months. Now, as we have moved into full-rate production, customers are getting more than just a product, they're getting a foundation for modern layered defense - one that can grow, shift, and respond as fast as the threat itself.

CACI

Breaking Defense thanks CACI for supporting this editorial eBRIEF. Sponsorship does not influence the editorial content of the eBRIEF.