A View from CT Foxhole: Brigadier General Matthew Ross, Director, JIATF-401

By Sean Morrow and Don Rassler

Brigadier General Matthew Ross is the Director of Joint Interagency Task Force 401. As Director, he supervises the Department of War's consolidated effort to rapidly develop and provide counter drone capabilities at scale to enable the department to protect U.S. and allied forces, defend critical infrastructure, and assist federal agencies in securing population centers from unmanned aerial system threats.

Throughout his career, Brigadier General Ross has deployed multiple times for combat and contingency operations. He has a bachelor's degree from West Point, a master's degree from Central Michigan University, and served as a fellow at Duke University's Sanford School of Public Policy.

CTC: You serve as the Director of the Joint Interagency Task Force 401, and you've previously spoken about how you've dealt with drone threats and counter unmanned systems in the field and on operations, and how you've also utilized drones for offensive operational purposes. How has your experience shaped your approach to the director role and the work that you're doing at JIATF-401?

Ross: Because of my previous roles, I think about every military situation as the aggressor, or from a proactive approach, and I try to share that with the JIATF team. I really see our counter-UAS [unmanned aerial systems] equipment as the last resort or last line of defense. It's easy to think, from a counter-UAS perspective, that the equipment will save us. But I'm convinced that there's no silver bullet and the equipment won't save you. It is going to be the responsibility of the individuals who are trying to accomplish a mission to ensure that the threat of small drones or unmanned systems does not prevent them from being able to accomplish their mission. And so that's the very proactive approach.

A lot of the things we've done here recently at JIATF focus on removing the archer instead of the arrow. So, you focus on attacking the drone pilot first. Even just in the last 24 hours, we had one case of a successful interdiction on a military installation, and that's how it ended up playing out. We identified the ground control station, and we were able to get a team out there to apprehend the individual.

CTC: Do you remember a moment in your career when you realized just how transformative small drones would be and that it wasn't just a tool you were fighting, but a revolution in tactics?

Ross: I think I will give an answer that's unlike others. I think a lot of people would reference Operation Spiderweb or other conflicts in the Middle East. They might reference day-to-day fighting in Ukraine and the proliferation of mass in terms of drones. For me, what was most concerning is the way adversaries fought with the use of proxies. We use proxies because we want to manage attribution and escalation, and so what you have to do to use proxies effectively is you have to be able to share or proliferate advanced conventional weapons to give them some type of state-like military capability. That's what drones do. Drones provide capability to small groups and individuals that were previously reserved for state adversaries. So, whether it's exquisite ISR [intelligence, surveillance, and reconnaissance], the ability to collect on signals of interest, the ability to weaponize an unmanned system that you could use from great distance, that is what has been most concerning for me.

I actually think that the larger transformation will be the inclusion of much larger systems. The advancements in autonomy are going to allow us to scale that even more. For example, when I was in a previous role, we were looking at autonomous breaching. This wasn't just limited to the use of small drones; it was an entire ecosystem of autonomous technologies that would allow you to accomplish a military task without putting service members at risk. I knew immediately that this was going to change the way we fight into the future.

CTC: JIATF-401 was established by the Department of War in August of 2025. Why was JIATF-401 created? What problems is it trying to solve? What unique features or authorities does it have, and what are its primary lines of effort?

Ross: First, I would say counter-UAS is a domain that's advancing so quickly that we wanted to ensure that we weren't just trying to keep pace with the threat within pockets of excellence. Instead, we wanted to *synchronize* efforts across the Department. We wanted to make sure that we shared everything that we have been learning with our interagency partners because counter-UAS is both a warfighting and a homeland defense imperative. We, as the Department, put a bunch of resources into RDT&E [Research, Development, Test, and Evaluation] and development of new technology. And so how do we take those investments and transfer them to federal authorities, to state, local, tribal, and territorial partners as they get responsibility to protect against the threat of drones? How do we make sure that they're well equipped to accomplish that task? That's what the team at JIATF-401 has been taking on.

