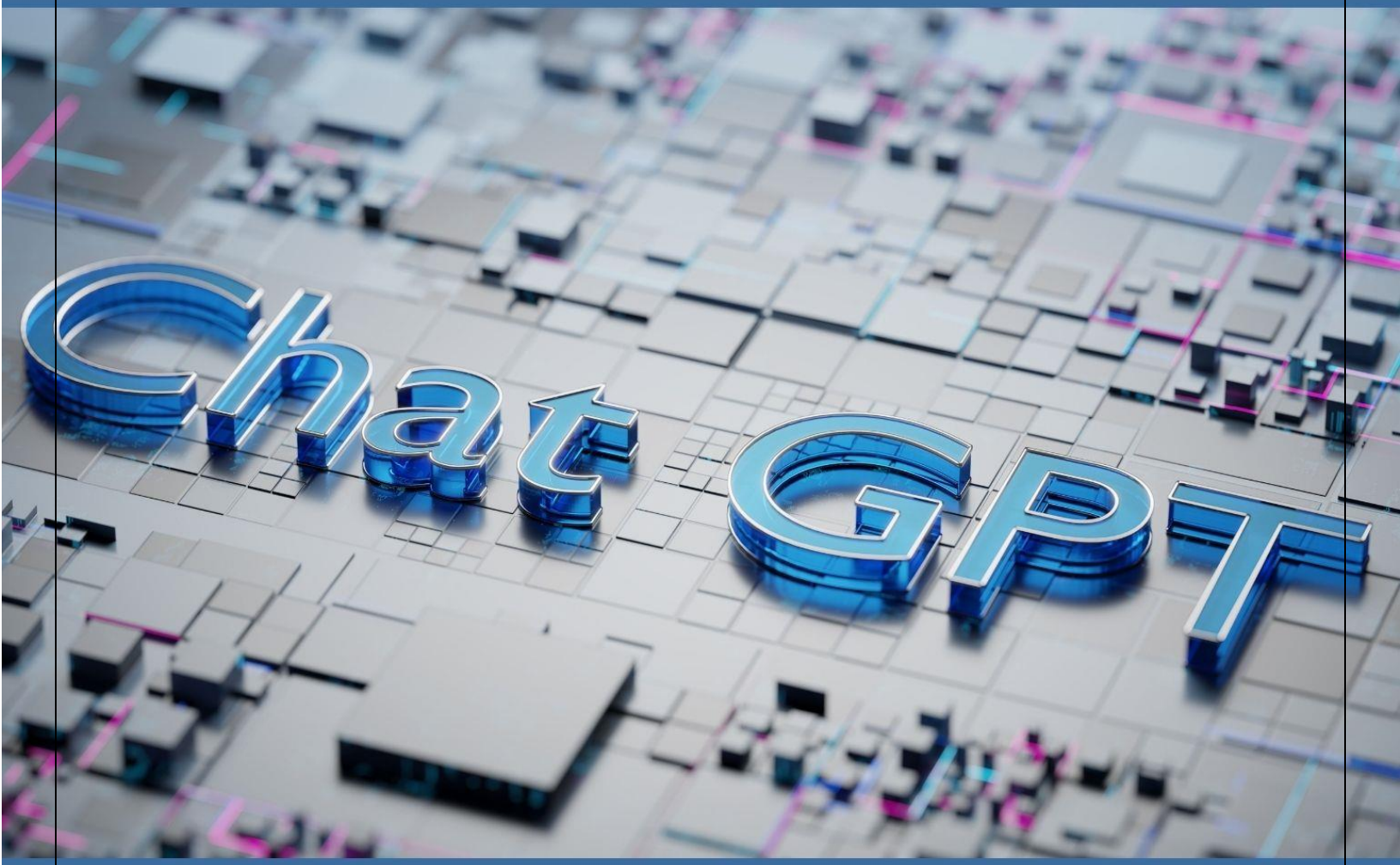
The Implications Of AI & ChatGPT



Written by Ravi Das for KAMIND IT, Inc.

The Implications Of AI & ChatGPT

Introduction

In a previous blog, we had introduced some of the concepts of what Artificial Intelligence (AI) is all about. Specifically, it covered the following topics:

- A definition of AI
- The components of AI

In this whitepaper, we do a much deeper dive into AI, focusing in on the following topics:

- A further review of the classifications in AI;
- The subspecialties in AI;
- The role of AI in Cybersecurity;
- The advances in AI - ChatGPT

A Further Review Of The Classifications In AI

In fact, Artificial Intelligence (AI) can be further subdivided into two main types of classification, which are as follows:

1) 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 to be a very primitive form of it, 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, each and every time that a new game is played, all the rules and outcomes have to be fed into it each and every time.

   - 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 feeds that are fed into it, this kind of system can literally learn all on its own from past observations, and use that knowledge in order to make informative decisions for the future. In other words, every effort is made so that it can emulate human thought and decision-making process as much as possible. The key differentiator here is that there is almost no human intervention needed for these kinds of AI systems; the only time this is really ever needed is if new information and data feeds have to be inserted.

2) Type 2:

   These kinds of Artificial Intelligence systems are based upon the functionalities that they possess or are anticipated to in the future. These include the following:

- Reactive Machines:

  This is considered to be the most rudimentary, or basic form of an AI system, and in fact is more like a Type 1, as just reviewed. In particular, their memory is very limited, and these kinds of systems can only store very limited amounts of information and data and cannot make future decisions or predictions on their own, without some sort of human intervention.

