

[www.vox.com /recode/2019/5/16/18511583/smart-border-wall-drones-sensors-ai](http://www.vox.com/recode/2019/5/16/18511583/smart-border-wall-drones-sensors-ai)

## The "smarter" wall: How drones, sensors, and AI are patrolling the border

Shirin Ghaffary

38-48 minutes

In an era of increasingly polarized politics, there are few issues as divisive as President [Trump's proposal to build a physical wall](#) across part of the 2,000-mile US-Mexico border.

The Trump administration has argued that the border wall is a necessary deterrent to drug smugglers and immigrants seeking to enter the country unlawfully. It says [unchecked immigration is a national security crisis](#), and one that needs to be addressed.

Critics, meanwhile, argue that the wall is a wildly expensive, ineffective, and misdirected effort. The actual crisis, they say, is a [humanitarian one worsened by Trump's restrictive immigration policies](#) — about refugees seeking lawful entry into the US to flee violence and poverty in their home countries.



President Trump tours the US-Mexico border wall in Calexico, California, on April 5, 2019.  
Saul Loeb/AFP/Getty Images

But there is another kind of border wall increasingly being talked about — one that proponents pitch as being less costly, less disruptive, and less politically controversial than a physical barrier: [a so-called "smart wall."](#)

The vision, as laid out by its bipartisan political supporters, is to build an ocean-to-ocean technological barrier made up of a patchwork of tools like drones and sensors to help surveil and identify unauthorized individuals crossing the border, specifically in remote stretches of land between established ports of entry.

Many have lobbed serious [ethical and human rights objections](#) to building this virtual wall. Some research has suggested that the last major effort to increase technology at the border may [have contributed to an increase](#) in the number of deaths of migrants crossing the border, because they were forced into taking more treacherous routes to avoid detection.

And then there are the privacy concerns. Major civil liberty and digital privacy groups like the American Civil Liberties Union, the Electronic Frontier Foundation, and Fight for the Future [have argued](#) that a hypothetical virtual wall integrating technology — like facial recognition and drones — could propel a

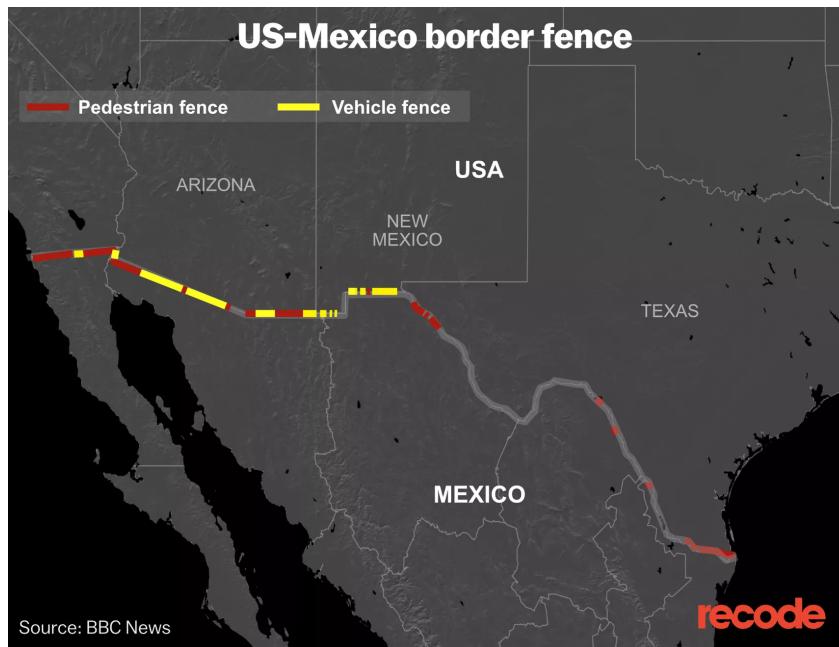
state of perpetual surveillance that would infringe on the human rights of immigrants and US citizens alike.

These groups' worries are understandable, particularly given the recent series of revelations showing how tech is already being used to enforce controversial immigration policies. Despite the company's previous assurances to the contrary, it was recently revealed by the organization Mijente that Palantir, the data analytics firm founded by Peter Thiel, contracted software to Immigration and Customs Enforcement (ICE) that reportedly helped target and arrest parents and other relatives of unaccompanied minors crossing the US-Mexico border. The Palantir case is just one revelation, but there are many more contracts between major tech companies and immigration agencies that remain under scrutiny and whose details are relatively unknown.

Nevertheless, the idea of bolstering a technological wall has backing from key politicians on both sides of the aisle. Those supporters include House Speaker Nancy Pelosi; Reps. Will Hurd (R-TX), Henry Cuellar (D-TX), and Brian Fitzpatrick (R-PA); and Sen. Jon Tester (D-MT).

"In this 21st century, we have challenges, and I think we can use 21st-century solutions instead of a 14th-century solution called the wall," said Cuellar in an interview with Recode. "Even if you put in a fence, 'bad guys' can use drones to carry drugs over that fence. So we have to be more flexible, more agile."

Politicians who control the purse for security spending find a smart wall's cost-effectiveness appealing over extending a physical wall that could cost millions of dollars per mile.



"We can literally do technology for pennies on the dollar as compared to a physical wall," said Tester, a member of the influential Senate Appropriations Committee. Tester had recently come back from a trip to the border, where he said he talked to families who lived and farmed there and were worried about seeing their businesses destroyed by a physical barrier that could divide their land.

