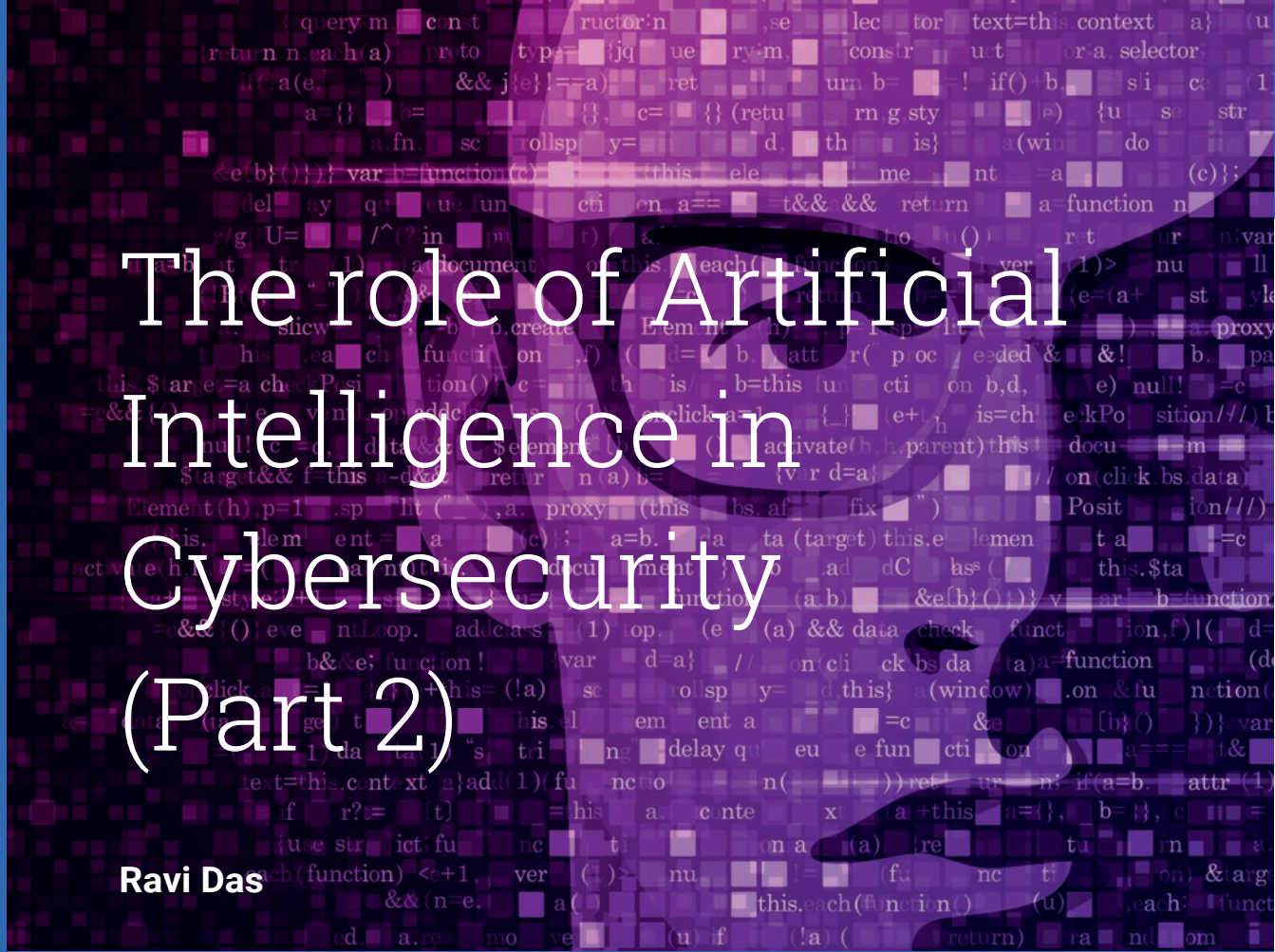
The role of Artificial Intelligence in cybersecurity (Part 2)

Ravi Das



The role of Artificial Intelligence in Cybersecurity (Part 2)

Ravi Das

Derived from many fields, AI systems vary in sophistication

The first part in this series provided a clear definition of what Artificial Intelligence (AI) is and an overview of its use in Cybersecurity. This article will explain the scientific origins of AI and unpack the various types and subspecialties of AI systems and their respective functions. Not all AI systems are created equal!

AI draws from several scientific fields

Believe it or not, the field of AI is actually a derivative of other fields, namely the following:

- Philosophy
- Logics and Mathematics
- Computational Algorithms
- Psychology and the Cognitive Sciences
- Neurosciences
- Evolution

For example, it is the logical structure of the mathematical algorithms that are used to "learn" from previous examples and apply those rules in making decisions about future decisions. And as for the neurosciences, AI tools also try to imitate, or mimic, the neuronic activity of the brain, especially in the way that neurons either fire or do not fire.