I do think that drones are changing the character of modern combat, but they're not changing the nature of combat. Victory still belongs to those who adapt fastest, those who strike the hardest and endure the longest, and so countering drones is key to force protection, mission success, and survival on the modern battlefield. So, I believe that incorporating unmanned systems into the fight is critical, and I would say that's true both from an offensive standpoint and from a defensive standpoint. We tend to bifurcate the two. But we have to continue to do that both with aerial systems, including

"I do think that drones are changing the character of modern combat, but they're not changing the nature of combat. Victory still belongs to those who adapt fastest, those who strike the hardest and endure the longest, and so countering drones is key to force protection, mission success, and survival on the modern battlefield."

unmanned aerial drones and counter-UAS, and unmanned systems more broadly, especially as we start incorporating larger ground vehicles, surface vessels, or underwater vehicles.

Over the past five years, two of the things that has changed the most when it comes to drones is their increased resiliency—their ability to operate in contested environments—and mass. What we've seen is that when the cost goes down, you're able to expand production and you're able to introduce mass to a battlefield. When I look at what we've seen in the most contested environments, like the current fight between Ukraine and Russia, what catches my attention most is the innovation cycle and the iteration. When we talk about innovation, people tend to think about the platforms themselves. I actually think it's the TTPs [tactics, techniques, and procedures]. It's how we use the tools that were provided, and so when people would say there's an iteration cycle of 72 hours or seven days in Ukraine, they're not saying that they're rolling out new technology every seven days. But the way they use that technology, the frequencies that they're using, the TTPs, that is what is evolving quickly. And that's what we need to replicate.

We have three lines of effort inside JIATF. The first is defense of the homeland. The second is support to warfighter lethality, and the third is joint force training. I think all three are critical, so defending the homeland is where we spend a lot of our effort in support of the Secretary [of War] through things like Domestic Shield and the provision of counter-UAS technology to help defend critical infrastructure. But support to warfighter lethality is also critically important. Operation Epic Fury has given us the opportunity to sprint towards that objective by introducing new technology, TTPs, and solutions into a contested environment. That enables us to see what works and what doesn't.

CTC: JIATF-401 has been a test case for new acquisition processes and authorities. Can you help our readers understand what's changed? How it's enabled your organization and if it's scalable outside of JIATF to the Army and DoW?

Ross: I think we were the first program acquisition executive as part of the changes to the acquisition process across the Department. One thing that is unique to us is our structure. I work directly for DEPSECWAR and serve as the senior advisor on counter-UAS to the Chairman [of the Joint Chiefs of Staff], which allows us to connect directly from the corporal on the frontline to the senior levels of the Department to understand the greatest challenges.

When people think about acquisition authority, they typically think about traditional acquisition process: how we go through the testing and evaluation of new technology to make sure that it's safe to use, it meets the requirement, and that we can get it out to the formations with full DOTMLPF [Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities] considerations. That's only a piece of it, as once we deliver those solutions, we've got to make sure the guidance, the ROE [rules of engagement], the permissions and authorities for those service members allow them to use the equipment effectively.

We say we have one measure of effectiveness inside JIATF and that's delivering state-of-the-art counter-UAS capability to our warfighters both at home and abroad. But I think that's so much more than delivering a new piece of equipment. As an example, if I go to talk to a patrol leader on the southern border as part of JTF [Joint Task Force] Southern Border today and I ask them what their greatest challenges with UAS are, they won't tell me that they need a new interceptor. They'll tell me that they need to be able to see everything they can see in the JOC [Joint Operations Center] on a mobile device when they're out on patrol. That is their greatest limiting factor, and so we should address that problem first before we start progressing into the next piece of advanced technology.

What I love about JIATF's mission is that we are responsible for all of that. The guidance, the policy, law, where it applies, the authority to operate, the authority to connect to a specific system, spectrum approvals, target engagement authority, and the training through the Joint Counter-UAS University (JCU). By looking at that whole ecosystem, we have the ability to affect meaningful change.

