Hed -

The Brave New World of Drone Swarms

Subhed -

AI-driven drones that "talk to each other" will change warfare and threaten the homeland

SEO - AI-driven drone swarms are no longer science fiction. Militaries in Ukraine, China, and the U.S. are racing to develop autonomous drones that coordinate attacks without human input—redefining warfare, challenging defenses, and raising urgent homeland security concerns.

Social - AI-powered drone swarms that "think" and act together could transform warfare—and threaten the homeland. As China, Ukraine, and the U.S. race to deploy them, experts warn: the future battlespace may belong to machines that no longer need us.

https://www.gettyimages.com/detail/news-photo/drones-fly-above-the-ground-on-november-8-2025-in-news-photo/2245886317

DEEP DIVE – A drone weapon heads behind enemy lines, on a mission to kill troops and destroy equipment. To its left and right are a dozen other armed drones, and as the mission unfolds they compare notes – on enemy positions, the success or failure of their strikes, and their next tactical moves. There are no humans involved – other than the people who programmed the drones and launched them on their way.

It may sound like a wild premise, but swarms of drone weapons that use artificial intelligence to "think" for themselves are no longer a subject for

science fiction; they are in the advanced stages of testing and in one instance at least – according to a recent report – they are already operational.

The Wall Street Journal reports that Ukraine has begun deploying AI–powered drone swarms in combat – using software developed by the Ukrainian company Swarmer. Battlefield units have used the system more than 100 times, according to the report, in deployments of between three to eight drones at a time against Russian positions.

"The technology is upon us," Rear Admiral (Ret.) Mike Studeman, who served as Commander of the Office of Naval Intelligence, told *The Cipher Brief*. "There are many miles to go in terms of the most sophisticated swarm abilities, but there are plenty of reasons to fear even where we are today."

Not long ago, the mere existence of drone weapons was a battlefield game-changer; this latest paradigm shift involves entire units of drones that carry out operations with humans almost entirely out of the loop.

"If there were a battle to go down today, some of the first engagements might be with unmanned systems," Studeman said. "The most central engagements would involve a lot of them. The race is on."

It's a "race" both in terms of offensive "swarm" capabilities and the technologies to counter them.

"It's an absolute game-changer for any campaign," Joey Gagnard, a former senior Army Chief Warrant Officer, told *The Cipher Brief*. "It's a force multiplier for special operations forces or for any military element. Now it becomes incumbent on the defender to figure out a way to down all of those drones, while not also hurting his own capabilities."

Save your virtual seat now for The Cyber Initiatives Group Winter Summit on December 10 from 12p – 3p ET for more conversations on cyber, AI and the future of national security.

What's in a "swarm"?

Experts define drone swarms as coordinated systems of at least three drones that act autonomously and with "swarm intelligence," mirroring the behavior of birds or insects when they travel in groups. An effective drone swarm will use artificial intelligence (AI) and machine learning to navigate obstacles and communicate changes in the environment to other drones in the group.

Experts draw a distinction between swarms in number only, and those with the ability to operate in dynamic conditions. A 2022 test in China, in which dozens of drones navigated their way through a bamboo forest, demonstrated the difference. The drones were able to move in and around the forest (you can watch the video here), but there was nothing more than the bamboo stalks to stop them – no defense systems, no one shooting at them.

"So we have the components in place such as microchips and microprocessors, we have battlefield experimentation and battlefield data that can enable these groups and swarms to operate," Samuel Bendett, an adviser to the CNA's Strategy, Policy, Plans and Programs Center, told *The Cipher Brief*. "But none of it has really come together yet to form a full picture from that mosaic that would spell a swarm."

The biggest challenge lies in the dynamism of a battlefield. A static environment – say a military base or airfield, or a bamboo forest – will be easier for a drone swarm to navigate than a moving force. "If something changes, is the swarm intelligent enough to adapt and then attack?" Bendett asked. "How is it going to adapt and attack if there are changes?"

Even Ukraine's complex June drone strike, dubbed "Spider Web", which deployed more than 100 first-person-view (FPV) drones against Russian air bases, still relied heavily on human direction.