Artificial Intelligence (AI) can be divided into two main classifications, which are as follows:

AI systems vary in level of intelligence and functionality

Type 1: This consists of the following:

- Weak, or "Narrow" based Artificial Intelligence: In this scenario, the AI system is focused on just accomplishing one specific task or goal. This can be considered a very primitive form of AI, as it can only do very basic tasks, such as playing against a competitor in a basic Chess game. In this situation, all the rules and probable scenarios must be fed manually into the AI system before it can engage a true competitor. In other words, it cannot learn on its own; every time a new game is played, all the rules and outcomes must be fed into the AI system.

- Strong Artificial Intelligence: This is the kind of AI that is used most typically in Cybersecurity today. For example, based upon the data and intelligence that are fed into it, this kind of system can literally learn all on its own from past observations, and use that knowledge to make informed decisions for the future. In other words, every effort is made to emulate human thought and decision-making processes. The key differentiator here is that there is almost no human intervention needed with this type of AI systems; the only time human input is needed is when new information and data feeds need to be inserted.

Type 2: These kinds of AI systems are based upon the functionalities they possess, or are anticipated to possess, in the future. These systems include:

- Reactive Machines: These are considered the most rudimentary or basic form of an AI system, It is, in fact, more like a Type 1, as described above. This type of AI system has a very limited memory and can only store very limited amounts of information and data. Such systems cannot make future decisions or predictions on their own; some degree of human intervention is required.

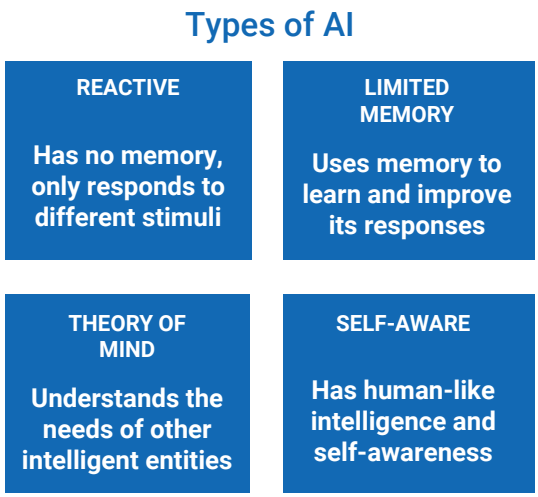
- Limited Memory: These are the AI systems that can "learn" from past examples and use those lessons to make decisions about future events. In fact, this is the classification that is most representative of AI systems that exist today, and which are currently used in the Cybersecurity industry.

- The Theory of the Mind: The main purpose of this kind of AI system is to embody "… emotion, belief, thoughts, expectations and be able to interact socially." (Source 1). Although Theory of the Mind has a very long way to go until it can even come remotely close to achieving the above, we are already seeing some very basic forms of this starting to take place. The best examples of this are the Virtual Personal Assistants such as Alexa, Siri, and Cortana. These kinds of applications try to learn our thought and decision-making profile so that recommendations and directions can be provided based upon previous actions.

- Self-Awareness: This is the ultimate goal of any AI system. Such a system would be very much like a

  live being and would even act like one. The best, most illustrative example of this is the character Data from the TV series, Star Trek: The Next Generation.

These classifications of Type 2 AI systems are illustrated below:



(Source 2)

Subspecialties of A1: Delving deeper

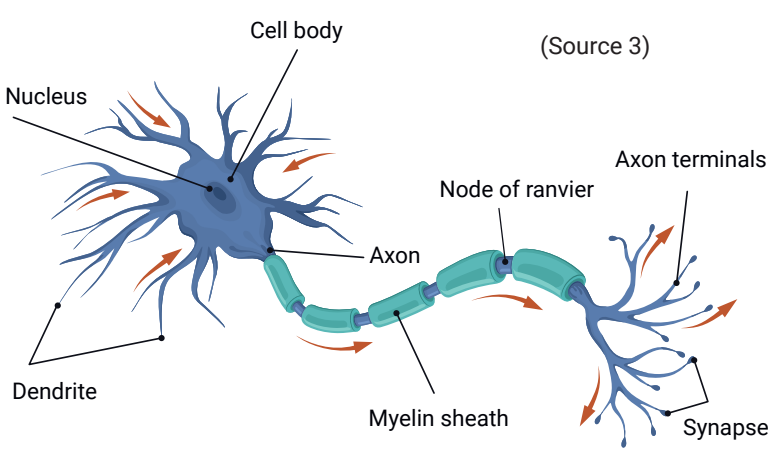
There are also many subspecialties from within AI, and these are as follows:

- Data Science: Today's Cybersecurity industry is experiencing a huge influx of information and data. It can take an entire IT Security staff days or even weeks to comb through all of this. Of course, this is an almost impossible task to be achieved. In this respect, AI can be viewed as the ultimate "Savior" when it comes to analyzing these huge datasets, also known as "Big Data". Within a matter of seconds, such an AI system will discover hard-to-detect and unseen trends and even recommend how they should be applied when modeling the Cyber Threat Landscape.