One of the things I'm most proud of that we did within our first 90 to 120 days is clarifying the guidance from SECWAR to our installation commanders on how they should be approaching the problem and their authorities to counter UAS because it wasn't clear at the time. While that seems like a really small thing, it makes a huge difference for that person who's sitting in the operations center, who has to identify an incursion and make a determination about what they should or should not do. Having clear guidance from the top is helpful in that process.

CTC: You've talked about JIATF's one clear measure of effectiveness (MOE)—to rapidly put state-of-the-art c-UAS capabilities into the hands of warfighters at home and abroad. What type of progress do you feel JIATF has made toward that goal thus far?

Ross: The first thing we did was to clarify the authorities and approvals for counter-UAS, and then we started addressing the network. We identified the fact that we need a common tactical user interface for counter-UAS. We should be able to share information between agencies that are working side by side, especially if it's inside the continental United States. We should also be able to share data with partners and allies if we're working OCONUS in places like the Middle East. And so first, we addressed the policies and authorities. Second, we addressed the network, and now we're at the point where we're starting to integrate additional sensors and effectors across the force.

For context, when I say sensors, I'm talking about a number of different sensors, including active and passive sensors. Passive sensors would be things like acoustic sensors and passive radars.

We're actually running a pilot program with passive coherent radar right now that uses available signals in the environment to identify a disruption, so you know that there's a device there. It gives you a less precise location, but it gives operators enough to know that there is an incursion that needs attention. Another layer of sensing would be day and night cameras, EO/IR [electro-optical/infrared] cameras. By layering all these sensors together, we can build depth in our ability to understand when a threat's coming at us. In the past, we would approach counter-UAS like integrated air and missile defense, and there's a concept in integrated air and missile defense called Castle Defense that is guided by the view that we're going to sit here within our walls and we're going to defend from inside of our perimeter. I don't think that's how we should approach counter-UAS. We need to get outside of that perimeter to be able to sense in depth so that we can increase our decision space.

When I talk about effectors, there's both kinetic and non-kinetic effectors. Non-kinetic effectors would include jammers, something that would deny a specific link that's targeted. It may be a barrage jammer that jams the entire spectrum so it's hard for adversaries to operate. It may be a cyber takeover system, and so with some systems, you can actually take over the flight and be able to land a drone into a safe area. And then there's kinetic effectors, which include interceptor drones, which is a place that we're investing in right now—think drone-on-drone warfare with small interceptor drones. We've had these for Group 3 [UAS] and above, and we've thought of it as ground-based air defense. We're building the exact same capabilities for Group 1 and Group 2 [UAS]. Then, there are also effectors that utilize directed energy. We're running a directed energy pilot for the Department, specifically looking at lasers and high-powered microwave and trying to determine where they are most applicable in our layered defense for counter-UAS.

For a long time, especially in the homeland, we have limited ourselves to non-kinetic options, meaning I would have a system that would detect a radio frequency for a ground control link and then I would try to attack that link to defeat the drone, which works really well for commercial systems. It's less effective for a system that has been modified. So, what we do now is attack the physics of flight. Every single drone has some type of physical mass, which means it's observable through passive and active sensing. It has some type of rotors that allow it to stay aloft and stable. It's got some type of camera or sensor that will allow it to see where it's going so it can get to its final objective. If we attack those first principles in terms of how we try to counter UAS, then our solutions will be more resilient as the modality of control changes for these drones.

For example, here's one other thing we've done over the past 12 months, which I think is a step in the right direction. We're working in support of NORTHCOM and JTF Southern Border and with the other federal agencies along the southern border, all 1,954 miles. We've surveyed the entire border to first ensure that we have shared air domain awareness. We've looked at where we need to place sensors along the entire border so that we have full domain awareness across the southern border and when that is integrated into a common C2 [command and control], we can start layering in effectors that allow us to protect the homeland. That is an effort that we've been moving against pretty quickly. We made a ton of progress over the past several months, and in just the last four months, we've allocated more than $20 million in counter-UAS technology to support this goal.

