AI, ML AND DEEP LEARNING IN SECURITY: THE FOREST VERSUS THE TREES

Rick Bentley, CEO and Founder of Cloudastructure examines how security systems get smarter and more sophisticated every year

Nowadays, there is a lot of new jargon being thrown around: artificial intelligence (AI), computer vision, machine learning, neural networks and now deep learning. Everything from your spellchecker to the stock market is using one or more of these new technologies, so we should expect security providers to use them too. Understanding the differences between each term can help us delineate between what is real and what is just fancy marketing.

What is AI?

Let's start with AI; it's essentially an umbrella term for any machine that an engineer has allocated with some ability to "think". A basic form of AI is the lowly thermostat from the last century, which has exactly two intelligent thoughts:

1. It is not warm enough in here, I'm going to turn on the heat
2. It is warm enough in here, I'm going to turn off the heat

There have been great advances in AI since the creation of the thermostat. Let's look at some of these newer terms.

Computer vision

One of the newer forms of AI – and one of the most relevant ones to a security professional – is computer vision. This gives a computer the ability to "see". Does that mean a computer really has eyes and sees the way we do? No. The computer has simply been trained to recognize the data patterns in photos and videos and classify them: people, cars, animals, etc.

Less than 10 years ago almost all computer vision was artisanal, meaning it was more art than science. If you wanted a computer to look at a camera and detect cars, you had to explain to a computer what a car looked like first, which is easier said than done.

As you can imagine, this kind of training with the computer did a poor job at detecting cars, until machine learning.

Machine learning

With machine learning, the engineer can give a computer 10,000 pictures of cars and 50,000 pictures of objects other than cars (boats, people, buildings, mailboxes, etc.) and tell it to sort it out on its own.

> **"THERE IS NO HARD AND FAST DEFINITION OF "DEEP" IN A NEURAL NETWORK, EVEN JUST THREE LAYERS MIGHT COUNT."**

Suddenly, the computer can do a better job of detecting cars than it ever could have with an engineer trying to describe them.

How does machine learning work? There are a lot of things involved, including vector calculus, tensors and more, but we will take on what is probably the most important and most relatable of them all: neural networks, as they are the most relevant to deep learning. The bottom line is that you can give the computer inputs, like a picture of a car and it comes up with an output, like "that's a car".

Neural networks

Scientists were inspired by the biological neural networks that constitute animal brains. Artificial neural networks loosely mimic the same approach as the brain does: our brain consists of billions of neurons, connected by synapses. Neurons generate signals that are transmitted to other neurons, changed and transmitted further. In between the input – you are shown a car – and the output – you say "that's a car" – there are many layers in the neural network in your brain.

We train our neural networks by passing a lot of information to them, then the neural network understands how to classify objects and can recognize objects of the same class even if they were not present in the training dataset.

Once you've seen enough cars, you know what cars look like. You can tell the next car you see is a car, even if you haven't seen that make and model before.