For a swarm to operate successfully, Bendett said, "there needs to be secure communication between members; they need to pass data to each other about their state of being, about their flight to target, about the conditions that affect their flight to target, about any movements or changes on the

ground or with a target, obviously communication with ground control stations and those that launched them and so on."

Studeman noted that in a fluid combat situation, "you have all sorts of other challenges that exist, including somebody who wants to jam you, using a high-power laser or microwave weapons, and you're encountering all sorts of things that maybe were not planned for at launch, may not actually be in the software parameters of the drones." For complex operational scenarios, he said that true swarms are "probably a bridge too far today," but he and other experts stressed that the battlefield application is coming soon.

Dr. Stacie Pettyjohn, Director of the Defense Program at the Center for a New American Security, envisions scenarios in which drones in a swarm display "command and control" capabilities, "not only acting on their own, but coordinating their behavior, without any human involved, with a bunch of other drones."

In such an operation, "the swarm as a whole makes decisions about how to modify its operations in the best way to achieve its objective," Pettyjohn told *The Cipher Brief*. "Another drone might take its place, or the collective might decide that they realized there were air defenses in place and they needed to flush those out and actually send a wave of them to attack the air defenses, force them to engage a few of the targets, which would then create a gap that the others could exploit to hit their actual objective."

Gagnard said that drone swarms will soon be doing the work of dozens – perhaps hundreds – of drone operators.

"Instead of one guy piloting one drone for a limited duration and being able to go through the entire targeting cycle, you would have a whole swarm of drones doing all of those mission functions simultaneously," he said. "You'll have drones conducting reconnaissance, tagging off to other drones that are going to conduct strikes or one-way attacks, tagging off to other drones that are going to do logistics. So they would make decisions on their own, and operate freely on their own, based on the stimulus and the feedback that they're getting in the environment."

Sign up for the Cyber Initiatives Group Sunday newsletter, delivering expert-level insights on the cyber and tech stories of the day – directly to your inbox. Sign up for the CIG newsletter today.

Coming soon

Whether true AI-driven drone swarms hit the battlefield next month, next year, or three years from now, this much is clear: the technology is already part of the planning for nearly every advanced military, and as a result, it's a booming business. Everyone, it seems, is training and experimenting with swarm technology – beginning on the battlefield where drone innovation is most apparent.

"Both Russians and Ukrainians are really busy trying to develop swarm technologies," Bendett said, and both sides are benefiting from outside help – the Russian military from China, the Ukrainians from the U.S. and Europe – to obtain the microprocessors and microelectronics that enable their operations.

Other militaries and defense tech companies have watched the Ukraine theater and entered the drone-swarm "race."

In the U.S., the Pentagon's Replicator initiative to fast-track innovation includes multiple drone swarm projects. The Defense Innovation Unit (DIU) has awarded contracts to Anduril Industries, L3Harris Technologies, and Swarm Aero to produce prototype software for drone swarms. The contracts are part of the DoD's "Autonomous Collaborative Teaming" (ACT) program, which seeks "automated coordination of swarms of hundreds or thousands of uncrewed assets," according to the DIU. Meanwhile, the Defense Advanced Research Projects Agency (DARPA) has been testing swarms for years, and says that by 2027, the U.S. could deploy swarms of as many as 1,000 armed drones. The DoD has also mandated the creation of dedicated drone testing ranges to support live swarm exercises.

The U.S. hardly has a monopoly in the field, even in the West. One of NATO's newest members, Sweden, is fast-tracking drone-swarm development, in what Defense Minister Pål Jonson said was a response to Russia's aggression in Ukraine. In January, the Swedish Armed Forces unveiled a drone swarm program, developed by defense giant Saab, that

would allow soldiers to control 100 drone weapons simultaneously. Elsewhere in Europe, the German drone manufacturer Quantum Systems has conducted tests on AI-controlled drones with the German military; Britain's Defence Science and Technology Laboratory (Dstl) has awarded contracts for "Mixed Multi-Domain Swarms"; the Dutch Research Council has funded an exploration of drone swarm technology; and Hungarian researchers reported the design of a 100-drone swarm operating without a central controller—based on algorithms inspired by flocking behavior in animals.