"This is about truly securing the southern border without ripping farms apart, without creating a zone that people won't be able to utilize," he said.

On the Republican side, Rep. Hurd — whose district includes a large area of the Texas southern border, and who is one of the few members of Congress with a computer science degree — has been one of the strongest advocates for a technological wall.

"Every mile of the border patrol is different — radar makes sense in one place, lidar may make sense in another, a high-resolution camera may make sense in some," said Hurd. "We should be agnostic as to what the sensor is, but we should be using the one that makes the most sense and the one that is the cheapest."

There's potential for a technological overhaul to increase efficiency at the border, but the last major effort to do so failed miserably. SBINet was a vast initiative to create a patchwork of interconnected surveillance equipment like towers and ground sensors. It was started under the George W. Bush

administration in 2006 but [was canceled](#) five years later, after a [government oversight report came out questioning its effectiveness](#) and more than \$1 billion had already been spent on the project.

But proponents of renewed investment in tech at the border argue that technology has come a long way since the mid-2000s — particularly in AI-backed image detection. Tech companies are taking advantage of this political opportunity, saying that their products could be a game changer for border security.

Surveillance and defense tech startups have found early success with the deployment of their tools like drones, AI software, and new sensors — some of them extending small-scale pilots into longer-term contracts.

While smaller startups take on larger defense company behemoths for lucrative government contracts, larger tech companies will have to weigh the reputational risk of expanding into border surveillance.

As the past year has shown, employees at companies like Google, Microsoft, and Amazon have grown increasingly critical of government uses of their technology for defense and surveillance purposes. Several firms, including [Microsoft](#) and [Salesforce](#), have faced criticism from their workforce over contracts with ICE and Customs and Border Protection (CBP), respectively.

Because of the newness of some of these projects, relatively little about their scope is known. Their potential to expand depends in large part on political support — and funding — as well as their ability to prove their effectiveness over existing technologies.

After interviewing government officials, executives at surveillance technology companies, and industry analysts, then combing through Department of Homeland Security (DHS) and CBP documents, Recode took a closer look at some of the latest tools and their potential — and peril — at the US southern border.



The Mexican side of the US-Mexico border barrier in Tijuana, Mexico, on March 30, 2019.  
Mario Tama/Getty Images

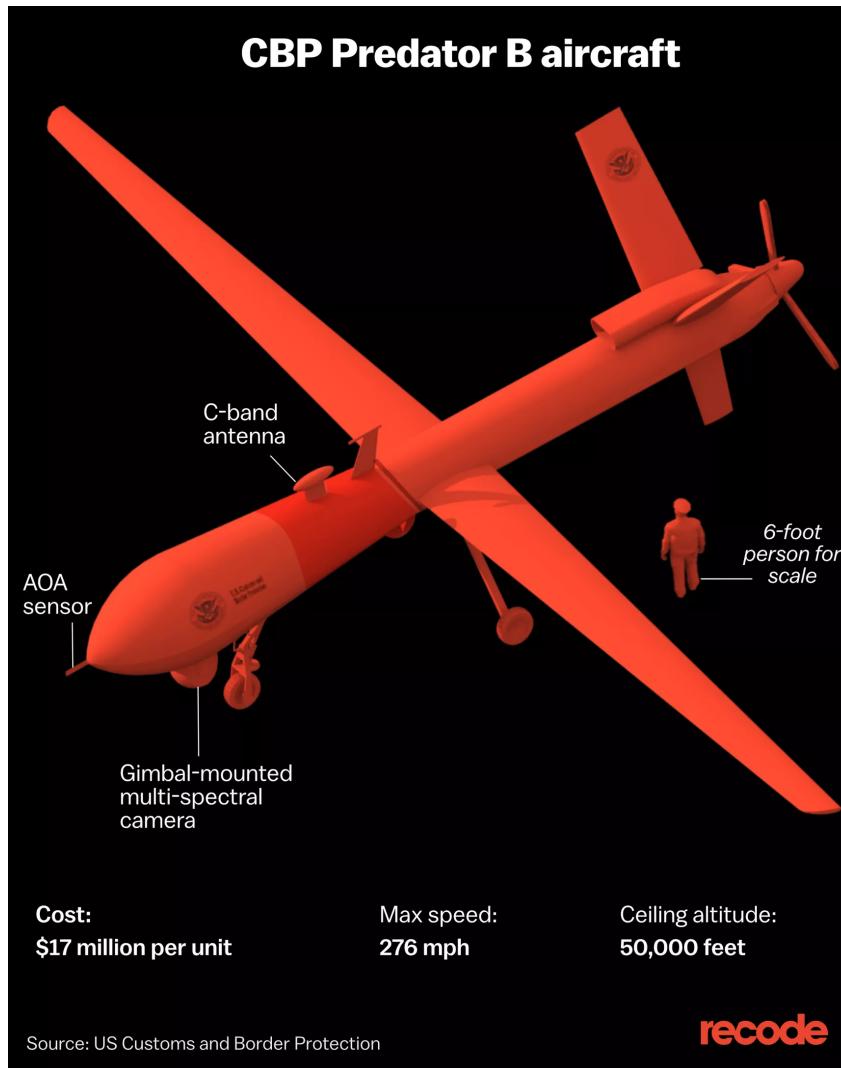
## Surveillance drones big and small

For border patrol agents trying to surveil the long, rural, mountainous stretches of the border, unmanned surveillance aircraft — more commonly known as drones — are a favored tool. They're used to detect suspicious activity along treacherous terrain and to get a closer look at areas that may be inefficient or unsafe for personnel to patrol in person.