- Limited Memory:

  These are the Artificial Intelligence systems that can "learn" from past examples and use those to make decisions for future events. In fact, this is the classification that is more representative of AI systems that are in existence today, and that are used in the Cybersecurity Industry today.

- The Theory of the Mind:

  The main purpose of this kind of Artificial Intelligence system is to "... emotion, belief, thoughts, expectations and be able to interact socially."

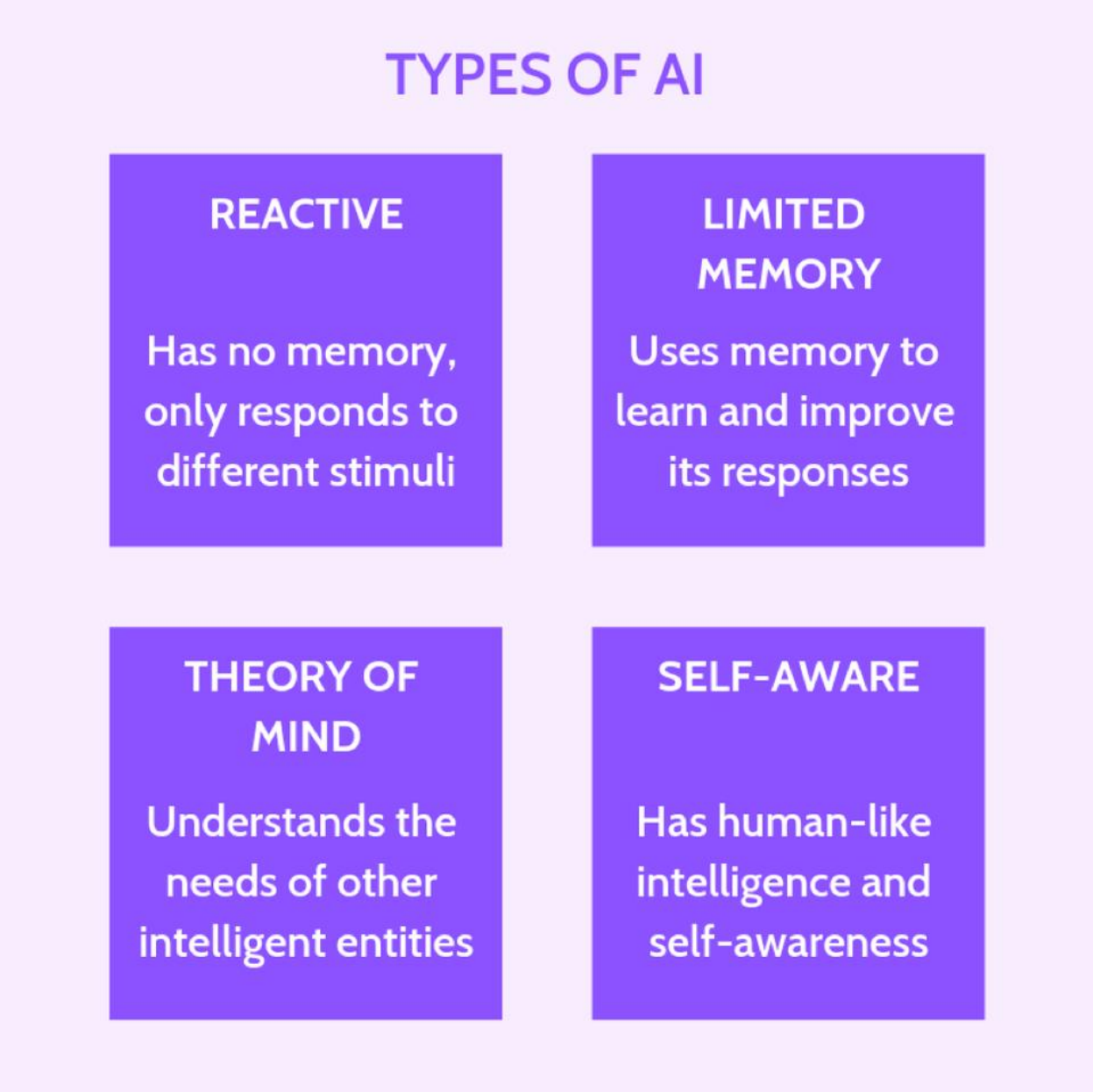
  (SOURCE: 4).

  Although this 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, namely those of 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 would be the ultimate goal of any Artificial Intelligence system. This entity would be very much like a being and even act like one. The best, illustrative example of this is the character Data from the TV series, "Star Trek: The Next Generation".

These two classifications are illustrated below:



(SOURCE: 1).

The Subspecialties In AI

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

1) Data Science:

   As mentioned, the Cybersecurity Industry at the present time, and going well into the foreseeable future, is experiencing a huge influx of information and data. It can take an entire IT Security staff literally days or even weeks in order to comb through all of this. Of course, we all know that this is simply an almost impossible task to be achieved. In this aspect, Artificial Intelligence can be viewed as the ultimate "Savior" when it comes to analyzing these huge

datasets, also known as “Big Data”. Within just a matter of seconds, hard to detect and unseen trends can be noticed very quickly, and recommendations can even be provided as to how they should be applied when modeling the Cyber Threat Landscape.