Need a daily dose of reality on national and global security issues? Subscribe to The Cipher Brief's Nightcap newsletter, delivering expert insights on today's events – right to your inbox. Sign up for free today.

Countering the swarms

Every military innovation – from gunpowder to the tank to the stealth bomber – prompts efforts to counter it, and AI-driven drone swarms are no exception.

"We're going to have to be as good on the defense as we are on the offense for how we use drones," Studeman said. Asked about U.S. counter-drone efforts, he cited partnerships between the Pentagon and the private sector and said, "I think we're moving as fast as we can."

If the world needed a reminder of the need for counter-drone capabilities, it got a stark one in July from Robert Brovdi, Ukraine's newly appointed drone boss, who told NATO commanders that his crews could turn a NATO base into "another Pearl Harbor" in 15 minutes, without coming closer than 10km (6 miles). "I'm not saying this to scare anyone," Brovdi said, "only to point out that these technologies are now so accessible and cheap."

He went on to warn NATO: you are unprepared.

"I don't know of a single NATO country capable of defending its cities if faced with 200-300 Shaheds (drones) every day, seven days a week," Brovdi told the LANDEURO conference. "Your national security urgently requires a strategic reassessment."

Bendett agreed, citing Brovdi's warning as well as the damage Hamas inflicted with drones against Israeli forces in the early days of the 2023 Israel incursion into Gaza. "So the question," Bendett said, "is what would it take for us to realize that we are facing the same threat and what would it take for our military to make these appropriate changes?"

As a starting point, he said that U.S. military facilities will need to guard against what he called the "Ukraine-type threat" of small groups using multiple drones to go after targets. "They only have to be used once, and you only have to be successful once," Bendett said. "I know the U.S. military is learning, and internalizing these lessons, and people are trying to understand what kind of threats they're facing. Is it happening fast enough?"

The U.S. military has worked for at least three years on counter-swarm defense – mostly involving high-energy lasers and high-power microwave (HPM) systems.

Recently the head of the Army's Rapid Capabilities and Critical Technologies Office (RCCTO) announced a competition for high-energy laser weapon systems focused on countering drone swarms. The RCCTO has already built several directed energy prototypes; this would be a higher-level weapon, and hopefully one that would move from prototype to operational system.

"We have to continue to work harder," Lt. Gen. Robert Rasch, the RCCTO director, said at this month's Space and Missile Defense Symposium. "We have to continue to work with industry to develop our directed-energy platforms and focus on the areas of reliability."

Among other American swarm-defense projects: The Air Force's THOR, an HPM directed energy weapon, and the Leonidas HPM system, developed by Epirus and fielded with the U.S. Army, both of which emit electromagnetic pulses capable of disabling multiple drones simultaneously.

On August 26, the Leonidas system defeated a swarm of 49 quadcopter drones in a test conducted at an Indiana National Guard base. Axios

reported that “suddenly, all 49 — like a flock of stricken birds — crashed into a grassy field.” Their circuits had been overwhelmed by the system’s electromagnetic waves.

Epirus’s CEO, Andy Lowery, says Leonidas creates an “electronic dead zone” that disables anything that carries computer chips.

“It works for drones, which are like flying computers,” Lowery told *Defense One*. “It will stop a Tesla in its tracks, it’ll stop a boat motor in its tracks, anything with a computer inside of it.”

[related module]

Other NATO members are working on counter-swarm technology as well. The German startup Alpine Eagle has developed a system known as Sentinel – a platform that deploys drone swarms against other drone swarms. Sentinel has been tested by the German Armed Forces and in Ukraine against FPV (first-person view) drone threats; Poland has deployed SKYctrl, which sends drones to collide in “non-explosive” fashion with other drones; and the British U.K. Ministry of Defense said recently that its “Radiofrequency Directed Energy Weapon,” mounted on a truck chassis, had successfully “defeated” swarms of drones. Far from Europe, India's Bhargavastra, developed by Solar Defence & Aerospace, used unguided rockets to eradicate swarms of drones at close range.