The oldest type of unmanned aircraft in use at the border is the hefty [36-foot-long, nearly 5,000-pound Predator B drones](#). These aircraft were built for military use, but CBP has been flying them [at the US-Mexico border since 2006](#). On the battlefield, the Predators can carry and deploy bombs, missiles, and other weapons, all while being remotely controlled by pilots at ground bases, sometimes thousands of miles away. At the border, they're used to detect and assist in surveillance along broad stretches of land, helping to identify illegal crossings and guide enforcement agents.

These aircraft can stay aloft for [nearly 30 hours at a time](#) and can read something as small a [license plate number from 2 miles high](#). They capture high-quality images using multiple sensors, including

sophisticated detection tools like an electro-optical infrared scanner and a thermographic heat sensor, sending data back to a ground control station via satellite link.



For CBP, a major flaw of these military-grade drones is their high cost. They [run around \\$17 million each and cost around \\$12,255 per flight hour to operate](#). Every time CBP uses a drone to apprehend an individual suspected of crossing the border illegally, it costs the federal government \$32,000, compared to an average cost of less than \$9,000 for other types of surveillance that could lead to an apprehension, [according to analysis of publicly available data](#) from the libertarian think tank Cato Institute from the years 2013 to 2016.

They also aren't exactly easy to use. [At least two of CBP's Predator drones have crashed](#) — one due to human error and the other due to a generator failure. A DHS [Office of Inspector General report in 2014](#) found that, overall, the program had failed to meet expectations and could not prove its effectiveness; the report concluded that the program had "not achieved the expected result," and therefore recommended that the government reconsider expanding it. Still, despite the questions about their efficiency and cost, CBP continues to use Predator drones.

But now, due to rapid advances in technology in the past two decades, a newer generation of smaller, cheaper drones is popping up. In the past two years, CBP has increased its testing and ordering of these new types of drone technologies. These devices, called [sUAS \(small unmanned aerial systems\)](#), weigh less than 55 pounds. They can't stay in the air as long as the larger Predators and they're more vulnerable to bad weather conditions, but they fly at a much more efficient cost and require far less training to use.

These sUAS systems are a way to fill a void in border patrol's operations; the agency is limited in how many hours it can spend piloting larger aircraft, according to Michael Harrison, associate chief of special operations with border patrol headquarters. Border Patrol has had "great success" with the sUAS systems they've used so far, he said.

These smaller drones look much less intimidating than their hulking Predator cousins. They were also initially developed for military use in Iraq and Afghanistan, but seeing as they can carry a much smaller payload than the Predators, they're used for surveillance rather than deploying weapons. The drones can collect images and video, and in some cases, using AI, they can automatically sense if there is a suspected person where there shouldn't be. They then send real-time video of the target to the person controlling the aircraft, who can be miles away, for further inspection.

Let's say, for example, that a border agent at a control center suspects possible unauthorized human activity at a mountainous part of the Texas-Mexico border that's difficult to reach by car. Instead of sending out an agent on a three-hour journey through rugged terrain to investigate what could be a false alarm — like an animal moving around — they can fly a drone to investigate instead.



The Chisos Mountains of Big Bend National Park, situated on the remote Texas-Mexico border.

*Robert Daemmrich Photography Inc/Corbis via Getty Images*

CBP says the drones are used not for prolonged surveillance but instead for targeted investigations.

For example, sUAS drones can help identify if someone is carrying a shovel or a gun — or, say, a small backpack or larger potential package of narcotics. CBP characterizes this as "situational awareness" to help ensure the safety of human agents on the ground.

There are limitations: sUAS drones can generally only fly for up to a couple of hours at a time, and only in fair weather.

With regard to where these devices are allowed to fly, CBP says it largely uses these drones within the "immediate border area" within 25 miles of the border. Legally, the agency is restricted by the Federal Aviation Administration to fly drones between [25 and 60 miles of the US-Mexico border, excluding urban areas](#). But many civil liberties advocates worry about scope creep (that these drones could be used to surveil beyond these areas), and that even within the legal ranges, many US citizens are vulnerable to being monitored.

"This idea of drones or sUASes that have the capacity to capture images and videos being used at the border is pretty concerning," said Neema Singh Guliani, a senior legislative counsel with the ACLU. "There's lots of people who live near the border, and there have been some concerns with privacy control. In some cases, the law is not as clear as it should be in terms of how DHS should share data."

Between October 2018 and April 2019, US Border Patrol flew these SUAS devices for a total of around 176 flight hours, resulting in 474 apprehensions of individuals at the border, according to a CBP spokesperson. Border Patrol said it will continue to increase the number of SUAS units deployed and expects the apprehensions to increase significantly over the next six months.

## Border surveillance small drones

<b>AeroVironment RQ-11B Raven</b> 	Altitude: 100-500 feet  Max speed: 50 mph  Endurance: 60-90 min.
<hr/> <b>Aeryon R80D Skyraider</b> 	Altitude: 1,500 feet  Max speed: 31 mph  Endurance: 30-50 min.
<hr/> <b>Lockheed Martin Indago 3</b> 	Altitude: 10-500 feet  Max speed: 25 mph  Endurance: Up to 50 min.