2) 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 to classify, put into specific categories, 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, for example) in order 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 those which are for real or have some merit to them to warrant further action.

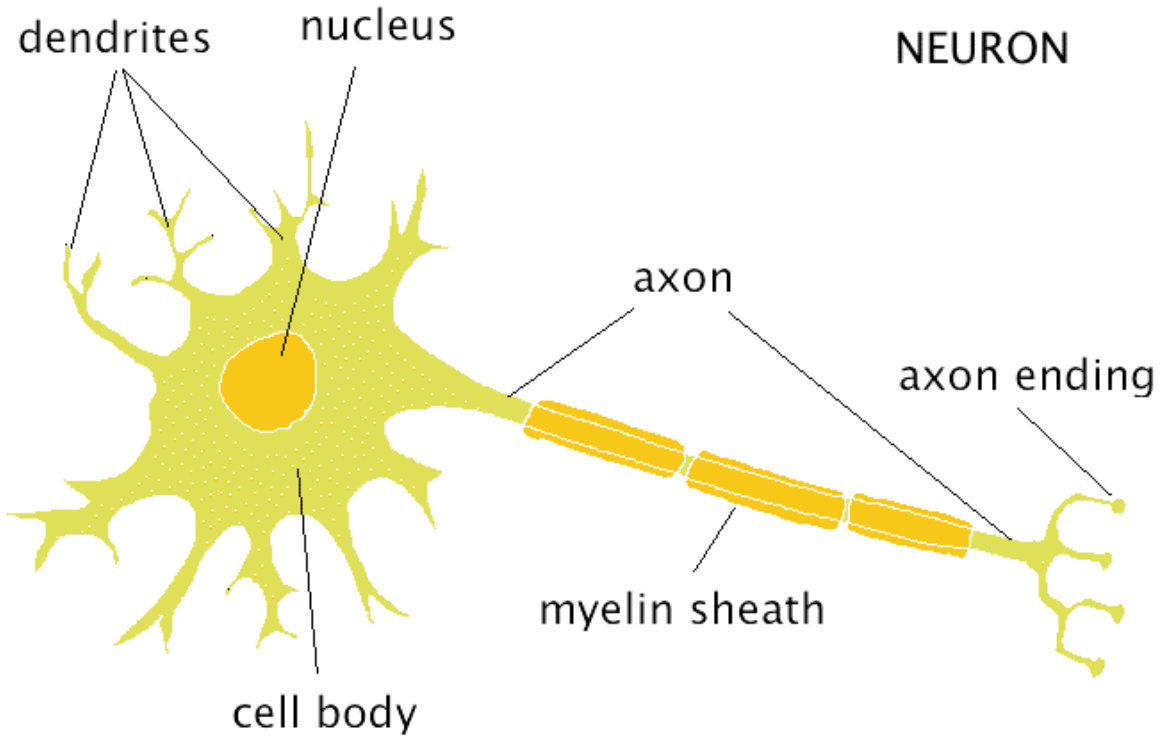
3) Neural Networks (NN):

This is the area of Artificial Intelligence 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: 2).

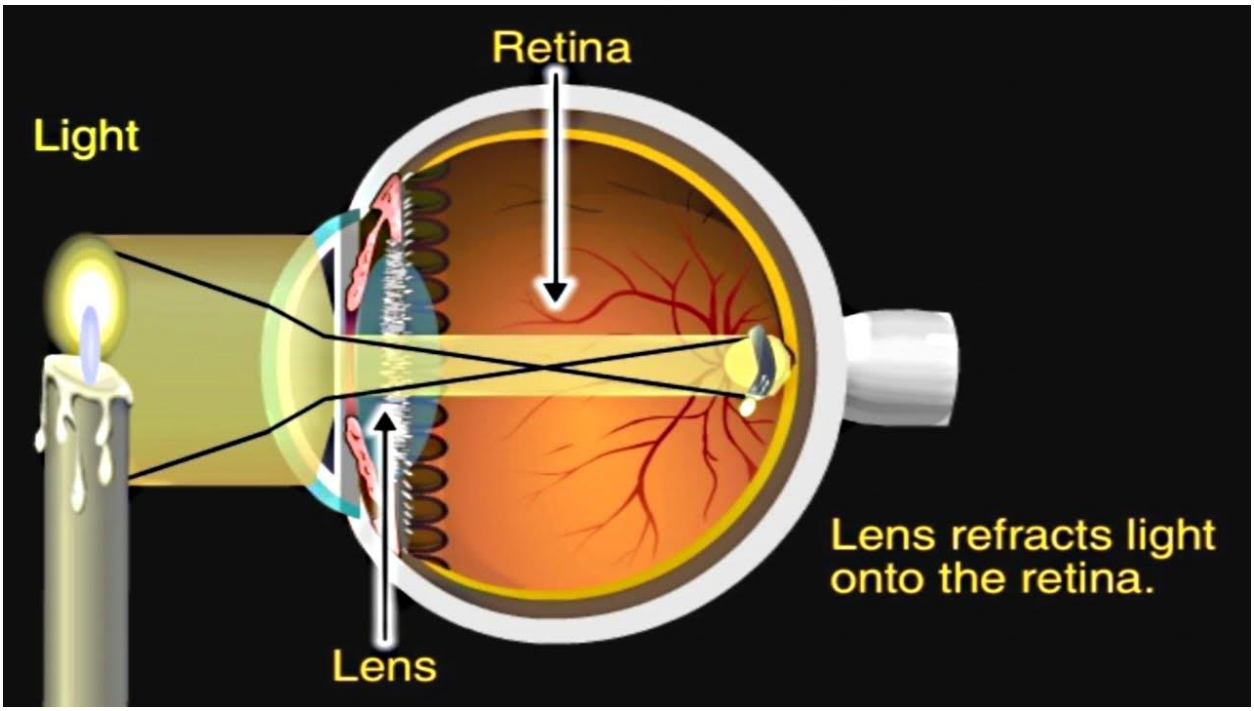
In fact, it is estimated that the human brain has an average of 100 million to 100 billion neurons, all connected amongst one another. The primary goal of a Neural Network system is to map these interactions, and hard code them so that they can be used for predictive behaviors, such as modeling the Cyber Threat Landscape. A typical neuron is illustrated below:



(SOURCE: 3).

4) Image Processing:

Without a doubt, every waking moment of our lives is spent seeing objects on a daily basis. This information is of course 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) so that vision becomes possible. This is illustrated below:



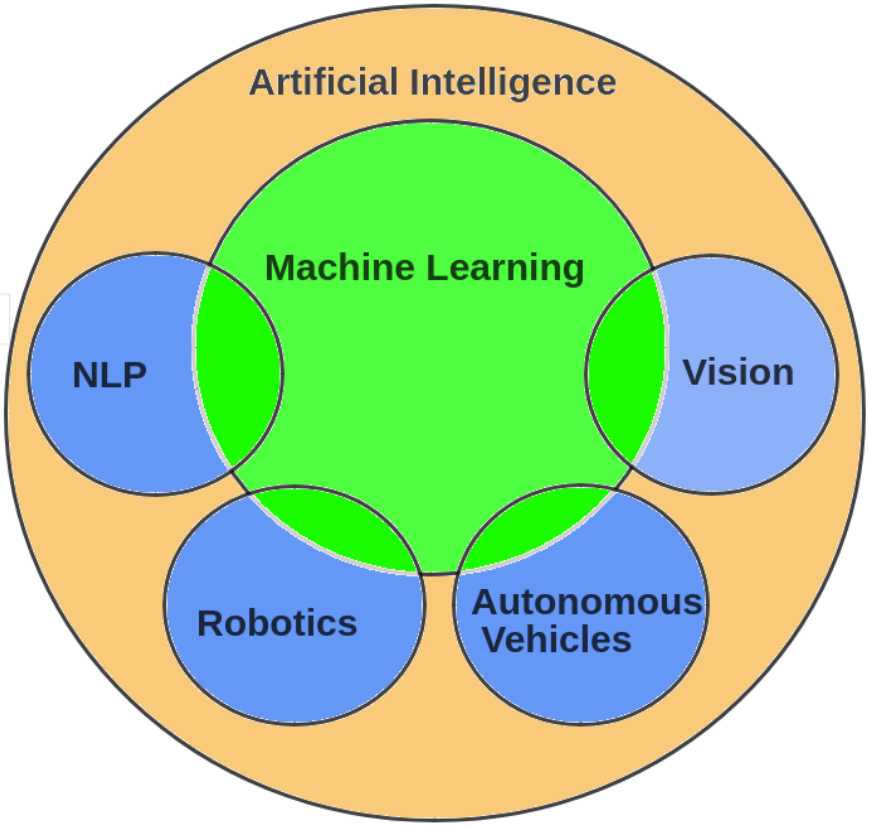
(SOURCE: 4).

This is the area of Artificial Intelligence that attempts to mimic this entire process. This is also very often referred to as "Computer Vision". One of the best examples of where this application is being used is in Facial Recognition. This is Biometric Technology that is very often used in conjunction with CCTV Technology, in order to confirm the identity of a particular individual. But by incorporating Computer Vision into these two, the robustness and reliability of a 100% identification system is made that much more possible.

5) Robotics and Embedded Systems:

Simply put, this is where Artificial Intelligence tools are being created and deployed into robots. This kind of technology is most widely used in the manufacturing industry, where they can perform very mundane and routine tasks on an automated basis with a much higher level of accuracy, and of course, at faster speeds as well.

These subspecialties of Artificial Intelligence are illustrated in the diagram below:



(SOURCE: 5).

The Role Of Artificial Intelligence In Cybersecurity

An Overview of the Applications of Artificial Intelligence In Cybersecurity

Artificial Intelligence can be used in the Cybersecurity Industry in many ways, which are still yet to be tapped into. Just as much as other technologies are constantly and dynamically changing, so too is this field. It has just started to make its debut for security applications, and there is a long way to go yet until it is fully adopted and deployed. But Artificial Intelligence is being used in some key areas in Cybersecurity, which are as follows:

- Many Cyberattacks are starting to go unnoticed today. There are two primary reasons for this:

  1) The IT Security team is so overworked that they are simply, through no fault of their own, are letting the real threat warnings and alerts fall through the cracks;
  2) The Cyberattacker is becoming so sophisticated that many of the threat vectors that they launch are very often not detected by the security tools that have been deployed at the lines of defenses.