“The more sophisticated, latest versions are the ones that can actually interfere with the commands inside the unmanned drones,” Studeman said. “This smart neutralization, through a kind of electronic interference that goes after the actual logic and the commands of the UAS unmanned aerial system itself, shows you where this is going.”

All that said, some experts worry that the U.S. military isn’t adequately prepared for the drone-swarm threat.

“The U.S. is not ready,” Pettyjohn said. “It has begun to procure some defenses that were specifically made to counter small drones…and that's good. But you really need these layered defenses, where you have cost-effective interceptors.” She and other experts say that for all the tests and pledges, the U.S. has yet to show that it has an effective multi-layered defense against potential swarm attacks.

“High-powered microwaves are the one emerging technology that the U.S. Army has fielded a few prototypes that hold the promise of actually being able to knock out a true swarm,” she said. “The challenge is it requires a lot of energy. It's a very short-range weapon, so it's like your final force field. You need those longer layers of kinetic and EW interceptors to try to thin out the herd. And you have to figure out how to use the high-power microwave in a way that doesn't fry the electronics of US military equipment that it's trying to defend.”

Gagnard agrees that more work needs to be done.

“I'd say we have weapon systems that can defeat drones on a small scale,” he said, “but on a large scale, right now the aggressor is going to have the decisive advantage if they're incorporating this swarm technology into their repertoire.”

China’s drone-swarm advantage

Military experts – including the head of the U.S. Indo-Pacific Command – have said that the opening salvos in any Pacific war would almost certainly involve cutting edge drone-swarm technologies. And last November, China unveiled a potentially devastating tool in the drone-swarm ecosystem. Experts called it a "drone mothership."

The Jiu Tian, introduced at the Zhuhai Air Show, China’s biggest aerospace trade fair, is an 11-ton aircraft billed as the world’s largest drone carrier. It is itself a drone, an enormous one, operating without a crew. According to several reports, the Jiu Tian can carry as many as 100 smaller UAVs more

than 4,000 miles and unleash them against a target. Essentially, it's a delivery vehicle for a drone swarm.

"China is going like gangbusters right now" in the drone space, Studeman said. "They have the manufacturing capability. They've built thousands of armed drones, and they've built the equivalent of motherships, where the intent is to throw lethal capability forward."

As *The Cipher Brief* reported earlier this year, China's military is in the throes of an innovation and manufacturing boom in drone weaponry to prepare Beijing for a potential war over Taiwan. China already produces some 70% of the world's commercial drones – and is building a rapidly growing AI industry.

"They have the production, they have large inventory and now they also have the AI," Dr. Michael Raska, a professor at the Military Transformation Programme at Singapore's S. Rajaratnam School of International Studies, told *The Cipher Brief*. "With all these combined, they have been experiencing a leap forward in the quality and quantity of all the drones across the different domains."

China also has more than 3,000 manufacturers producing anti-drone equipment. In 2024, Beijing issued 205 procurement notices related to counter-drone technology; the figure was 122 in 2023, and only 87 in 2022.

"Our manufacturing is weaker than the Chinese manufacturing in this regard, and scale matters," Studeman said. "Even with simpler technology. If somebody puts more robots on the front lines, we've got a problem, Houston."

"This is definitely one area where China has an upper hand with the numbers," Bendett said. "If Ukraine and Russia can manufacture millions (of drone weapons), then China can manufacture tens of millions, maybe hundreds of millions of UAVs."

It's not a stretch, Bendett said, to imagine China launching, in the early hours or days of a conflict over Taiwan, "10,000 mid-range UAVs at a

suspected American carrier battle group east of Taiwan. Do we have enough to defend against that group?" he asked. "What do we have in our arsenal?"

Are you Subscribed to The Cipher Brief's Digital Channel on YouTube? There is no better place to get clear perspectives from deeply experienced national security experts.

The terror threat

Beyond the military applications for drone swarms, there are important civilian uses. Disaster relief, search and rescue missions, and fighting wildfires are often mentioned, given the ability of drone swarms to map affected areas and conduct support operations in dangerous conditions.