*6-foot person for scale*

Source: [avinc.com](http://avinc.com), [aeryondemand.us](http://aeryondemand.us), [lockheedmartin.com](http://lockheedmartin.com)

**recode**

Overall, CBP said it recently placed an order for around 100 more sUAS systems, including about 40 [Aeryon SkyRaiders](#) and 60 [Lockheed Martin Indago 3 systems](#), as well as AeroVironment Ravens and InstantEyes on loan from DHS. This batch of drones will be placed all across the US southwest border, as well as a few at the northern border, as the agency continues to run pilot programs assessing their use.

There hasn't yet been an efficiency study like those for the older Predator drones, so aside from anecdotal evidence from trials that CBP says are promising, it's hard to say exactly how useful these tools are proving.

"We don't want to buy tech that we think is a great idea, buy mass amounts of it and then not realize any value of it in the end," said Harrison, who said the agency is continuing to use these technologies in relatively "small numbers" until they better understand how well they're working and what scenarios they're best suited for.

### AI-enabled drones and surveillance towers

Even smaller autonomous drones aren't really fully autonomous. Human beings have to launch and operate them, and that requires training. So far, for example, AeroEnvironment said it has trained 25 Border Patrol agents on how to fly its sUAS drones.

Aside from those operators, these vehicles also require a small team of several staff who are manually looking over the live images they transmit, sometimes for hours on end. And, of course, staffing people to review footage around the clock proves to be a big cost for CBP.

That leaves room for a new batch of Silicon Valley-backed companies to market AI-enabled devices that they claim can process surveillance images from the border more efficiently and with greater accuracy than human beings. What differentiates these tools, say their makers, is their ability to detect patterns to identify human activity in a noisy stream of images and signals coming from a patchwork of sensors.

New machine-learning algorithms, taking advantage of advancements in the field, can process signals and images at rapid speed, their creators say, and can detect anomalies with greater accuracy than human beings.

"I don't think there's an organization on the planet that doesn't want to do something more efficiently using AI," said Ari Schuler, director of CBP's Innovation Team, a recent Silicon Valley-style unit within the agency that's tasked with finding and deploying innovative technologies into Border Patrol agents' daily operations. "The art of letting a computer see like a person is tremendously valuable," he said.

Of course, letting a computer see like a person can introduce its own problems. Facial recognition technologies in particular raise a host of ethical questions, as they've been criticized for having baked-in [racial and gender bias](#).

Schuler says CBP is not currently using facial recognition tools for surveillance at the border, although [the agency has expressed interest in acquiring drones with facial recognition technology](#) for future use. And biometric technologies that use facial recognition to match travelers' pictures to databases are already being used at established [points of entry such as driver checkpoints and airports](#).

In the meantime, though — while it's not facial recognition — CBP has increasingly started using new drones and surveillance towers that can employ AI-powered software to more rapidly process information from radars and cameras at the border.

One of the leading companies [making that technology is Anduril](#), a 2-year-old startup that's been heralded in national defense circles. The company's high-profile young founder, Palmer Luckey, is something of a Silicon Valley wunderkind who developed the virtual reality company Oculus. He [sold that company to Facebook for \\$2 billion in 2014](#), only to be [ousted from the company in 2017](#) amid political controversy. The 26-year-old, Hawaiian shirt-wearing exec stands out among many of his tech peers for being a [vocal supporter of the Trump administration](#) and the defense industry.

There's a futuristic, gamer feel to Anduril's products, which, going back to Luckey's background with Oculus, bring a kind of virtual reality simulation experience to border surveillance. While Anduril isn't licensing this technology to CBP yet, it's easy to envision a future where agents could be wearing headsets that immerse them in a 3D rendering of real-time activity at border areas.

Anduril's [helicopter-style drones](#) are small enough that they can fit in a backpack and are barely audible at 400 feet away. From a hardware perspective, what differentiates them from sUAS drones is that only one person is needed to launch and operate them and can do so remotely from a mobile phone. Anduril says its tools are a fraction of the cost of sUAS drones, which can run around six figures for a system.

The company has made an impression on politicians. "Clearly, they're smart people," said Sen. Tester about executives at the company. About a year ago, Tester took a meeting with Anduril to hear the company's pitch to outfit the border with surveillance technology. He was impressed by their claim to be able to provide a significant level of security for \$100 million — what he found to be a minuscule cost compared to the tens of billions proposed to build a physical wall. "They've dealt with technology, and they take the best of AI and put it with cameras and surveillance systems the right way," he said.

But while drones work well for targeted surveillance, they aren't as well-suited to monitoring wide stretches of land for a long period of time. For that, Customs and Border Protection uses integrated fixed towers (IFTs). These are 80- to 140-feet-tall metal structures, similar to radio towers, [laced with day and night sensors](#) and radars. The most common type of IFT used can surveil up to a radius of around 6 miles from where they're stationed. They've been deployed along remote sections of the southern border to fill in gaps of areas not regularly covered by agents. They work in concert with ground sensors and some other types of mobile and surveillance equipment.



Surveillance cameras overlook a section of the US-Mexico border outside of Nogales, Arizona, on October 12, 2016.