CTC: A cornerstone of JIATF-401's effort has been the creation of a counter-UAS marketplace, "a centralized mechanism that allows interagency and law enforcement partners to access DoW test data, operational user feedback, and validated procurement options."[1] The marketplace went live in February and reportedly features at least a dozen counter-UAS systems and a "continuously expanding inventory … [of] a wide array of sensors, effectors, and system components."[2] Tell us a bit about the marketplace, the process of building it, some of the capabilities or systems you're excited about, and how you plan to evolve it.

Ross: I would say that there are two problems we need to solve with the marketplace. The first problem is where we typically start inside of the War Department and that is making drones and counter-UAS capability available to our formations. That's a very real challenge. In the past, when we thought about unmanned systems, we centrally managed those systems because they were expensive, complex, and we had limited quantities, like MQ-9 reaper drones. Over time, we saw that those systems got smaller and less expensive and that we required them at echelon.

So, we changed our approach and said, 'Hey, we actually need these at every level of our formations.' And so, we need to make sure that they're accessible to the companies, the battalions, and the brigades. And that's what SECWAR laid out with his drone dominance memo last year.[3]

I would argue that counter-UAS is the same thing, and so in the past, these systems have been large and complex, limited in quantity, and centrally managed. What that means is that in an Army formation, if you go to a division, the only thing they have for counter-UAS may be a counter-UAS battery. That is completely insufficient. We need a variety of counter-UAS tools at echelon based off their most likely threats.

So, problem one is ensuring that we have accessibility across the Department to those capabilities for counter-UAS. Problem two, and this is the part that I'm more interested in from a JIATF-401 perspective, is making sure the counter-UAS technology is available to all members of the JIATF *and* our partners and allies. What that means is that the other interagency parts that use different systems for their procurement need to be able to have access to our market, understand the testing and validation that we've done on these systems, and then have access to the industry partners that provide those capabilities.

Counter-UAS is a problem not just inside of the Department. It's a problem for the FBI and DHS like we've talked about on the southern border. The Department of Corrections, anybody who runs a prison today has problems with drones delivering contraband inside of their walls. So, they also have a requirement for counter-UAS. But they don't know where to go to fill that requirement. Similarly, industry can't see the aggregated demand for counter-UAS systems. So, what we have done with the counter-UAS marketplace is we've made it fully open—a two-way marketplace. If somebody wants to deliver a counter-UAS solution into our ecosystem, they can go to the counter-UAS marketplace and upload their product and say, 'Here's what it does.' Then we as JIATF-401 will test the product, and if it does exactly what they've described, we'll put a JIATF-401 badge on it, so people know that it's been validated. If it does not perform as advertised, they need to make improvements before we will endorse the product.

Brigadier General Matthew Ross

I think this is really important for counter-UAS, especially as you talk about investment over time because 80 percent of what we buy or field, especially in the small drone space, is commercial equipment. So, by pulling this marketplace together, we have the ability to aggregate demand so that U.S. industry can build breadth and depth in our industrial base, so that we have the capacity for that next conflict where we know our requirements are going to be higher than they are today.

CTC: What is the role of private capital in the c-UAS fight? How can we incentivize companies to invest in your needs, particularly from non-primes, who maybe haven't historically had access to DoW development?

Ross: I've actually spent quite a bit of time with private capital investors trying to help them see what I believe the market is. I think the biggest thing we can do to help them is aggregate that demand, and so part of the counter-UAS marketplace [is] it will provide analytics and be able to tell us things like the purchases for a 12-month period. We'll be able to tell you that two and a half billion dollars went to small-form radars with a range of 20 kilometers and below. When industry sees that, they'll be able to make a better assessment of where they should put their capital. We'll be able to tell you how much money went into specific interceptors, acoustic sensors, or software that enables an operator. Today, we struggle to see that because we have treated counter-UAS as a military-specific problem; that is just not the case anymore.

If you look at what's happening in Colombia with the FARC, the Colombians have a very high demand for counter-UAS technology, and they're trying to figure out where to put those resources. If you go to the Middle East today, all of our partners and allies are trying to buy counter-UAS technology, and they want to buy from the U.S. industrial base. So, we've got to make it accessible to them.

