

With drones, a bigger fence around your facility doesn't protect you anymore





Traditional thinking about protecting facilities must adapt to threats such as drones or downstream attacks

By **BREAKING DEFENSE**

Securing facilities both inside and outside the US is becoming increasingly complex, as new threats such as drones mean the old model of “gates, guards and guns” is no longer sufficient.

Protecting against constantly evolving, adaptable threats is driving a need for more and better data, but that creates its own challenge: keeping personnel informed and aware of threats without being overwhelmed by massive amounts of data while being able to identify whether a blip on a radar is a flock of birds, a hobbyist flying a harmless drone or something potentially dangerous.

It's not just drones. AI-driven cyberattacks are becoming ever more common and facilities face not only the threat of a direct attack, but downstream incidents such as attacks on data centers or power stations that could paralyze a facility.

“We’re facing these threats that no longer have a prepositioned posture in terms of who the threat is coming from or where it’s coming from,” said Jason Rahimitabar, Executive Vice President of LEXSO (Layered Extended Security Operations) at Constellis. “It is multi-domain, it is air, land, sea, space, cyber, and it is now more easily accessible to our adversaries.”

Defending against such a wide array of threats is not easy, but it is doable. It requires a combination of technology, personnel and adaptivity to be able to quickly identify potential threats and respond to them effectively.

The changing face of threats

Conflicts in Ukraine and Iran have highlighted an economic issue when it comes to protecting facilities, equipment and

On the cover: Building effective facility security to defend against modern threats requires more than traditional fences and security checkpoints. (Adobe Stock image)



LEXSO Security Operations Command, operating at the Constellis Training Center in Moyock, N.C. (Photo courtesy of Constellis)

people. The explosion of cheap, expendable drones allows for adversaries or rogue actors to launch waves of attacks in an attempt to overwhelm defense systems, and when those drones are shot down they are often being destroyed with effectors that are much more expensive.

"You have all these cheap drones that can cost 50 bucks and you're mitigating it with something that's costing anywhere from \$15,000, up to \$4 million per round" Rahimitabar said. "The economics just doesn't work."

That same conundrum exists outside of the frontlines. A military installation in the continental United States can be targeted with drones as easily as frontline installations can, as evidenced by a recent incident where Barksdale Air Force Base was overflown by drones in multiple instances. Although no damage was done, it highlighted one of the challenges of present-day security, which is that it's no longer sufficient to build defense out; they have to be figuratively built up, as well.

That doesn't mean building a taller fence. Instead, it's about having systems in place to track, identify and intercept airborne threats, which is made more difficult by the maneuverability and small size of readily available drones. They aren't easy to pick up with sensors or radar, and they don't follow a set flight path

or have to stay a certain distance from the ground.

"That threat from a \$50 drone that someone can buy online or at a hardware store, you don't mitigate the threat through a gate, guard or a gun," said Rahimitabar. "You need counter-UAS measures and UAS tracking and detection that makes it a more complex picture, and it extends out the need of where you actually detect threats. You're used to seeing the threat right on the perimeter line and if somebody jumps over that fence, they are a threat. But now because of how fast and how capable UAS are, you actually have to detect them much further out to be able to mitigate their potential risks."

Quickly identifying whether a drone is actually a threat is critical, because not every drone is dangerous. Facilities that are not isolated may have hobbyist drone pilots in the area who are undertaking harmless activity such as flying a drone in a nearby park, but if the drone wanders off course or gets too close to the perimeter, it can trigger a security alert. Activating counter-UAS measures in that case is not only expensive, but a potential public relations headache.

The economic calculus becomes less important when a drone is identified as dangerous. While it may be disproportionately expensive to take down an adversarial drone, the value



From left, U.S. Air Force Tech. Sgt. Roderick Gurumendi, security forces craftsman, Senior Master Sgt. Renato Simoni, senior enlisted leader, and Senior Airman Jose Martinez, security forces journeyman, all with the 156th Security Operations Squadron, Puerto Rico Air National Guard, secure the perimeter during Sentry South 26-2 exercise at Gulfport Combat Readiness Training Center, Mississippi, Feb. 20, 2026. (Photo by U.S. Air Force Master Sgt. Rafael Rosa, 156th Wing)

of what is being protected matters, as well. Spending a lot of money to destroy an innocuous drone doesn't make sense, but doing so to protect the lives of people or critical infrastructure certainly does.