*Frederic J. Brown/AFP/Getty Images*

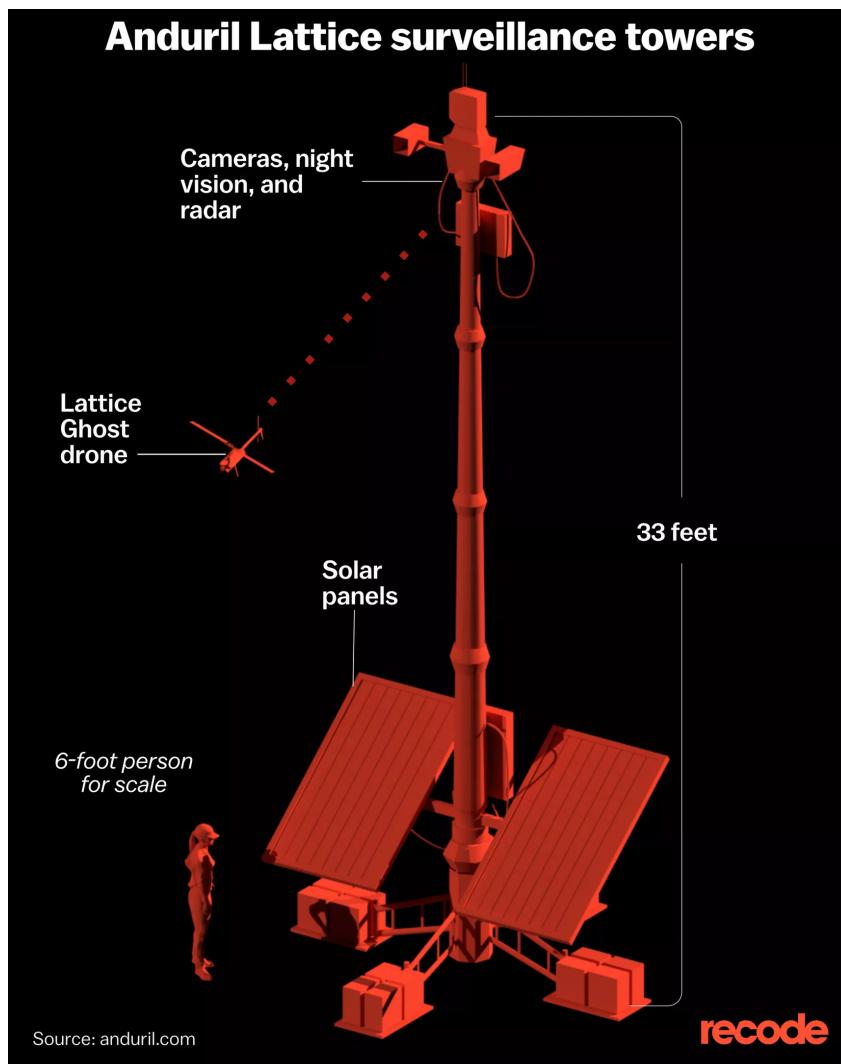
Historically, one contractor — the Israeli-based Elbit Systems — has grabbed the lion's share of contracts for this equipment. It's deployed 55 towers so far along the Arizona-Mexico border as part of a \$145 million federal contract with CBP. And it plans to install at least 10 more. The company has experience outfitting contentious border zones in Israel, where it supplies surveillance technology along the West Bank barrier between Israel and Palestine. It's currently [Israel's largest nongovernmental defense and surveillance company](#).

But companies like Anduril, which also makes its own version of the tower, are positioning their tools as better, and homegrown, alternatives to Elbit's technology. While the drones are the flashiest of Anduril's offerings, their leaner, cheaper, AI-backed version of surveillance towers are where it's found the most success so far at the US-Mexico border.

Last summer, Anduril ran a test on its tower equipment on private land in Texas that helped border agents apprehend [55 people crossing the border and seize 982 pounds of marijuana](#) in a 10-week period, according to Wired. The company recently [expanded the scope of its technology to the California border under a contract with CBP](#).

The main advantage companies like Anduril say they have over older equipment is their ability to process on the back end the images their devices capture, without human input. While the cameras on the towers aren't as expensive as some of their competitors, the company says the AI it uses on the back end can help identify patterns more precisely.

Matthew Steckman, who is the head of corporate and government affairs for Anduril, said AI is more efficient than having "scores of people sitting in front of screens. Let technology do what it does well and let humans do what they do well."



For Border Patrol officials, finding enough of those humans to staff their agency has been a challenge. Historically, CBP has struggled to hire and retain Border Patrol agents, especially for posts at remote stretches of the border. Last year, the agency [had around 2,000 vacant job positions](#). There's only more pressure now that President Trump's administration has been [pushing a proposal to hire 2,750 more agents](#). Companies like Anduril are still proving their case that they can be as effective as a human at doing part of the job of a Border Patrol agent; if they're able to pull that off, they're tapping into an opportunity to fill a gap in staffing.

Similar to Anduril, another tech startup, the Silicon Valley-based Cogniac, is developing AI image processing software that it's marketing for use at the border, along with other commercial applications such as for monitoring quality control at factories. Unlike Anduril, though, Cogniac doesn't build hardware. [Its pitch](#) is that by focusing only on the software, it can make its AI best in class.

Gradient Ventures, an investment arm of Google's parent company Alphabet, is one of a handful of investors in the company. This could raise questions with many of Google's politically active employees, who in the past have [protested Trump's restrictive immigration policies](#) and successfully pushed the company to [drop its defense contracts with the Pentagon](#).

Cogniac uses what's called a convolutional neural network to process images. Neural networks, modeled after the human brain, have revolutionized AI's capacity to train itself to recognize images. A convolutional network is a specific kind of neural network well suited to identifying images and sensing patterns in them.