CTC: A lot of what we have learned about c-UAS is rolling off the battlefield of the Ukraine war. Given the speed of innovation that we have seen, how do you make sure that we're learning the right lessons at the right speed while also considering future threats so that our responses do not quickly become obsolete?

Ross: I've been studying the Ukraine conflict closely, partially because I am a member of the profession of arms, and I think anytime somebody's in conflict, you must watch really closely, especially as we see these changing characteristics of warfare. When I look at what works really well in Ukraine, I think of it similar to our first-principles approach. How could that apply to our warfighting concept? It doesn't mean we can pick up what they're doing in Ukraine and directly transplant it to another environment because our ecosystem is going to be different. The Ukrainians fight very well with limited resources. We fight very well and have access to more resources, and what that means is as we take their lessons learned, we need to apply it to the U.S. Department of War's Joint Warfighting concept to get the full benefit from those lessons.

What's most impressive to me as I watch the Ukrainians is their ability to innovate and evolve rapidly. That's what I want to build for us. I don't think it's about any specific platform. It's about building an ecosystem that allows us to identify an emerging or adapting threat and then evolve with it fast enough to keep our warfighters safe.

CTC: Can you share a bit about some of the testing and experimentation that you've done regarding platforms and systems? For example, we've been able to read about your testing of the Bumblebee V1 C-UAS drone round ammunition, which "breaks apart mid-flight and effectively becomes buckshot"[4] and multipurpose, high-energy lasers.

Ross: When it comes to testing and experimentation, the first thing we have to do is make sure that when we test or evaluate something, we share it across the Department and our interagency. So, probably the most impactful thing we have done in this area is that we established a common characterization for counter-UAS evaluation. We developed test standards and put them out across the entire department and across all the labs. We've got 77 labs across the U.S. Department of War that are actively working on this problem. We publish our list of problems so that people are working on the challenges that we see in the counter-UAS fight. Then, when somebody develops a countermeasure and they evaluate it, they evaluate it to the standard. That allows us to make a relative comparison between two different systems that were tested on different days in different locations. As an example, EUCOM and USAREUR-AF just ran Flytrap 5.0, which is a counter-UAS exercise executed at scale and echelon. They did it with 7th ATC [Army Training Command] in Lithuania. Simultaneously, we had testing going on in Nevada for counter-UAS. We should be able to compare how something performed in Nevada to how something performed in Lithuania, and we can't do that without establishing a common standard, and that's what we've done.

Second is we've started looking at the inclusion of kinetics because I believe that kinetics will be imperative as we attack the first principles of flight for a drone that could present a threat. If we want to be able to take that drone out of the sky, then we have to be able to test those kinetics. That's what we've done with the Bumblebee V1 and V2, which are small drone interceptors enabled with automatic target recognition and pilot enhancing

software that allows it to go on a terminal attack. The automation is software enabled instead of hardware enabled, which means it can be updated immediately. If you buy one of those today, and we continue to iterate on the algorithm, then 12 months from now, the system is more capable because all you have to do is load the update.

The other thing that we've done with testing and evaluation is ensure that we can use all available tools in the national airspace, and we're doing that with the FAA [Federal Aviation Administration], who's been a great partner for us. As we talk about directed energy or the testing that we've done with high-energy lasers, which are now being approved for use inside the national airspace, we're ensuring—if you go back to those authorities and approvals, which are our greatest challenge, it's not necessarily the technology itself—that we have an ability to use it effectively. We're making sure that as part of our testing: one, it's common across the department and then two, everything that we introduce into the counter-UAS ecosystem is actually usable by our service members that are out on the field.

CTC: What can you tell us about the Domestic Shield initiative, formerly known as Replicator 2, and Operation Clear Horizon and how JIATF's work intersects with and supports the drone focused executive orders that the Trump administration has issued?

