

VIDEO SURVEILLANCE | VIDEO ANALYTICS | REAL WORDS OR BUZZWORDS?: ARTIFICIAL INTELLIGENCE, MACHINE LEARNING AND DEEP LEARNING

Real Words or Buzzwords?: Artificial Intelligence, Machine Learning and Deep Learning

Examining the differences in these technologies and their respective benefits for the security industry

RAY BERNARD, PSP, CHS-III SEPTEMBER 24, 2019

ARTIFICIAL INTELLIGENCE



SecurityInfoWatch.com contributor Ray Bernard examines the differences between Artificial Intelligence (AI), Machine Learning (ML) and Deep Learning (DL) technologies and discusses how they're being leveraged in security applications today in his latest 'Real Words or Buzzwords?' column.

Editor's notes: This is the 45th article in the "Real Words or Buzzwords?" series from SecurityInfoWatch.com contributor Ray Bernard about how real words can become empty words and stifle technology progress.

At the ASIS GSX 2019 event I participated in a panel session titled, "How IoT, the Cloud and AI Deliver Business Intelligence." The video/audio recordings will be available online from ASIS in a few weeks. I have been holding off on writing about artificial intelligence (AI),



artificial intelligence (AI) and deep learning (ML,) which are the subjects of this article, because offerings powered by AI technologies were newly emerging and the related vendor vocabularies were still evolving.

However, the #1 question for our panel session was, “What’s the difference between AI, machine learning and deep learning?” Nearly all of the attendees nodded their heads to indicate their strong interest in the question.

I’m going to define the terms here and then provide references to well-written articles that will let you delve as deeply as you like into the topics. Before presenting the definitions, you should know – and maybe you do already – that machine learning is a type of artificial intelligence, and deep learning is a type of machine learning and thus is also a type of artificial intelligence.

An Important Aspect of AI History

The history of the AI research goes like this:

- **Artificial Intelligence** – 1950’s to 1980’s and still ongoing
- - -> **Machine Learning** – 1980s to 2010s and still ongoing
- - -> - -> **Deep Learning** – 2010s to now and still ongoing

For decades the AI researchers weren’t getting the results they wanted, and eventually many of the leading AI scientists wondered if there was something wrong with their approaches to AI software. The actual issue was not the software, but the hardware capabilities they were using to design and run the software.

The hardware wasn’t capable of handling what the AI scientists wanted to do. This became obvious as now – thanks to the exponential advancement of computing technologies including hardware virtualization and cloud computing – we have hardware that is capable of supporting the kinds of software that can perform amazing amounts of processing tasks in parallel. That’s the story behind the story of the development of machine learning, and then its refinement into deep learning.

A lot of this story, and some very well-written explanations about the technology, are available on Nvidia’s company blog (links follow later in this article). Nvidia is one of the companies that makes the computer cards holding multiple high-speed parallel-processing computer chips that make the running of machine learning and deep learning software feasible.

Such processing involves the handling of massive amounts of data, and so today’s computer CPU chip designs include support for massive data throughout to and from the GPU (graphical processing unit) chips that Nvidia and others make. Initially they were developed for video gaming, because the video displays – especially for 3D games – had to be able to process the three-dimensional visual aspects of hundreds and thousands of objects on the display screen or video virtual reality headset. They also had to process all the computer



ual displays, such as is required to realistically bounce a ball across a floor. That's a lot of parallel processing power, and soon AI researchers found that they could use these chips to run various parts of their AI software in parallel.

That processing capability made such a great difference in AI results, that Nvidia, Dell and other chip makers began designing chips just to support the kind of software that AI scientists wanted to create. Somewhere along the line the scientists realized that their theories about what AI software could do were correct – they just needed hardware that could support the vast amounts of data processing required for their software.

Definitions

These topics involve incredibly complicated logistics and very complicated software design that goes far beyond the ways we're used to thinking. We can easily deal with two-dimensional and three-dimensional concepts because we live in a three-dimensional world that is often represented visually in two dimensions. What about data that's twelve-dimensional, where many dozens of tiny software programs are all exchanging data with each other at the same time? Now multiply that by a million or two, and you have computers performing data processing tasks that are literally mind-boggling for humans. Our discussion in this article is about mind-boggling technology – but we don't need to understand the mind-boggling parts. We just need an accurate description of that the AI software does, and how we can use it for security system applications. That's the scope of this article's discussion.