Tracking and identifying drones or other threats requires excellent sensor capabilities, and that is one of the key capabilities that LEXSO is built around, said Rahimitabar. It is designed to integrate multiple sensing technologies including radar and LIDAR, and is built to be sensor agnostic. The system provides real-time data through a unified operating picture that operators can use to quickly identify potential threats and decide how to respond based on the information available to them.

"It brings all of those sensors into an orchestrated layer," Rahimitabar said. "It simplifies the interface for the operator to be able to make decisions in near real time, action those threats and make sure that they're not actioning the false alarms, which is just as important as actioning the threats. And you have this single pane of glass, if you will, that allows you to do that regardless of the sensor type or sensor manufacturer."

Downstream attacks

Defending a single facility is a relatively straightforward proposition. But modern facilities rely on off-site power generation, communications infrastructure and data centers to run effectively, and they are increasingly becoming targets of opportunity for those looking to hamstring a facility. Notably, in the recent Iran conflict two Amazon Web Services data centers in the United Arab Emirates were targeted, highlighting that threats are not contained to single sites, Rahimitabar said.

"Because of the interconnected world that we live in right now, that could be a commercial site like a data center, like a water storage facility, like a power facility. If you look up and down the supply chain of how the military operator will work, you can then track it now to commercial installations, commercial infrastructure and that is actively being targeted."

That means that security must be comprehensive to consider all factors instead of being isolated to only thinking about the physical footprint of the facility. Security personnel at a facility not only need to be able to protect that facility, but also be ➤

able to communicate with other facilities that provide critical resources and first responders.

Rahimitabar shared a recent example where LEXSO was meeting with a government customer, and the meeting didn't just include the head of security. Fire and safety was represented, as was search and rescue because the facility is located on a waterway. Information technology personnel were also there because of cybersecurity concerns, and IT infrastructure is critical to security operations. For all of those departments, having a common operating picture is crucial to ensure everyone is working from the same information.

"If you don't answer it as a holistic problem, then you're actually losing sight of where the threat could be coming from and how best to mitigate," said Rahimitabar. "Having all those stakeholders and not changing around the common operating picture on each of the stakeholders is important."

AI-driven security management

Data is critical to effective security. Being able to actually use that data instead of drowning in it, however, is even more critical. Saturating your coverage area with sensors only offers so much benefit if your operators are overwhelmed by the influx of data and can't figure out what it's all telling them quickly enough to make good decisions.

Artificial intelligence (AI) helps with that by quickly sorting through data and presenting it in a form that operators can understand and draw accurate conclusions from. In the case of LEXSO, layers of security measures all report to the same system, then that information is processed and presented to operators. That capability matters because AI can process massive amounts of data far faster than humans, and it can quickly compare against previous data to help identify what exactly is going on, said Rahimitabar.

"Because we have a layered approach to where we're getting multiple pings, maybe it's a radar, maybe it's visual line of sight that the camera got, maybe it's an acoustic sensor

that heard a noise," he said. "What AI can do is process the level of confidence through the layered approach to those sensors and give it to the operator, the human in the loop. Instead of AI just saying that, 'yes, that is a person and they have a drone and it's dangerous,' it can confirm that information through four different layers of data, four different types of sensors.

Securing facilities entails a number of challenges, including ever-changing threats, downstream attacks and managing data effectively to ensure that all stakeholders have a clear understanding of potential threats and how to respond to them. Those are big tasks, but can be handled through a commitment to the idea that security is a holistic endeavor that is constantly changing, not a static operation.

"We haven't fully adapted to this complex environment in terms of realizing that the security posture of critical infrastructure is not ready, nor does it have budgets yet to be able to handle the threat we're talking about," Rahimitabar said. "We have siloed our security operators and that security budget into just being the guards at the front gate, and we haven't thought through the complexity of the problem and evolved that level of thinking of what they should truly be securing."

That complexity makes security a constantly evolving challenge, but by offering capabilities such as sensor integration, AI-driven data management and a single interface for operators to quickly identify and respond to threats, LEXSO offers its customers the flexibility and adaptability needed to meet whatever security challenges they face.

"The true discriminator for LEXSO is that we solve these problems based on the customer need, but we have a foundational system that allows us to do it rapidly," said Rahimitabar. "By being super flexible, by being device agnostic, by making sure that we understand our customer needs and can deploy anywhere, we make sure that we solve that problem with our customer and understand what's the quickest and cheapest path to being super proficient and effective in their security posture."