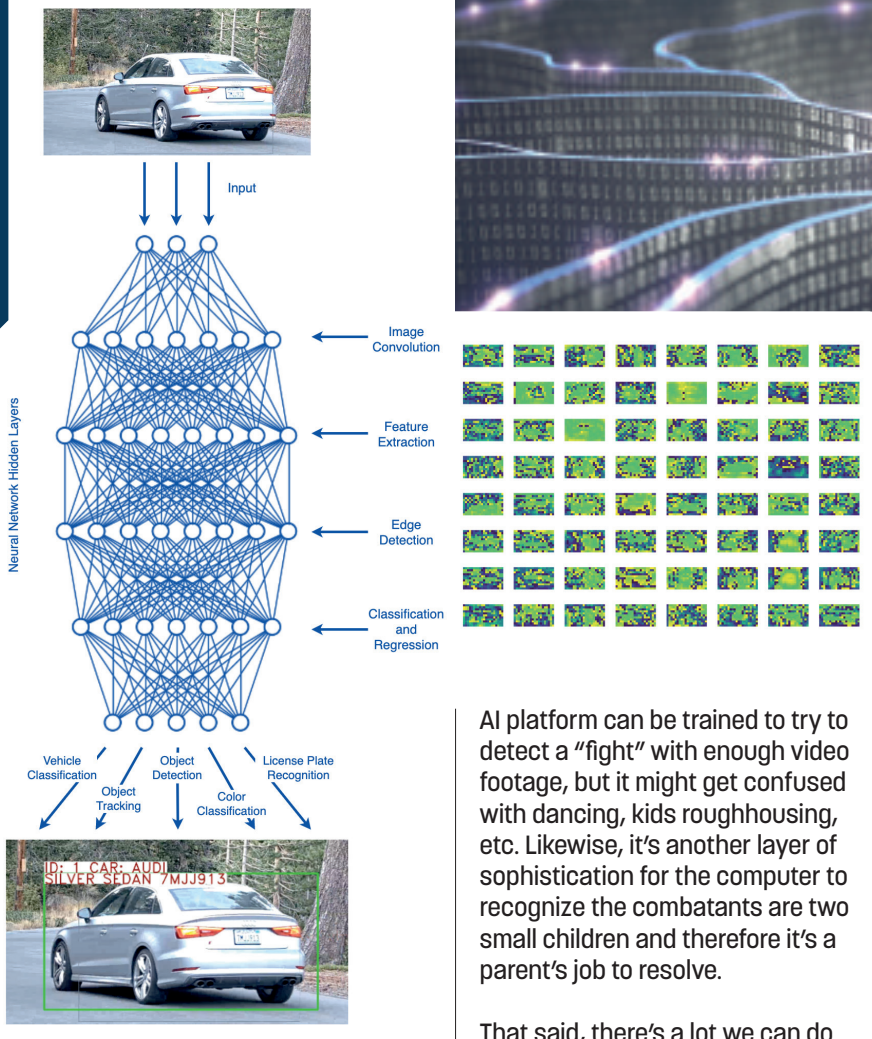
Today's artificial neural networks are not nearly as complicated as a human brain. However, machine learning has proven to work better than trying to explain things to a computer.

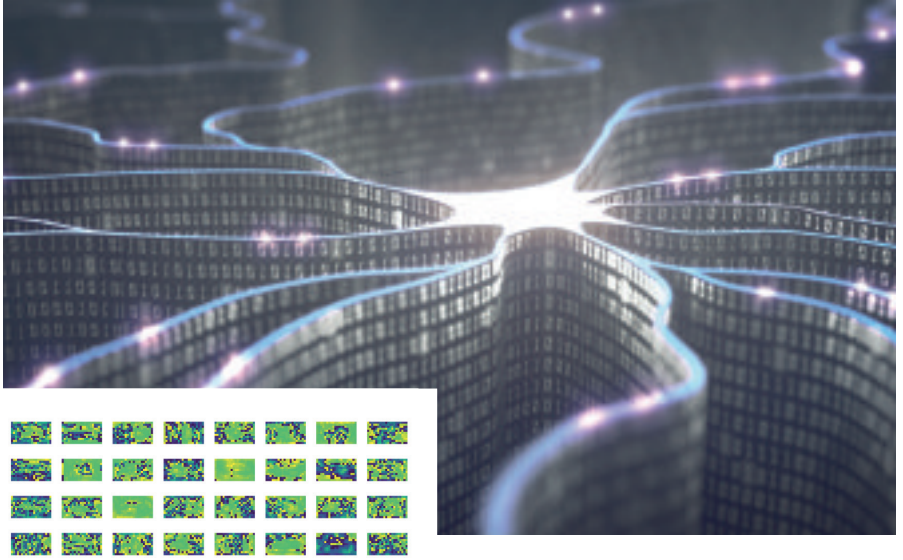
The value for a security professional is obvious: if a surveillance system transmits images to an AI platform with machine learning, these neural networks can now recognize a specific car, person or anomaly on their property, all without having to hire a team of guards to stare at empty parking lots or office hallways, waiting for an event to occur. Unlike a team of guards, the system never blinks, never gets tired or distracted.

Deep learning

Deep learning is when you have enough layers in your neural network that you can call it "deep". At some point, making them deeper doesn't help, but still costs more in terms of computations.

Here's an analogy: is an 8' pool in your backyard a "deep" pool? Your realtor is going to say so, as compared to most pools. The fact that it's a little deeper has some value to buyers. Does that mean if you put in an 80' deep pool that you will see an even greater return? Highly unlikely. ▸





There is no hard and fast definition of "deep" in a neural network, even just three layers might count. So, anyone who says authoritatively that they are selling "deep learning" is probably from the company's marketing department.

