SECURITY SYSTEMS NEWS
THE NEWSPAPER OF RECORD FOR THE SECURITY SYSTEM INTEGRATOR & INSTALLER

AI within security: Is it fully realized yet?

The capabilities of AI have increased exponentially in the last few years, and government and industry alike are taking notice. What does this mean for the security industry?

by: Lilly Chapa

WASHINGTON—Back in early 2017, an unlikely leader emerged in the global artificial intelligence enterprise: Canada. The country announced the establishment of a national artificial intelligence strategy and pledged close to $1 million to developing talent and research communities geared toward AI. Following Canada's declaration, 18 countries followed suit—including China, Russia, and Mexico—each issuing their own unique national approach to AI. The United States is the most recent country to join that list after President Trump signed an executive order in mid-February instructing the U.S. government to prioritize artificial intelligence research and spending. Following that announcement, the Pentagon released its own artificial intelligence strategy, which focuses on using AI on the battlefield.

The global AI race has spilled over into private industry and popular culture, sparking questions—and concerns—about what a future with intelligent machines might look like. Indeed, in a recent Security Systems News poll about potential security industry trends in 2019, the majority of responses pointed to the increased role of AI in security as a leading technology trend. The buzz around using artificial intelligence in physical security applications is nothing new to most practitioners—for years, flashy demos on trade show floors have sparked the imagination, while concerns about privacy violations or machines taking over jobs leave some skeptical.

In reality, though, AI is a new way of accomplishing what the security industry has been doing for years. In its artificial intelligence strategy summary, the Pentagon defines AI as the ability of machines to perform tasks that normally require human intelligence—for example, recognizing patterns, learning from experience, drawing conclusions, making predictions or taking action—whether digitally or as the smart software behind autonomous physical systems.

"AI, or machine learning, is kind of a universal perimeter monitoring application that we, the industry, have been trying to do for a long time," Evolv Technology CEO and founder Michael Ellenbogen told *Security Systems News*. "Up until now, if you set up your camera system in December, and then the leaves come out in March, every time the leaves blow the system would alert the guards that there's motion along the fence line. That's because of some of the fundamental limits of traditional computer vision approaches and computing hardware that the industry has been wrestling with for a while."

Ellenbogen said that neural networks—which recognize patterns and power machine learning—have been around for decades, but up until a few years ago the architecture, learning processes and computing horsepower were not enough to fulfil the potential of AI.

"The industry has been trying to train computers to identify targets, and this is a better way of training them," he said. "These brand-new techniques are truly breakthrough—now we're doing things that just weren't possible even a few years ago."

Ellenbogen described the rapid advances in AI as if a switch were thrown three or four years ago—and believes that AI-powered security technology will be pervasive in the coming years.

"It's going to become not just accessible, but commonplace within the next two years," Ellenbogen said. "Anybody who's in the analytics business can't afford not to embrace machine learning and AI. By definition it's coming, and the differences in performance are so significant that if I don't embrace these modern techniques, I'm just going to get left behind."

The same type of machine learning techniques that are used to tell the difference between the movement of a tree's leaves and an intruder can now identify the threats people carry—and ignore innocuous items that may have been flagged in the past. Organizations like Ellenbogen's develop AI-boosted technology for soft-target locations such as stadiums, airports and government buildings. One of Evolv's solutions, for example, processes the data of what people carry when they walk through millimeter wave scanners and alerts for weapons but ignores cell phones and belts.

There are many misconceptions about artificial intelligence, especially when it comes to security applications. Ellenbogen acknowledged that there's a lot of buzz around the concept, and said he prefers using the term "machine learning," which falls short of the AI premise of machines teaching themselves tasks they have never been given.

One common concern is about computers replacing people in the security industry. Ellenbogen said he believes it's unlikely the human element will ever be completely removed from security. Instead, AI will enable the human IQ—what machine learning can't yet replicate—to focus on unusual or complicated situations. In fact, by using machine learning to conduct an initial screen, security officers can avoid alarm fatigue and remain more alert.

The Department of Defense took such a stance in its artificial intelligence strategy report, noting that one key tenet of AI is its ability to reduce inefficiencies from laborious, data-centric tasks.

"These changes have the potential to shift human attention to higher-level reasoning and judgment, which remain areas in which the human role is critical," according to the report. "Examples include improving situational awareness and decision making, increasing the safety of operating equipment, implementing predictive maintenance and supply and streamlining business processes."

Ellenbogen agreed, noting that automated alarming systems are rendered ineffective if they go off too often, causing people to ignore them or turn them off.

"If you look at the way guards work as people walk through a metal detector at a stadium, everyone is holding up their phones above their heads as a typical way of coming through, so everybody is beeping through the detector," he said. "The guards are looking up and confirming that, 'oh yeah, it's the phone.' It's becoming too easy to show the guard what they're expecting to alarm—it's only my phone or watch or belt, and meanwhile I've got a gun on my hip."

As for concerns about facial recognition and privacy, while machine learning has exponentially increased the capabilities and accuracy of facial recognition, Ellenbogen said he believes there's great value in combining identity with detection—while keeping a person's identity separate from their appearance.

This could come into play, for example, at venues that have a list of people banned from entering, which is typically enforced by showing security guards pictures of who to look out for.

"There's a bad combination of the fact that humans are just bad at remembering faces from pictures, especially if it's more than two or three people, not to mention the extremely high turnover rate in the guard force, so you're constantly worried about keeping people up to date, and you can't have enough labor to watch everyone coming in and out of a facility," Ellenbogen said. "In these instances, face recognition is not trying to determine people's identities, but instead is saying, is this anyone on the watch list, yes or no?"

Another concern with machine learning technology is that it will eventually realize its full potential—a computer that can grow and change on its own, without human input. Ellenbogen explained that AI-based security solutions don't work like a smart thermostat, for example, which will learn an occupant's behavior patterns and adjust the home's temperature based on that information.

"All the training happens back at headquarters—we don't allow the systems to update themselves on the fly," Ellenbogen said. "The systems collect data, our scientists and software people analyze and process it and update the algorithms, we verify that the changes will give us better performance, and then we upgrade our systems."

That's not to say that machine learning technology won't be used to combine facial recognition and unique identification, or that the evolution of AI will always be checked and approved by humans. The ethics of machine learning will be an important aspect of using the technology, whether in the security industry beyond.

The Pentagon made clear in its report that developing AI best practices is paramount to its success. "We will also seek to develop and use AI technologies in ways that advance security, peace and stability in the long run," the report noted. "We will lead in the responsible use and development of AI by articulating our vision and guiding principles for using AI in a lawful and ethical manner."

Ellenbogen agreed, noting that it is up to the security industry to understand—and respect—appropriate uses of artificial intelligence.

"I think that's where people get concerned about AI—the idea you have something that could be autonomously changing," he said. "That's absolutely not the case, and is certainly something that, as a security technology provider, we feel very strongly is not the appropriate way to use the technology."

Lilly Chapa is a contributing writer to Security Systems News.