"AI in its current form really only started to exist in 2012; before then, this type of technology was a toy," said founder and CEO Bill Kish, who added that previous attempts at outfitting the US-Mexico border with technology like SBINet weren't successful simply because the kind of technology to rapidly process images just wasn't available then.

Cogniac says it has participated in trials with CBP and that it's exploring ways for a bigger deployment.

Still, a majority of the surveillance towers currently in place at the border are sending the images they pick up to human beings, not AI. Elbit isn't taking this new technological revolution lying down, though. It says it's building AI capabilities into its technology systems used at the border as well.

"There are lots of great companies coming up in Silicon Valley," said Elbit's vice president of Americas, Gordon Kesting, "We keep our eyes on those developments and look to adopt any capabilities that are coming out there and look to adopt them into our solutions."

## Sensors, sensors everywhere

Images are just one kind of signal that officials use to monitor the border. Audio, radar, seismic, acoustic, and magnetic cues from ground sensors are often a first line of defense for detecting activity. They also make up the bulk of tools in CBP's arsenal as measured by pure volume. Thousands of ground sensors are currently in use between ports of entry at the US border.

Once a sensor detects activity such as movement in an area that could signify a group of people crossing the border, CBP may send an agent or a drone camera to the area for further inspection.

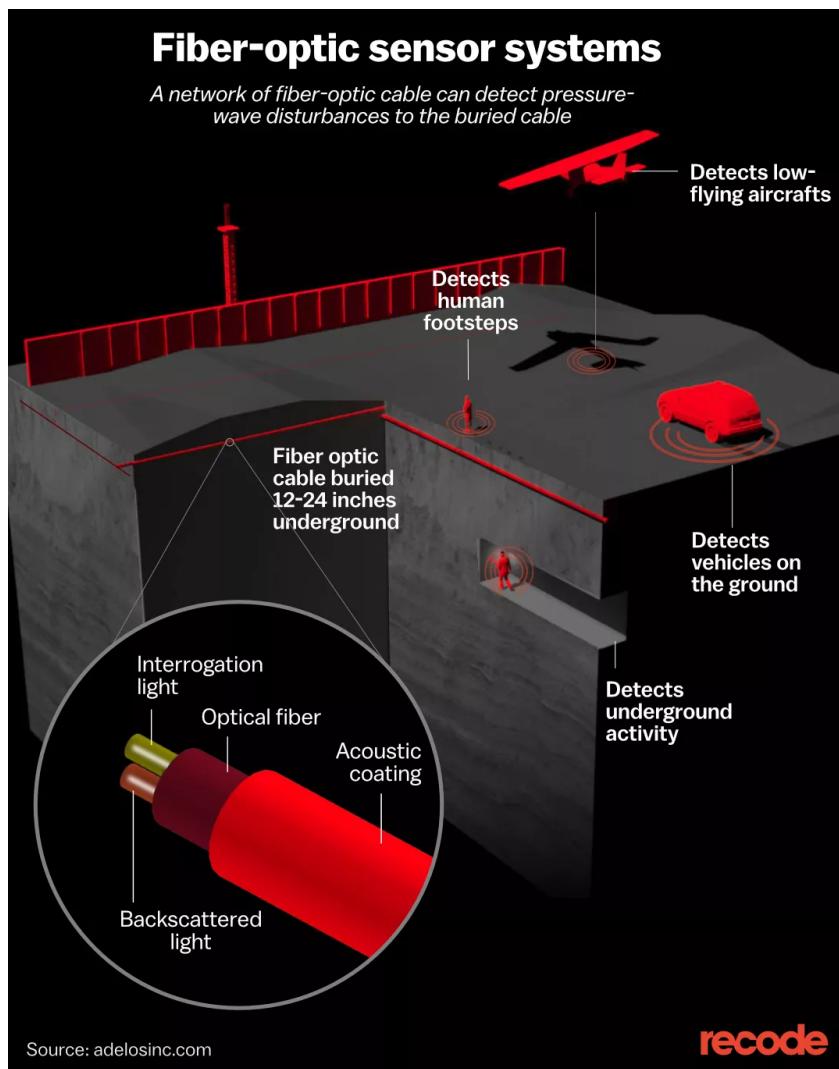
But sometimes these sensors give false alarms — like a stray cow roaming around or the sound of rocks falling from a mountain on a windy day. And when a response to a bovine incursion might require hours for an agent to reach the remote sensors, it's obvious that a more sensitive detection system could help. That's why some tech companies are pushing new kinds of sensor technologies.

One proposed solution is lidar, a [precise surveying method](#) that can measure and model targets in 3D. Lidar sensors do this by emitting pulsed laser light, then measuring the reflection of this energy from the solid objects it hits. If all that sounds familiar, that's because it's the same kind of technology used to help some driverless cars determine if a human being or object is in its way. It's also used by archeologists to detect topography, like where [ancient Mayan ruins might lie beneath a dense tropical rain forest](#).

One Sunnyvale, California-based company, Quanergy, tested lidar technology with local law enforcement agencies in Texas last year and is reportedly [vying for a contract with CBP](#). Last year, the Department of Homeland Security's Science and Technology division also [awarded the company \\$200,000](#) to develop its lidar capabilities for use at airport security and customs processing queues. It's still a very new area for CBP, and one it's working out.

Another new kind of sensing tool that's been proposed at the border is fiber optic sensing technology. CBP has only recently begun testing this technology, in some limited cases.