  Through the use of Artificial Intelligence tools, many of these kinds of attacks are now starting to get noticed, and by establishing a threshold of interoperability with other devices (such as Network Intrusion Devices, Firewalls, Routers, etc.) these kinds of threat vectors are now getting

stopped in their tracks even before they make an entry into the IT and Network Infrastructure of an organization.

- As it has been described previously, the severe shortage of skilled workers in the Cybersecurity Industry has left a huge void that needs to be filled by the existing employees in the workplace. Thus, this is adding on an extra layer of burden and workload, especially when it comes to conducting routine and daily tasks. In this aspect, Artificial Intelligence can automate these kinds of job functions, thus allowing the IT Security staff to focus on the more crucial areas of their job functions. Another added benefit is that depending upon the tool that is being used, many Artificial Intelligence systems of today do not require any sort of human intervention. This simply means that once they have been programmed to any certain kind of task, the reliability of them to deliver a high-quality product is quite robust. The graphic below clearly demonstrates how the use of Artificial Intelligence can help augment an IT Security staff, based upon the number of labor hours that can be saved by automating the following tasks:

Table 1. Labor hours spent containing cyber exploits each week	Not facilitated by AI	Facilitated by AI	Difference in hours and cost
Organizing and planning approaches to cyber defense	25.32	16.05	9.27
Capturing actionable intelligence about cyber exploits and malware infections	80.20	41.11	39.09
Investigating and detecting application vulnerabilities	195.88	70.48	125.40
Investigating actionable intelligence about cyber exploits or malware	66.28	24.23	42.05
Cleaning, fixing and/or patching networks, applications and devices (i.e., endpoints) damaged/infected by cyber exploits or malware	212.89	39.63	173.26
Documenting and/or reporting upon the cyber event (in conformance with policies or compliance mandates)	25.07	15.91	9.16
Time wasted by security staff members chasing erroneous or false positives	400.83	41.42	359.41
Unplanned downtime due to cleaning, fixing or patching of malware-infected networks, applications and devices	3.95	1.90	2.05
Total hours per week	1,010.42	250.73	759.69
Total hours per year	52,541.84	13,037.96	39,503.88
Estimated total cost per year	$3,283,865.00*	$814,872.50*	$2,468,992.50*

*IT and IT security fully loaded pay rate is $62.50 (source: Ponemon Institute).

(SOURCE: 6).

- In Cybersecurity today, one of the hot topics that is coming about is that of Multi Factor Authentication, or "MFA" for short. This is where more than one layer of defense is used in order to protect IT and Network Assets. For example, rather than just using a password to gain access to shared resources, there are other authentication mechanisms that an individual will have to go through in order to positively confirm their identity. This could include incorporating the usage of Challenge/Response Questions, RSA Tokens, Smart Cards, Biometrics, etc. While all

of these are very reliable means of authentication when they are used in conjunction with another, there is still fear that a Cyberattacker can still break through any of these. Thus, there is very serious consideration being given to using Artificial Intelligence as yet another layer of authentication. But the difference here is that these kinds of systems can actually build a profile of the end user and allow for authentication based upon that person's predictive behavior. In other words, Artificial Intelligence can make a holistic judgement (based upon an infinite number of variables) in real time if the end user is really claiming with 100% authenticity who they are to be.

- At the present time, Artificial Intelligence is being used to aid in the protection of certain aspects of the IT and Network Infrastructure, from both a hardware and software application standpoint. In other words, it is only being used in local instances, not at an enterprise level, which will encompass the entire organization. It is highly anticipated, by the way that the AI technology is rapidly advancing, that this particular level of protection will become a reality in the short term.

- One of the oldest and still most widely used form of threat vectors that is used is that of Phishing. There are many new variants of it that are coming out today, especially in the way of Business Email Compromise (also known as "BEC") and Ransomware. Once again, there are so many of these that are rampant today that it is close to impossible for an IT Security staff to keep up with all of this. For example, it has been cited that 1 out of every 99 Email messages is a Phishing based one. While that may not seem like a lot, just think about the total number of messages that are sent in one day from just one business. This ratio can multiply at least 100X. An Artificial Intelligence tool can track these notorious Emails much quicker than any human being can at a rate of 10,000 messages at any given moment in time. Another advantage of using Artificial Intelligence there are no geographic limitations in which it can detect for Phishing Emails (it can virtually understand any language if it has been programmed that way), and it can also differentiate between a spoofed website and an authentic one in just a matter of seconds.

  (SOURCE: 7).

The Functionalities, or Characteristics Of An Artificial Intelligence System In Cybersecurity

As it relates to Cybersecurity, there are three main functionalities of an Artificial Intelligence system which makes it very different from the other security tools that are available. They are as follows:

1) It can learn:

   One of the main themes that has been pointed out is that a good AI system can learn, with or without human intervention (of course, the latter is much more preferred). The way that it learns is that literally billions of pieces of data are fed into it, via many intelligence feeds. Once this data is fed into it, the Artificial Intelligence tool can then "learn" from it by unearthing any trends or threat vector-based attack signatures that have not been discovered previously. It can even also learn from known trends as well. By combining these two together, the AI system can then make reasonably accurate observations or predictions as to what the Cyber Threat Landscape will look like on a daily basis, if that it is what the main purpose of has been designed to accomplish. It is important to note, while this is done on a 24 X 7 X 365 basis, the data and

information that is fed into it must be done on an almost minute by minute basis. If this is not done, the AI system can lose its robustness very quickly, and can literally become "stale". Also, based upon the datasets that are fed into it, a good AI system can also even make recommendations to the IT Security team as to what the best course of action it can take in just a matter of minutes. In this regard, Artificial Intelligence can also be used as a vehicle for threat mitigation by the Cyber Incident Response Team. An AI system that is designed for the Cybersecurity Industry can also digest, analyze, and learn from both structured and unstructured datasets (this even includes the analysis of written content, such as blogs, news articles, etc.).