Ross: I'll start with Operation Clear Horizon. Within 30 days of being established as JIATF-401 by SECWAR, we ran an exercise to look at all the services, and their programs of record for counter-UAS. We brought all of the services' equipment out to a location, and we flew really complex threat profiles. We threw Group 3 drones at them. Group 2 Drones. Group 1 drones controlled over radio frequency, LTE, GPS, and fiber-optically controlled drones. We flew the most advanced technology and profiles that we had seen on the battlefield in Ukraine against our countermeasures. In fact, the red team that we used for that came from 10th Special Forces Group who had just recently been in Ukraine and in eastern Poland, working against this problem. We did that so we could identify those areas where we have gaps or seams in our protective capability and then that allowed us to prioritize our efforts.

That helped to set the stage to get where we are today, and to build a more robust layered defense for counter-UAS. When I talk about the need for a common C2 and the requirement for physical effectors for Group 1 and Group 2 drones, that all came from Operation Clear Horizon and those lessons learned.

Domestic Shield started off as Replicator 2. Replicator 1 was the provision of one-way-attack drones and loiter munitions. We wanted to provide them across all the Department. Replicator 2 was a recognition that we needed to do the same thing on counter-UAS, and we needed to protect our critical infrastructure in the homeland and our power projection platforms. That effort started with reconciliation funding and was previously run by DIU [Defense Innovation Unit]. Right after JIATF-401 was established, it was transitioned to our team and became the Domestic Shield initiative. What we did with that problem is we looked at defense critical infrastructure across the Department and we tiered it by priority based off what types of activities and operations they conduct to make sure that we understood what locations required the most protection. Then, we worked with the services. They conducted a survey of every one of our installations. Some would argue that when you identify a really good counter-UAS set of equipment, why don't you just give one to every installation? Well, that doesn't work well because all our installations are different; they're different sizes, different shapes, they've got different types of security forces. In some cases, we manage them with air force security forces. Sometimes on army bases, you just have MPs [Military Police] that are patrolling. In some cases in shipyards, you actually have contractors who are providing security. So, we needed some level of tailorability for counter-UAS at each of those installations. We worked closely with the services to conduct the surveys.

Those surveys told us the following: 'Based off what I'm protecting and the resources that I have available, here's what I require in terms of counter-UAS solutions.' We validated those against the systems that we've tested and evaluated across the Department, and if everything lines up, we're procuring those systems and we're delivering them at scale. It's important to note that none of our installations were completely uncovered. We're just making sure that as we continue to adapt to the evolving threat, we systematically and continuously update our counter-UAS posture with the most recent technology so we can keep pace.

CTC: JIATF-401 has accomplished a lot in 12 months. Where would you like to see the organization in a year?

Ross: My track record to predict the future is really poor, but I can tell you how we're approaching it today. When JIATF was stood up, we knew that it was going to be temporary. As a result, we need to be able to transition the functions we are providing back into the services and the COCOMs, and so for this short period of time, we are going to continue to sprint against the problem. I don't think that our defenses are static. We were just talking about Domestic Shield. I think we have to constantly evolve and mature to ensure resilience, redundancy, and creativity in our counter-UAS posture. That means everything from active patrolling to physical barriers to the counter-UAS measure that would serve as the last line of defense.

We talk about our power projection platforms—our CONUS bases/installations—the homeland is no longer sanctuary, so we have to be prepared to defend our power projection platforms inside the U.S. from nefarious drones. We need to get our formations from fort to port and into a combat theater if and when required. We're also going to continue to pursue emerging technology in conjunction with the services, which is specifically important for directed energy and layered kinetics as we integrate that into our countermeasures more robustly across the United States. That's how we project power. That's how we build a layered defense that gives our warfighters the tools they need to counter this threat. CTC

Citations

1 Adam Scher, "Joint Interagency Task Force Integrates Skills, Creates Layered Counter-Drone Defense," U.S. Department of War, December 18, 2025.

2 Adam Scher, "Counter-UAS Marketplace Streamlines Acquisition, First Purchases Total $13 Million," U.S. Department of War, April 15, 2026.

3 Editor's Note: "Memorandum for Senior Pentagon Leadership Commanders of the Combatant Commands," U.S. Secretary of Defense, July 10, 2025.

4 Nicholas Slayton, "Soldiers with the XVIII Airborne Corps are training with anti-drone rounds," Task and Purpose, April 14, 2026.