Fiber optic sensing works by measuring the backscattering of light in an optical fiber when it encounters vibration, strain, or temperature change. Fiber optics is most associated with telecommunications technology that can transmit internet, television cable, or cellphone signals; you've probably heard of it in relation to Verizon's FiOS or undersea cables. In the case of the border, however, this technology can be used to measure slight changes in the atmosphere that might detect human activity.



Thin glass-fiber optic cables, buried 1 to 2 feet underground, can pick up faint vibrations to register nuanced sounds as the highly sensitive glass cables bend based on the pressure waves at specific frequencies. These cables can also pick up on sounds underground, which makes fiber optic sensing technology an attractive tool for detecting illegal tunnels used to transport drugs across the border — a major problem for Border Patrol [since El Chapo first popularized the method in the 1980s](#). Since these systems don't carry electrical signals, they're also less detectable by smugglers than many other types of sensors.

Rep. Hurd, in particular, has been a vocal [proponent of fiber optic technology](#). He's said it should be outfitted across the entire 2,000-mile stretch of the US-Mexico border and has proposed combining the underground sensors with fiber optic communications technology to provide high-speed internet access to remote stretches at the border, including remote rural areas in his district that currently lack internet.

Adelos is a Montana-based company that makes fiber optic sensing systems and has several contracts with the Defense Department to secure areas outside the US-Mexico border, such as military bases.

The firm's founder and CTO, Alex Philp, says some of the sensors currently being used at the border run on "Vietnam-era" tech, and that fiber optics has the power to drastically improve the precision of signal detection at the border. Philp says that Adelos's systems can distinguish the sound of a drone from the wind, or a motorcycle from an ATV. That's partly because the company uses machine learning to create profiles of these unique frequencies and separate them from one another.

The bottleneck with operationalizing new technologies like fiber optic cables isn't just funding but also the slow, methodological, and often painstaking process of federal contracting.

"DHS, which is massive, has a lot of responsibility for a lot of different threat types," said Philp. "It can take a long time for contracts to be understood and for them to field new technology."

## Mobile data surveillance and communication

CBP and ICE can detect, locate, and collect information about people around the US-Mexico border by acquiring their location data.

According to a February report by the Wall Street Journal, CBP and ICE have bought [access to a commercial database](#) that tracks “millions” of cellphones in America, and the agencies are using it to identify and arrest undocumented immigrants at the US-Mexico border.

DHS spent \$250,000 in contracts in the past few years from Venntel, a company that licenses location data and is affiliated with the mobile ad company Gravy Analytics. And in September 2019, CBP bought \$1.1 million in licenses for Venntel subscriptions and other software.

The agency previously acknowledged it may acquire “commercially available location data” from “third-party data providers” in order to “detect the presence of individuals in areas between Ports of Entry where such a presence is indicative of potential illicit or illegal activity,” according to a [DHS privacy report](#) last year. The report states that CBP buys location data that includes an anonymized unique ID for a device detected, along with that device’s location, time, date, and how many other signals are near it. CBP has said that it doesn’t collect personally identifiable information, however, only enough to detect the presence of individuals at the border.

While DHS hasn’t said that it purchases historical cell location data in particular, for years, cellphone carriers have been selling customer’s location data to third-party brokerage firms, which then resell the information — mostly to advertisers but also to government agencies. Wireless carriers have faced increasing scrutiny over these practices for violating people’s privacy. Most major carriers such as [AT&T](#), [Verizon](#), and [T-Mobile](#) have pledged to stop due to public outcry and the potential for [FTC or FCC intervention](#).



Cellphones of asylum seekers wanting to stay in the US charge in Juventud 2000 migrant shelter, in Tijuana, on March 5, 2019.

*Guillermo Arias/AFP/Getty Images*

When asked about the practice of mobile surveillance at large, CBP acknowledged that if there is commercially available location information and a company is selling it, “the government could be one of those entities” that purchases that data if it is in the agency’s enforcement zone.

“The No. 1 thing that’s key to understand here is that we’re not looking at *who* is there; we’re looking to see *if* there is someone there,” Schuler said.

CBP also [uses devices referred to as “stingrays,” “cell site simulators,” or “IMSI catchers,”](#) according to the ACLU, which can detect and intercept cellphone signals in real time, although it’s not known if they are being used at the US-Mexico border specifically. These devices mimic legitimate cellphone towers and pull the location and other information from mobile devices trying to connect with the fake tower. Stingrays can not only detect the presence of a cell but also intercept text and voice messages and in some cases even send them out. From 2010 to 2014, CBP spent about \$2.5 million to acquire cell-site simulator technology, according to a [US House of Representatives Committee on Oversight and Government Reform report](#).

Meanwhile, CBP is working to enhance its own secure but agile communication networks. Much of the US southern border doesn't have cell or internet service. That's why the agency is actively commissioning new communications technologies that are more sophisticated than the radios and walkie-talkies that many agents still rely on.

"All the technology in the world means nothing if you don't have a reliable network that can bring that data to a customer," said Schuler.

CBP said it employs satellite communications that are used in commercial space applications and small form-factor radios with a mesh network. It's still a limited form of connectivity, but Schuler compares it to how people can use an offline version of Google Maps on their phones even when they don't have signal.

As mobile data connectivity across the border increases, CBP will have increased opportunities to better communicate among its workforce, as well as surveil other people within the border zone. How exactly it chooses to do so, and whether that infringes on US citizens' lives, is a major worry for many.