2) <u>It can reason</u>:

Unlike the other traditional security technologies, Artificial Intelligence tools can also reason and even make unbiased decisions based upon the information and data that is fed into it. For example, with very high levels of accuracy and reliability, it can "... identify the relationships between threats, such as malicious files, suspicious IP addresses or insiders." (SOURCE: 8). In other words, an AI system can look at multiple threat vectors all at once and take notice of any correlations that may exist between them. From this, a profile of the Cyberattacker can be created and even used to prevent other new threat variants from penetrating into the lines of defenses. Very often, a Cyberattacker will launch differing attacks so that they can evade detection. For example, Cyberattackers have been known to hide their tracks after penetrating an IT/Network Infrastructure by covertly editing the system logs of the servers, or even just simply reset the modification date on a file that has been hijacked but replaced with a phony file. These cannot be detected by the standard Intrusion Detection Systems (IDSs) that are being used today; they can only be discovered by anomalies if significant deviations can be found. But with the use of AI, these and other hidden commonalities can be discovered very quickly in order to track down the very elusive Cyberattacker. Also, an AI system does not take a "Garbage In/Garbage Out" view of a threat vector. It tries to make logical hypotheses based upon what it has learned in the past. In fact, it has been claimed that Artificial Intelligence can respond to a new threat variant 60X faster than a human could ever possibly do.

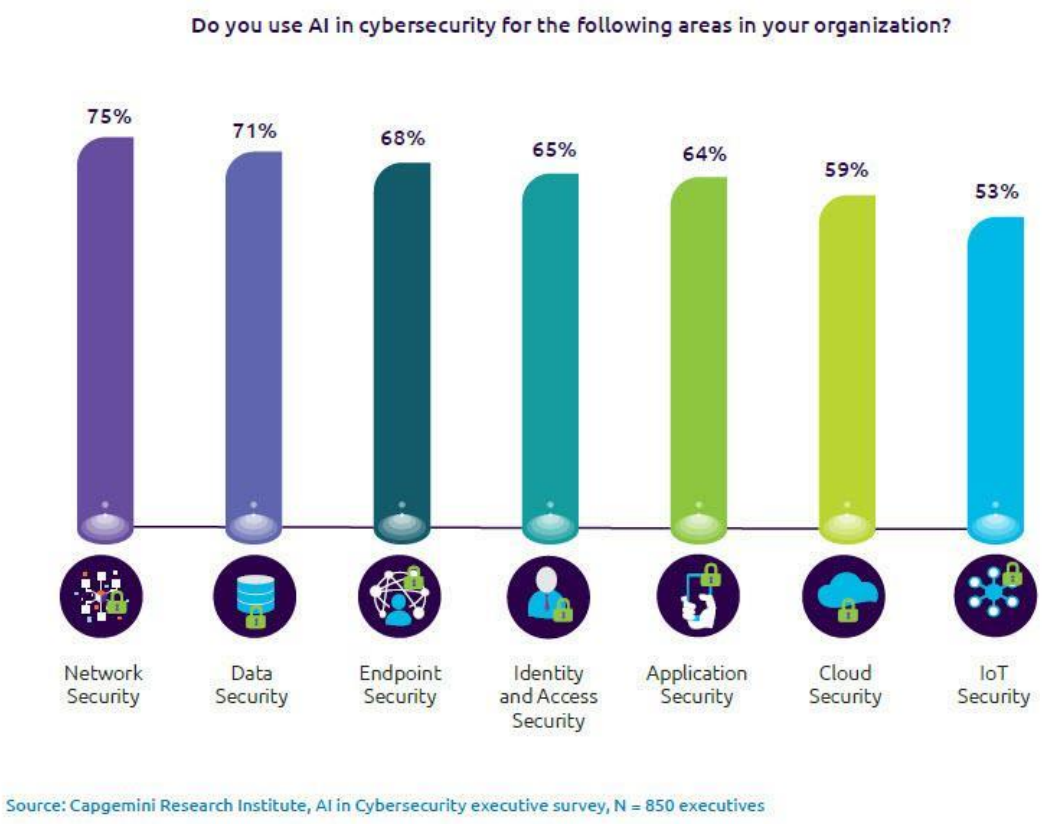
(SOURCE: 8).

3) <u>It can augment</u>:

Again, as it has been mentioned before in the last subsection, one of the biggest advantages of Artificial Intelligence in Cybersecurity is that it can augment existing resources. Whether it is from filling the void from the lack of the labor shortage, or simply automating routine tasks that need to be done, or even filtering through all the false positive warnings and messages to determine which of those are for real, AI can absorb all of these time-consuming functions that can take an IT Security team hours to accomplish and get them done in just a matter of minutes. It can also be a great tool to conduct tedious research-based tasks, can calculate the levels of risk very quickly so that the IT Security team can respond to a Cyber Threat in just a matter of seconds and mitigate it quickly.