Then there are the nightmare applications – primarily, the fear that as the ease and accessibility of drone-swarm technology grows, so will the odds that it will land in the hands of terrorists.

In March 2025, the U.S. conducted a war game that envisioned multiple drone attacks against U.S. military facilities. The exercise, which involved more than 100 participants from 30 agencies, uncovered deficiencies in response and highlighted the need for coordination among federal, state, and local authorities. A lack of clear rules of engagement across nearly 500 U.S. military installations was identified as a major concern.

Experts also worry about attacks on non-military sites – which as a rule are far less well defended.

"They could be at different sporting events or other large gatherings," Pettyjohn said. "Obviously, as with any form of terrorism, you're not going to be able to protect people everywhere, but there needs to be a lot more counter-drone defenses for the homeland to prevent terrorist attacks from succeeding in really critical locations, either in terms of infrastructure or where there are large numbers of people."

“American infrastructure is very vulnerable,” Gagnard said. “We don't have solid defenses that are institutionalized, that are in use everywhere, and American infrastructure is a prime target for that type of attack.”

He added that drone technology – and lax U.S. laws – could allow a would-be terrorist to conduct reconnaissance on a target without being noticed. “In America, we have a relatively free sky,” he said. “You could fly drones all day long over certain things and never really raise anyone's radar.”

In the nightmare scenario for a drone-swarm terror attack, Gagnard said, the target would be assessed, the swarms well “briefed,” and – depending on the target – defenses might be porous.

“You wouldn't need very smart drones in order to do that,” he said. A drone swarm attack, he said, “could be very successful in America.”

Gagnard, who serves as a senior advisor at the Institute for Critical Infrastructure Technology, has argued for a “national counter-drone doctrine.”

“How are we going to counter drones? What's acceptable, what isn't acceptable? And then we need some sort of unified command. Someone needs to determine exactly how we're going to counter drones.”

Several experts cited Ukraine’s June Spider Web operation as a reason for concern – given how deeply it penetrated Russian territory, even *without* using the AI tools that might produce a “thinking” drone swarm.

“We should really, really worry” about a drone-swarm terror attack, Bendett said, “because if anything, the Spider Web operation showed that a well-organized effort that is enabled by commercial technologies can be devastating against an unprepared target.”

David Ochmanek, Senior International Defense Researcher at RAND, said that the U.S. has been “a little slow to recognize the magnitude of the threat” of drone attacks, in part because Americans are so far from Russia and Ukraine, where the drone-war realities play out on a daily basis.

“We've seen how clever adversaries can smuggle these kinds of capabilities,” Ochmanek told *The Cipher Brief*. “So we shouldn't be lulled into a false sense of security that our oceans will protect us, even from

attacks by fairly short range. The Houthis have shown us that they can launch these things. One can imagine an enemy loading them onto ships off our coast that would be indistinguishable from merchant ships, and launching from there."

While this year's White House executive order for a "Golden Dome" mandated a defense against all air threats, the order specifically referenced sophisticated missiles – not swarms of inexpensive drones.

Pettyjohn and other experts said that for domestic drone-swarm defense, the preference will be for non-kinetic systems – microwaves, lasers and so forth – to avoid shoot-downs that result in explosions or damage from falling debris. "In the homeland, there are a lot more restrictions on how you can take down foreign objects in the sky," she said. "The FAA gets involved, Homeland Security, local authorities – the U.S. needs to work through all of these issues and figure out bureaucratically how it would respond and what the policies and procedures are that are in place."

Studeman raised another concern – that drone swarms would be particularly effective if tasked with pursuing an individual.

"You think about protection of senior principals in government – a president, prime minister and on down," he said. "There could be a swarm of drones coming to simply do one thing: keep pounding until just one penetrates while one principal leader is exposed."

It's a collection of worrisome scenarios, few of which can be dealt with by even the most sophisticated "Golden Dome" defense – which of course is years if not decades away.

As Pettyjohn put it, "there is no easy fix to this challenge."

Read more expert-driven national security insights, perspective and analysis in The Cipher Brief because National Security is Everyone's Business.