## Privacy and civil liberties concerns

The smart wall may be appealing to politicians who think it's a superior alternative to a physical wall, but some civil liberties advocates argue that from a privacy perspective, it's actually worse.

"People throw out the idea of a smart wall as if it's harm-free, and that's generally not the case," said Giuliani, [who co-authored a blog post for the ACLU](#) raising objections to increasing funding for a smart wall.

Under the Fourth Amendment, US citizens are protected from random and arbitrary stops and searches. However, under federal law, those [protections are somewhat limited in the border zone](#) — [defined as a 100-mile radius](#) from any US border.

More than 200 million Americans, or nearly two-thirds of the US population, technically live in a border zone, [according to the ACLU's estimates](#). Some states are entirely encompassed within one — including ones you probably wouldn't think of, like Maine. So technology used at the border in Arizona could set precedent for what kinds of surveillance the government can use toward someone living on the other side of the country.

Privacy advocates worry that this could have dangerous implications for CBP to potentially spy on US residents in their daily lives.



An overview of El Paso and Ciudad Juarez, Mexico, from Texas, on January 19, 2019.  
Joe Raedle/Getty Images

"Surveillance at the border doesn't stay at the border," said Mana Azarmi, policy counsel with the Center for Democracy and Technology, [who specializes in security technology](#) legal issues. She said she worries that sophisticated new surveillance tools will be used to surveil the lives of US citizens: "People living in these areas shouldn't feel like they're being monitored every time they go to their doctor or place of worship."

While there's currently no evidence that CBP is doing that, there are several examples of other law enforcement agencies using surveillance technologies beyond their intended use, such as police departments using drones to surveil underserved communities and political activists.

For example, an aerial surveillance "eye in the sky" system explicitly designed for military use in Iraq was later used by local police to quietly watch [the residents of the entire city of Baltimore](#). In another case, police in the San Francisco Bay Area [used drones](#) — unknown to the public — to monitor protests in the area.

Critics fear that the increasing video and images taken at the US-Mexico border could similarly be used beyond their stated purpose of monitoring illegal border crossings. CBP policy currently states that data captured from drones should only be stored for five years. After that, the information is supposed to be destroyed.

DHS Border Patrol officials say the agency follows strict privacy guidelines and does not use its technology to surveil US civilian life.

"Our highest priority is always technology that can keep our agents and officers safe," said Schuler about CBP's potential use of privacy-sensitive technologies, but also said that the agency also puts an "extreme lens on maintaining the utmost parity with our laws" and is "very, very strong on privacy."

However, privacy advocates are concerned that data CBP collects could be improperly shared — willingly or unwillingly — with outside sources.

A privacy audit from [DHS's Office of the Inspector General](#) from last year cast doubt on how well some data collected from UAS drones is being protected. The report found that CBP had "not ensured safeguards" around the privacy of photos and videos of individuals at the border. The report concluded that this information is "at increased risk of compromise by trusted insiders and external sources" due to "security deficiencies."

Guliani said that, ideally, Congress would pass clear legislation on how new surveillance technology should be used at the border, but so far, that hasn't happened.



A US Border Patrol agent watches over the US-Mexico border in Nogales, Arizona, on July 22, 2018.

*John Moore/Getty Images*

### **It may not solve the problem, but at least politicians agree on it**

Many academics in the field see a border wall as a distraction from the systemic issues at hand. They point out that one of Border Patrol's chief concerns, drug smuggling, primarily happens by cartels hiding narcotics in cargo vehicles going through established checkpoints, not through rugged terrain in isolated areas where transport is more difficult.

According to US Customs and Border Protection statistics, [between 80 and 90 percent of narcotics](#) such as heroin, cocaine, methamphetamine, and fentanyl seized across the border in the first 11 months of the 2018 fiscal year was caught at legal points of entry, a.k.a. official crossings.

These experts also say that, as with a physical wall, tech alone won't address the underlying causes of mass immigration or drug smuggling. No matter how sophisticated the technology is, they say, there are always workarounds such as bribes and tunnels.

"In the end, there are many studies that show that walls don't work where the demand to get past them is very strong," said Guadalupe Correa-Cabrera, a professor of policy and government at George Mason University. "Whether digital or physical, walls are always porous."

Nevertheless, some proponents of the smart wall acknowledge that deeper immigration issues — like the humanitarian crisis causing refugees to flee countries like Guatemala en masse — won't be solved by new tech. But politicians like Tester view smart-wall funding as a rare part of the immigration issue where there's a beacon of hope for bipartisan agreements.

"There are some folks on the Republican side of the aisle who are willing to talk about what the facts are — and the fact is that it's not the best use of our funds to spend on a physical wall," said Tester. "I hear Republicans and Democrats alike telling me, 'A smart wall is the way to go.'"



A toy is seen from Piedras Negras, Mexico, on the border fence as members of the US Border Police guard the international bridge in Texas, on February 6, 2019.

*Julio Cesar/AFP/Getty Images*

**Correction:** A previous version of this article misstated Palmer Luckey's title at Anduril Industries.

**Update 2/07/2020:** Additional reporting included on federal agencies purchasing cellphone location data for immigration enforcement.

---

*Recode and Vox have joined forces to uncover and explain how our digital world is changing — and changing us. Subscribe to [Recode podcasts](#) to hear Kara Swisher and Peter Kafka lead the tough conversations the technology industry needs today.*