To further substantiate the need for Artificial Intelligence in Cybersecurity, a recent study by Capgemini (which is entitled "Reinventing Cybersecurity With Artificial Intelligence") discovered the following:

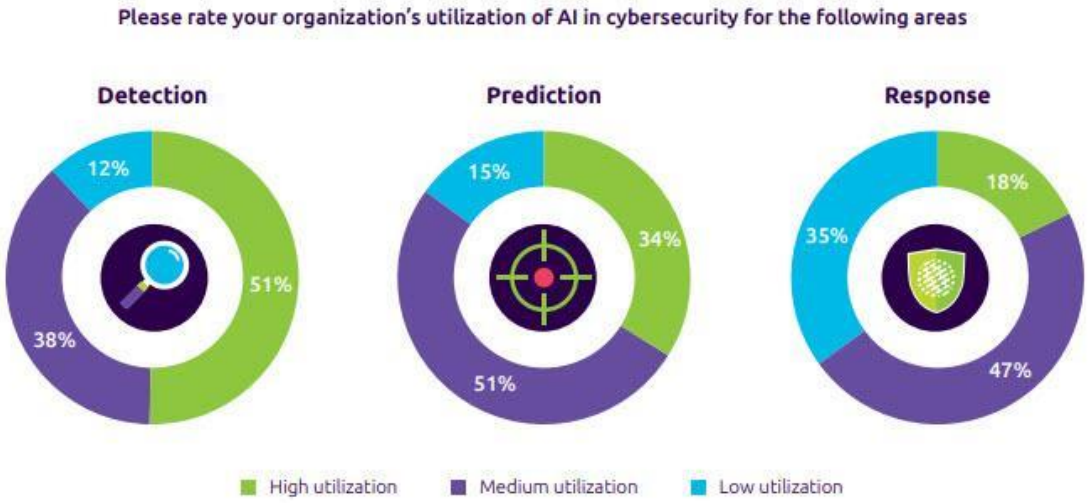
- 64% of businesses feel that they need robust AI tools in order to combat the threat from Cyberattackers;
- 73% of businesses are now developing test cases for using Artificial Intelligence primarily for Network Security purposes. This is illustrated in the diagram below:



(SOURCE: 9).

- 51% of CIOs and CISOs are planning to make extensive use of Artificial Intelligence as it relates to Threat Hunting and Detection. This is illustrated below:

Figure 3: Higher utilization of AI for detection than prediction or response



Source: Capgemini Research Institute, AI in Cybersecurity executive survey, N = 850 executives

(SOURCE: 10).

- 64% of the CIOs and CISOs claim that using Artificial Intelligence actually decreases the time it takes to respond to a particular Cyberattack, and the corresponding response time has increased by 12% as can be seen in the diagram below:

Figure 4: AI in cybersecurity lowers the cost to detect and respond to breaches

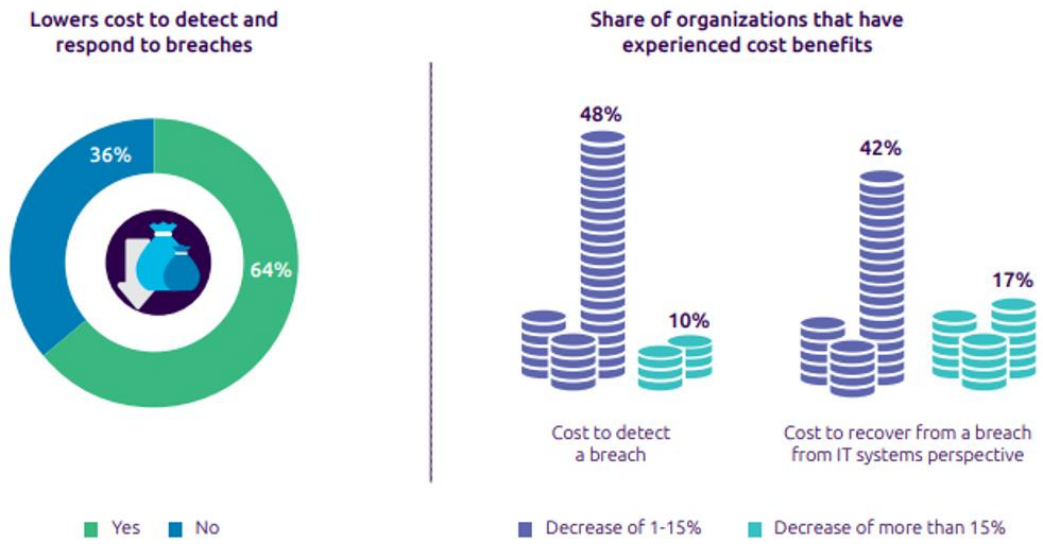
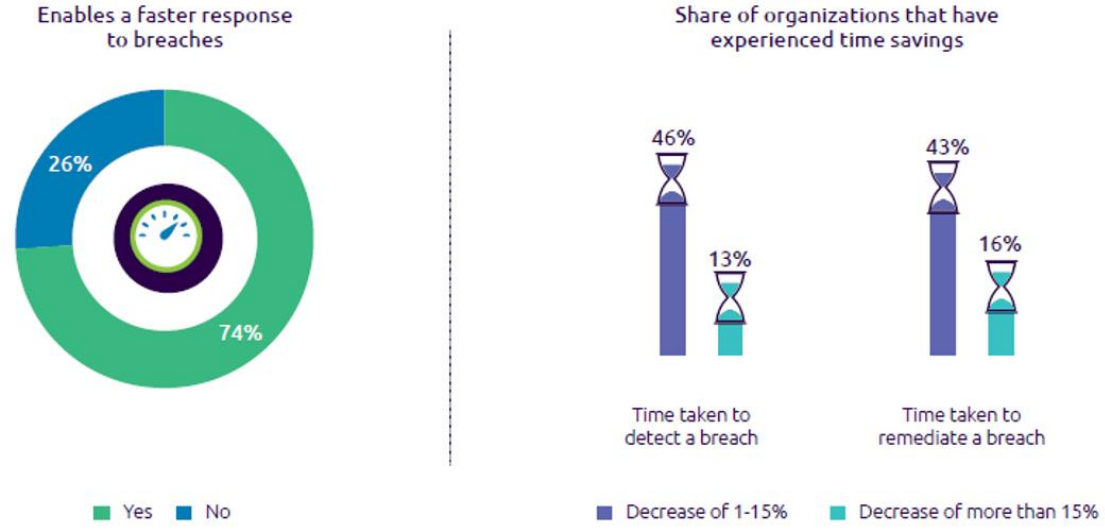


