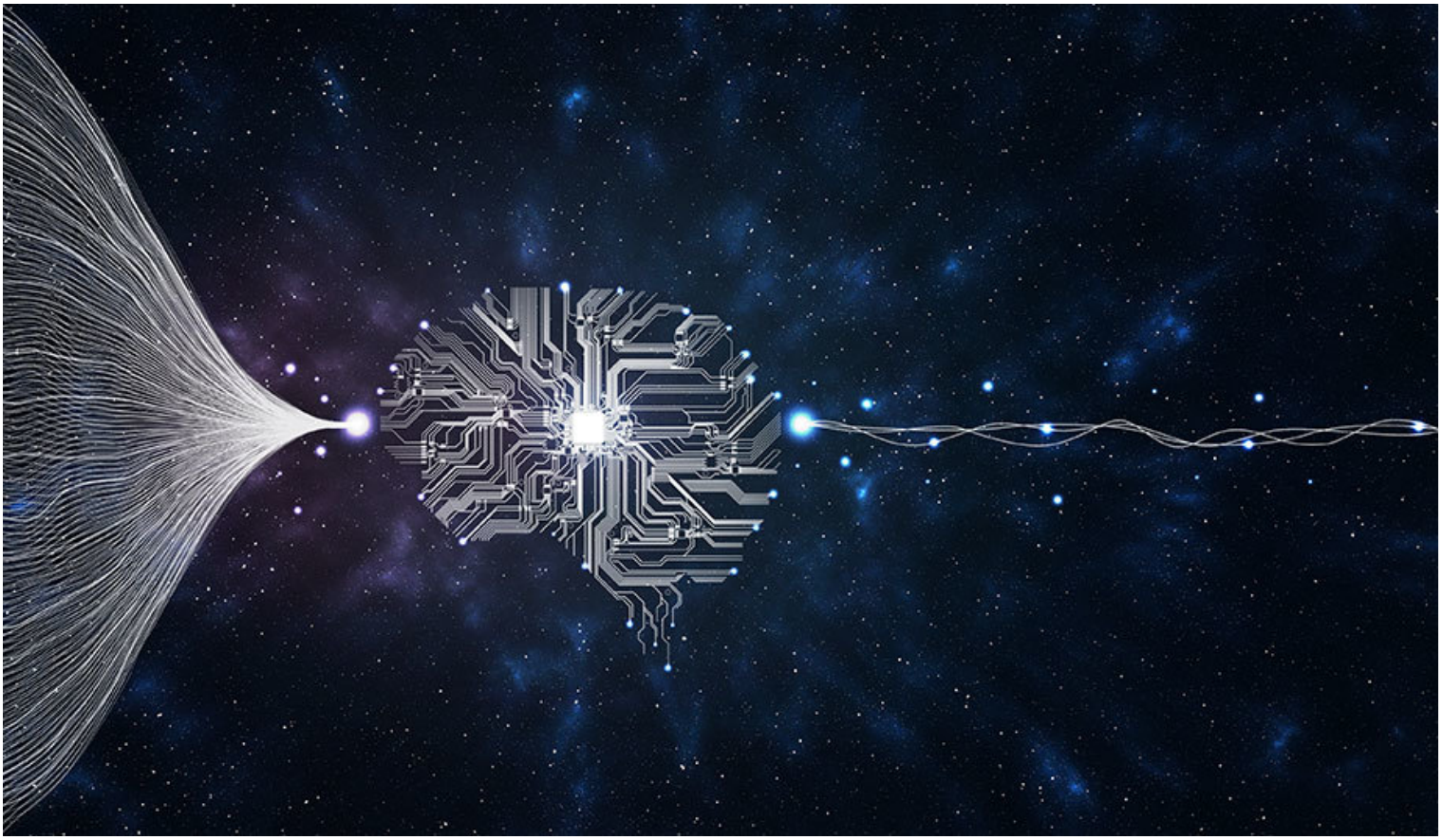
The basics of Artificial Intelligence and deep learning in physical security

Published on 30 Jan 2019



AI Is currently a buzzword in the physical security industry, and it is also a force that has the potential to transform the industry. Following are the basics of AI (and the related term “deep learning") in part one of our AI series.

Artificial intelligence (AI) is the broad computing category referring to intelligence that is displayed by a machine, as opposed to a living creature. Informally, AI refers to machines that mimic the cognitive functions we associate with living creatures, such as learning and problem-solving.

Trends driving growth in AI

Three trends in the computer industry are driving rapid growth in artificial intelligence. The trends are:

Data capture form to appear here!

> Video surveillance data makes up 60 percent of Big Data, and the amount is rising 20 percent annually

Emergence of computer hardware capable of solving complex calculations, specifically graphics processing units (GPUs, which use “parallel processing” instead of “serial processing” used by familiar central processing units [CPUs]). Multiple computations are carried out simultaneously, in parallel rather than in a series. It’s a more scalable approach: Large problems are divided into lots of smaller problems that can be solved at the same time.

Development of programming approaches to “train” systems more effectively, specifically neural networks, which work in conjunction with the parallel processing of GPUs. A neural network is a computing system made up of numerous simple, highly interconnected processing elements, typically organised in layers, with each layer made up of interconnected nodes. As each layer computes a result, that result determines the input for the next layer. There may be more than a hundred layers, which enables processing of large amounts of data into complex classifications.

A proliferation of sensors (including video cameras) that produce a large enough mass of data to enable systems to be “trained” effectively (a.k.a., “Big Data”). The proliferation of “Big Data” ensures there is plenty of data for training. Video surveillance data makes up 60 percent of Big Data, and the amount is rising 20 percent annually. This proliferation of data feeds artificial intelligence and increases capabilities for a range of systems.

