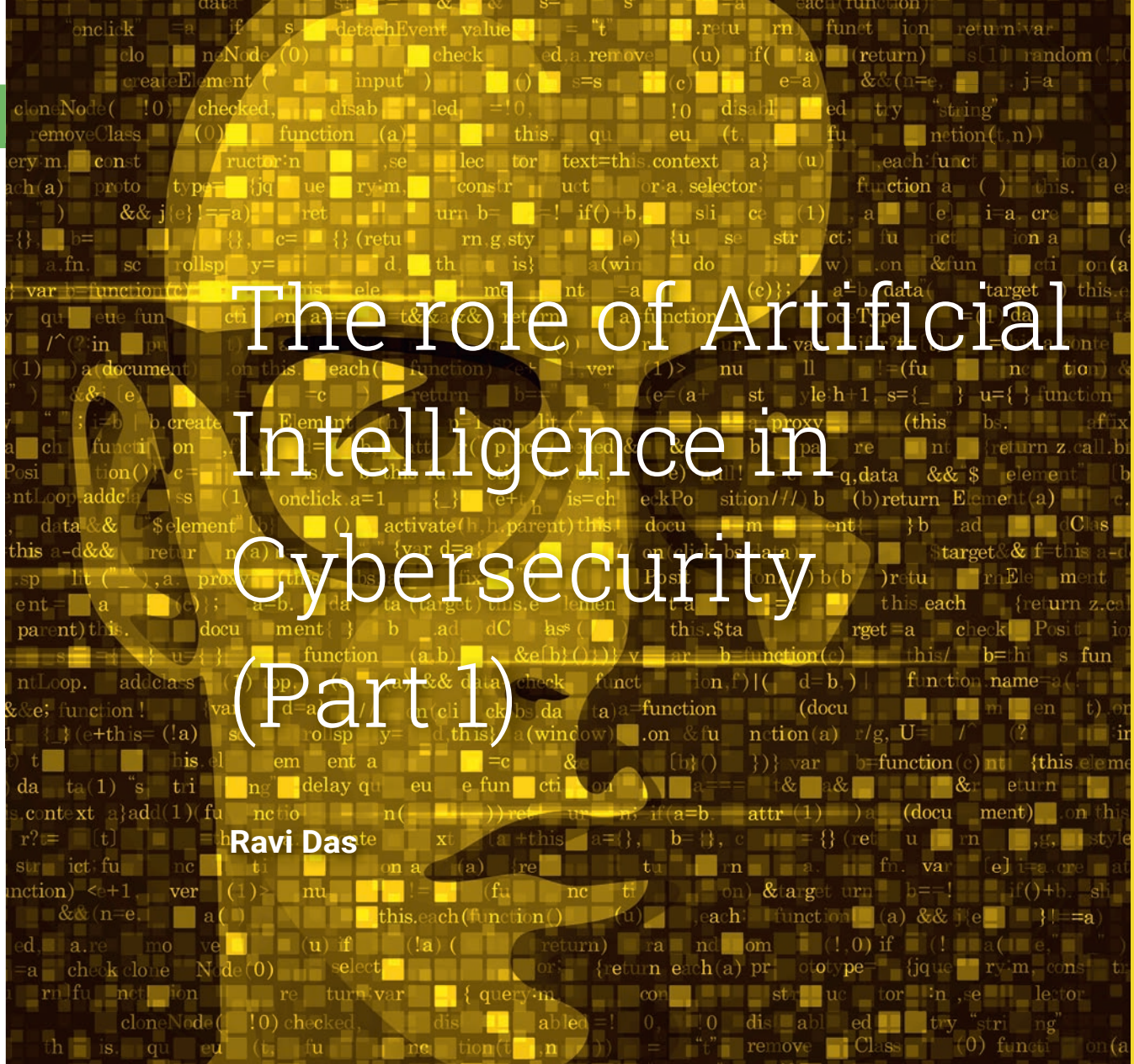

The role of Artificial Intelligence in Cybersecurity (Part 1)

Ravi Das

How an emerging technology can provide smart IT protection

One thing that Corporate America can be certain of in the future is that Cyberthreats and their attackers will abound, stealthier and more covert than ever. In other words, gone are the days of the so called "Smash and Grab" campaigns, where the goal of the Cyberattacker was to launch an all-out, brute force attack against a target and harvest whatever they could.