Artificial Intelligence is the computer performance of tasks that have been thought to require human intelligence. Such tasks are composed of processes like *learning* (getting not just information but also the rules for how to use the information), *reasoning* (using the rules to reach exact or approximate conclusions), and *self-correction* (for which software uses feedback loops that enable the software to evaluate the results of the reasoning that it applied).

Just like some people are smarter than other people, especially from one subject area to another, so some AI software is “smarter” than other AI software across various subject areas. While that's interesting, the most important question is whether or not the AI software can do what it is intended to do, with the data that it's intended to use. Can the AI software get the results we want it to?

Machine Learning involves using AI software to give systems the ability to automatically learn and then improve from experience, without the system having been specifically programmed for those improvements. Machine learning originally required structured data. An email is a piece of structured data – sender, recipient, subject, and message body – and even the message body can contain a structure such as salutation, message content, and signature. Thus, it was possible to feed machine learning software thousands of emails classified as spam emails and good emails, and give it rules about the various parts of the data structure, and train it (by feeding it example) to use those rules to tell the difference. That was how some types of spam filtering software came about.



type of machine learning that can go beyond structured data. It's designed using software called neural networks, which are pieces of software code (called nodes) that exchange data with each other in specific ways. Each node has its own data evaluation task to perform, and the outputs of those data evaluation tasks become inputs to other data evaluation tasks. It mimics the way that scientists think the human brain's nerve cells work (that's why it's called a neural network). Each group of software nodes that perform their processing in parallel is called a layer. Technically speaking, more than three layers of machine learning is called deep learning.

But how many layers of parallel processing there are is irrelevant to us, the security system designers, manufacturers and end users. What matters is the end result, and that result is in our security domain, not in the domain of data science and computer processing.

Getting Real About AI

The greatest immediate impact of AI for us is for video analysis, both in real time and in after-the-fact review and data extraction. The big advantage we have – that information technology folks working with business data AI systems don't have – is that video data is already visual. We don't have to convert the data into charts and graphs for visualization. So physical security systems AI-enabled products can be easily evaluated just by seeing if the results match the video images. This is one reason why AI-enabled security systems will be easier to adopt and have faster success than AI for business data.

We don't have to learn anything new to evaluate AI-enabled products or platforms, except what results they get.


However, the technology behind it is interesting – especially to those of us who deal directly with it – and so here are some links to broader and deeper discussions about AI, ML and DL technology:

- [What's the Difference Between Artificial Intelligence, Machine Learning, and Deep Learning?](#) This Nvidia blog article expands on the discussion above.
- [What's the Difference Between Deep Learning Training and Inference?](#) This Nvidia blog explains the technology that makes possible what I wrote about in my most recent Convergence Q&A column titled, "[The Move to Enable Proactive AI in Security Operations.](#)"

Future *Real Words or Buzzwords?* articles will discuss more aspects of AI, ML and DL as products using them continue to emerge.

About the Author:

*Ray Bernard, PSP CHS-III, is the principal consultant for Ray Bernard Consulting Services (RBCS), a firm that provides security consulting services for public and private facilities (www.go-rbcs.com). In 2018 IFSEC Global listed Ray as #12 in the world's Top 30 Security Thought Leaders. He is the author of the Elsevier book *Security Technology Convergence**

 *Special Contributor on Amazon. Mr. Bernard is a Subject Matter Expert Faculty of the Security Executive Council (SEC) and an active member of the ASIS International member councils for Physical Security and IT Security. Follow Ray on Twitter: [@RayBernardRBCS](#).*

Sign-up for the Security We

Delivered straight to your inbox, a weekly review and re

Email Address

First Name

Last Name

Title

Country

Join the conversation!

This site requires you to **login** or **register** to post a comment.

No comments have been added yet. Want to start the conversation?