Training of an AI-powered system

In a neural network operating on a GPU, learning rules modify the weights (importance) of

connections; each layer has a different “weighting” that reflects on what was learned at the previous layer. When presented with a data pattern (such as a video image), the neural network analyses what the pattern might be.

Training involves determining how far the initial answer is from the actual one and making appropriate adjustment in the connection weights. In highly simplified terms, that’s how the system “learns.” There are multiple stages of classification, almost like filters, with each guiding the path to a correct analysis.

Deep learning is part of a broader family of machine learning methods and the concept that is most relevant to the video market. Deep learning involves use of large amounts of data (for example, video images) from which the system can “learn” in a neural network.

Deep learning in video surveillance systems

> By being exposed to many instances of data, deep learning systems discern patterns and begin to generalise

The interconnected processing elements of a neural network, working in parallel on a graphics processing unit (GPU) to solve a problem, are designed to mimic the human brain and its billions of interconnected neurons. This aspect of artificial intelligence, known as deep learning, is the basis for a new family of video surveillance systems offering superior performance to historic systems.

This approach is poised to transform the effectiveness of video surveillance systems. Historically, computers have been programmed using video analytics algorithms. In contrast, deep learning systems are “trained.” If you want to identify a cat, you provide lots of images of cats, data which the system breaks down into smaller components and looks for commonalities. It then “learns” the common characteristics among the examples.

To maximise training, the more data a system is presented, the more refined it becomes – i.e., the more it “learns.” By being exposed to many instances of data, deep learning systems discern

patterns and begin to generalise.

From training to inference

> Deep learning can achieve super-human pattern recognition accuracy, resist interference, and classify and recognise thousands of features

While a computer programmer might spend months writing instructions to tell a computer what a car looks like, a neural network can “learn” by being exposed to many examples – no additional programming involved. But training a neural network is also time-consuming; it might take hours or days to complete. Training is also computationally intensive.

However, once a neural network has been trained, it can be used to “infer,” for example, to decide whether a new image is a cat. Inference is less computationally intensive, which enables deployment of trained systems on devices such as network video recorders (NVRs) or even in video cameras at the network edge.

Deep learning can achieve super-human pattern recognition accuracy, resist interference, and classify and recognise thousands of features. Those qualities make it especially useful for video analytics applications.

Part two coming soon.

Author Profile

Larry Anderson

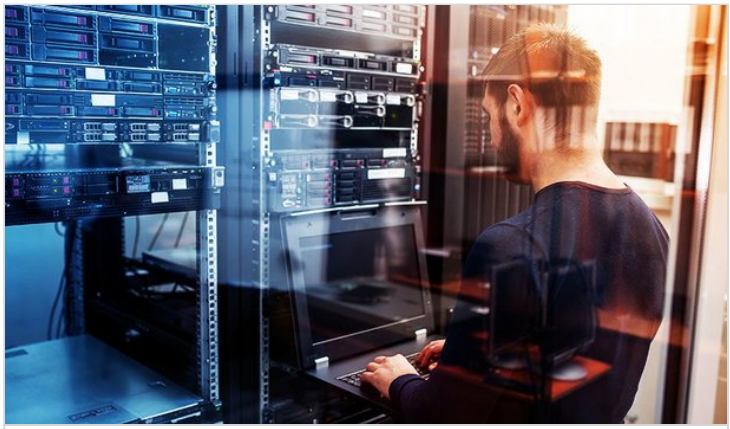
Editor, SecurityInformed.com & SourceSecurity.com

An experienced journalist and long-time presence in the US security industry, Larry is SourceSecurity.com's eyes and ears in the fast-changing security marketplace, attending industry and corporate events, interviewing security leaders and contributing original editorial content to the site. He leads SourceSecurity.com's team of dedicated editorial and content professionals, guiding the "editorial roadmap" to ensure the site provides the most relevant content for security professionals.

You may also be interested in...

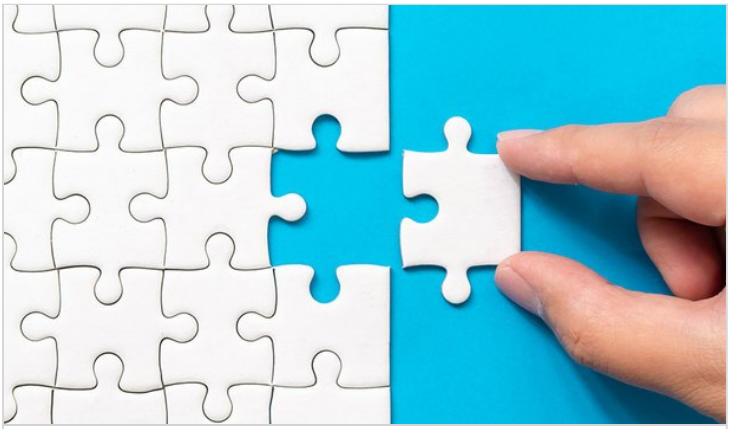
Is the physical security industry doing enough to prevent school shoot...

School shootings continue, as does a search for answers. What solutions are there to prevent school shootings and/or to improve the response...



Adapting servers for IP video surveillance systems: Why manufacturers...

Security integrators are often tasked with a multitude of responsibilities which could include a variety of installation, integration or des...



A busy year: rapid mergers & acquisitions suggests more to come in 201...

A rapid string of merger and acquisition (M&A) transactions as 2018 passed into 2019 suggests the physical security industry may be on t...

U.S. partial government shutdown: what's the impact on the physical se...

Security is arguably at the heart of the United States partial government shutdown: President Trump’s demand for $5.6 billion to start...