> **"WITH REMOTE GUARDING, OTHERWISE KNOWN AS LIVE MONITORING, WE CAN SMOOTHLY TRANSITION FROM AI TO HUMAN INTELLIGENCE."**

Looking ahead

AI still has a lot of growing up to do. By way of example, consider a fight in the parking lot. Today, an AI platform can be trained to try to detect a "fight" with enough video footage, but it might get confused with dancing, kids roughhousing, etc. Likewise, it's another layer of sophistication for the computer to recognize the combatants are two small children and therefore it's a parent's job to resolve.

That said, there's a lot we can do with the AI we have right now: we can set alerts to bad actors so you know when they enter your property, license plate detection so you can identify the culprits destroying your property, alerts to anomalies such as a mob gathering before it gets out of control. All in real-time. We also have something better than handing the reins entirely over to a machine: remote guarding.

With remote guarding, otherwise known as live monitoring, we can smoothly transition from AI to human intelligence: a guard can receive an alert of someone at the front door after hours and distinguish between someone fumbling for their keys and using a crowbar to open the door. Using IP speakers, the guard can then talk through the speaker to the person with the crowbar, let them know they are on video surveillance and that police/security has been called.

Assuming they attempt to run, a human can track them from camera to camera, capture what they look like, what make and model of car they're climbing into, capture the license plate and add their face to the bad actor list so an alert will go out if they return. That's why remote guarding has up to a 93% deterrence rate and up to a 95% apprehension rate. It can also save up to 40% on a company's guard costs, as well as reduce liability and losses.

Deep learning or not, AI that supports remote guarding is a moon landing ahead of the largely forensic measure surveillance was for the previous 30 years. It moves video surveillance from "let's see what caused all that damage last night" to preventing the damage from occurring in the first place. That's not jargon. ■

Rick Bentley

Rick Bentley is the Founder and CEO of Cloudastructure, an AI surveillance company. A longtime Silicon Valley engineer and CEO, Rick founded Televoke Inc, in 1998, where he personally raised eight figures of venture capital from VCs including Softbank and WI Harper. The company was then later acquired by Uber. He spent much of 2015 as a full-time Advisor to Google X, directly reporting to Andy Grove (CEO of Intel and the "Father of OKRs") for five years. He was also at General Magic, Machina, Sensory and various consulting jobs, including two tours of Baghdad with USAID.

cloudastructure

Cloudastructure

Winner of EIGHT Homeland Security 2022 Astor Awards

FOR CLOUD-BASED AI SURVEILLANCE AND A SAFER TOMORROW

ASTORS AMERICAN SECURITY TODAY 2022 PLATINUM AWARD WINNER
HOMELAND SECURITY AWARDS

BEST Video Surveillance Solution

ASTORS AMERICAN SECURITY TODAY 2022 GOLD AWARD WINNER
HOMELAND SECURITY AWARDS

BEST Video Analytics Solution

ASTORS AMERICAN SECURITY TODAY 2022 PLATINUM AWARD WINNER
HOMELAND SECURITY AWARDS

BEST Video Management

ASTORS AMERICAN SECURITY TODAY 2022 GOLD AWARD WINNER
HOMELAND SECURITY AWARDS

BEST Video Data Storage Solution

ASTORS AMERICAN SECURITY TODAY 2022 PLATINUM AWARD WINNER
HOMELAND SECURITY AWARDS

BEST Cloud IoT Cyber Security Solution

ASTORS AMERICAN SECURITY TODAY 2022 BRONZE AWARD WINNER
HOMELAND SECURITY AWARDS

BEST Cyber Critical Infrastructure Solution

ASTORS AMERICAN SECURITY TODAY 2022 GOLD AWARD WINNER
HOMELAND SECURITY AWARDS

BEST Cloud Computing

ASTORS AMERICAN SECURITY TODAY 2022 PLATINUM AWARD WINNER
HOMELAND SECURITY AWARDS

BEST IoT Product of the Year

ABOUT THE ASTORS AWARDS

As the preeminent U.S. Homeland Security Awards Program, the Annual 'ASTORS' Awards Program is specifically designed to honor distinguished government and vendor solutions that deliver enhanced value, benefit, and intelligence to end users in a variety of government, homeland security, enterprise, and public safety vertical markets. "'ASTORS' nominees are evaluated on their technical innovation, interoperability, specific impact within the category, overall impact to the industry, relatability to other industry technologies, and application feasibility outside of the industry."

Learn more at **www.cloudastructure.com**