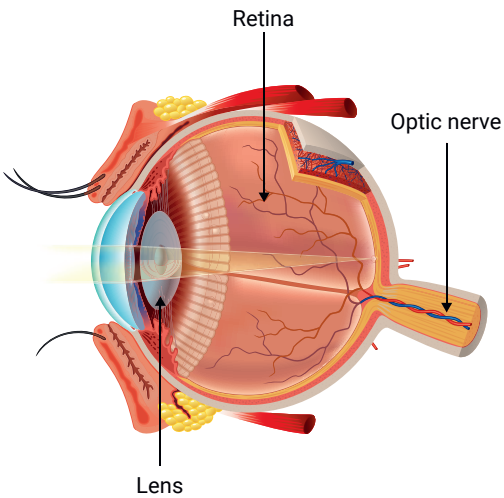
- Machine Learning (ML): This subspecialty can be considered as an extension of the above, but with the main difference being that super sophisticated mathematical algorithms are used to help the IT Security team classify, categorize, and even predict data extrapolations from any given dataset. These mathematical algorithms are actually coded into a specific programing language (such as that of Python) to help create and build an entire Machine Learning system. This is the one area of Artificial Intelligence that can be used to help filter through false positives and determine which are real or have enough merit to warrant further action.

- Neural Networks (NN): This is the area of AI that tries to mimic the central nervous system and the neurological functions of the human brain. It is the neuron that forms the basis of these two, and it can be defined specifically as follows:
  "The neuron is the basic working unit of the brain, a specialized cell designed to transmit information to other nerve cells, muscle, or gland cells. Neurons are cells within the nervous system that transmit information to other nerve cells, muscle, or gland cells. Most neurons have a cell body, an axon, and dendrites."
  (Source 3).
  In fact, it is estimated that the human brain has an average from 100 million to 100 billion neurons, all connected to one another. The primary goal of a Neural Network system is to map these interactions, and hard code them so they can be used for predictive behaviors, such as modeling the Cyber Threat Landscape. A typical neuron is illustrated below:

(Source 3)



- Image Processing: Without a doubt, every waking moment of our lives is spent in seeing objects. This visual information is captured by the eye and then transmitted to the brain via the optic nerve (which is the collection of blood vessels at the back of the eye), making vision possible. This is illustrated below:

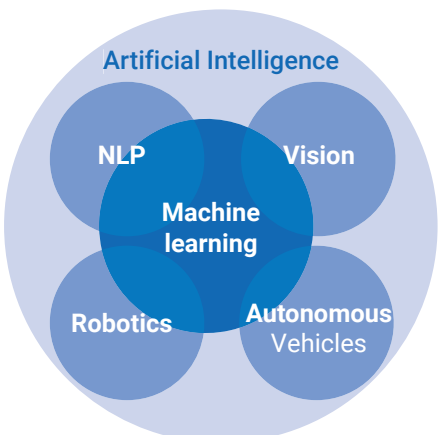


(Source 4)

Image processing in AI (also known a "computer vision") attempts to mimic visual processing in human beings. One of the best examples of how this application is being used is in Facial Recognition, a biometric technology that is often used in conjunction with CCTV Technology to confirm the identity of a particular individual. Incorporating Computer Vision into such a system makes greatly enhances the degree of accuracy and reliability.

- Robotics and Embedded Systems: Simply put, this is where AI tools are being created and deployed into robots. This kind of technology is most widely used in manufacturing, where it can perform very mundane and routine tasks on an automated basis with a high level of accuracy, and of course, at faster speeds.

The subspecialties of AI just described are illustrated in the diagram below:



(Source 5)

About the author: see page 41.

Part 3: The role of AI in Cybersecurity today

The use of AI in Cybersecurity is ever evolving, with future applications not yet tapped into. The next article in this series will provide an overview of the many ways AI is being used in Cybersecurity today.

Sources:
1. forbes.com/sites/cognitiveworld/2019/06/19/7-types-of-artificial-intelligence/#301ec3a6233e
2. brainfacts.org/brain-anatomy-and-function/anatomy/2012/the-neuron
3 .webspace.ship.edu/cgboer/theneuron.html
4 youtube.com/watch?v=YcedXDN6a88
5. medium.com/@chethankumargn/artificial-intelligence-definition-types-examples-technologies-962ea75c7b9b