Today's Cyberattacker, however, is very deliberate and calculative in every move that they make. For example, they take their own time to deliberately study the profiles of their intended victims, and once the appropriate weak spot has been found, they make their move.

The role of Artificial Intelligence in Cybersecurity (Part 1)
Ravi Das

But Cyberattacker's goal is not to stay in for short periods of time but rather for long stretches, in an effort to steal as much as they can, in small amounts, so that the victim will not realize what is going on until it is too late.

In fact, many Cyberattacks like these often go unnoticed, evading all means of defensive protection that have been deployed by the business. So, is there a way that these threat vectors can be detected and mitigated before further damage occurs?

Yes, there is. The solution is the use of Artificial Intelligence (AI) tools. This kind of technology can virtually learn and detect just about any looming threat and alert the IT security staff so that proper re-mediative actions can be taken.

Artificial intelligence is still an emerging concept in Cybersecurity and is very broad in nature. This article will provide a general overview of this exciting technology.

What Is Artificial Intelligence?

The term "Artificial Intelligence" often conjures up an image of the human brain. To a large extent, this is a good graphical representation of what AI is. The basic idea is to mimic the thought and behavioral process of the human brain, to learn and apply these "experiences" towards discovering hidden trends and predicting the future. Specifically, artificial intelligence can be defined as follows:

"The term artificial intelligence (AI) refers to computing systems that perform tasks normally considered within the realm of human decision making. These software-driven systems and intelligent agents incorporate advanced data analytics and Big Data applications. AI systems leverage this knowledge repository to make decisions and take actions that approximate cognitive functions, including learning and problem solving."

Artificial intelligence (AI) also makes it possible for machines to learn from experience, adjust to new inputs and perform human-like tasks."

(Sources 1 and 2)

As one can see from the above definition, the potential that Artificial Intelligence has in Cybersecurity is enormous. For example, many of today's IT security teams use many kinds of tools from various kinds of vendors in order to beef up their lines of defense.

As a result, they are completely inundated with all sorts of information and data from all sources. Because of this, many false positive warnings and messages are created, putting an extra burden on the IT security team to filter through them.

But with the use of Artificial Intelligence, it can use the concepts of data warehousing

to instantaneously filter through all the warnings to determine which of them are truly indicative of an impending threat vector. In this regard, Artificial Intelligence has also started to make a splash as a task automation tool for both Penetration Testing and Threat Hunting Teams.

As a result, such teams can devote more time and attention to unearthing all unknown gaps and vulnerabilities that exist within an IT Infrastructure and provide timely solutions for the client on the remediative actions that they need to take.

The field of Artificial Intelligence is in desperate need of staff augmentation. At the present time, there is a severe worker shortage in the Cybersecurity industry, with some 3.5 million jobs that remain unfilled. (Source 3)

In this regard, AI tools can be used to help predict what the future Cyber Threat Landscape will look like, and even provide recommendations to the IT Security Staff as to how best prepare for it. Typically, this would be the role of a Cybersecurity Analyst, but until enough staff positions are filled, Artificial Intelligence will literally become the "virtual" version of that position.

The next article in this series (see part 2 on page 46) will dive deep into the origins and types of Artificial Intelligence, including the various fields that gave rise to it, as well as the subspecialties of AI.

Sources:
1) sas.com/en_us/insights/analytics/what-is-artificial-intelligence
2) datamation.com/artificial-intelligence/what-is-artificial-intelligence
3) cybersecurityventures.com/jobs/

ABOUT THE AUTHOR

Ravi Das is a Cybersecurity Consultant and Business Development Specialist. He also does Cybersecurity Consulting through his private practice, RaviDas Tech, Inc. He is also studying for his Certificate In Cybersecurity through the ISC2.