Figure 5: Nearly three in four executives say AI in cybersecurity enables a faster response to breaches



Source: Capgemini Research Institute, AI in Cybersecurity executive survey, N = 850 executives

(SOURCE: 10).

- The top 5 use cases for Artificial Intelligence are as follows:

  *Fraud Detection;

*Malware Detection;

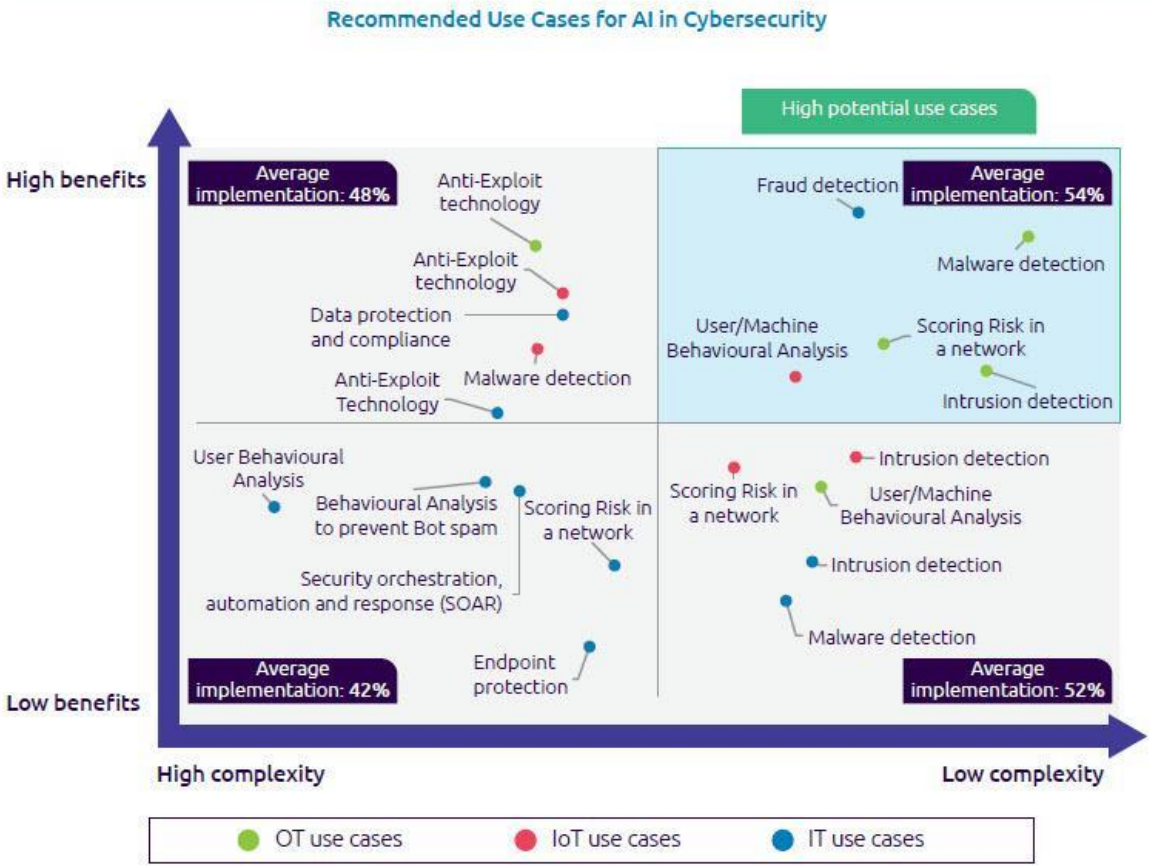
*Intrusion Detection;

*Calculating risk levels for Network Security purposes;

*Behavioral Analyzes.

This can be seen pictorially below:

Figure 7: OT and IoT use cases have higher rates of adoption



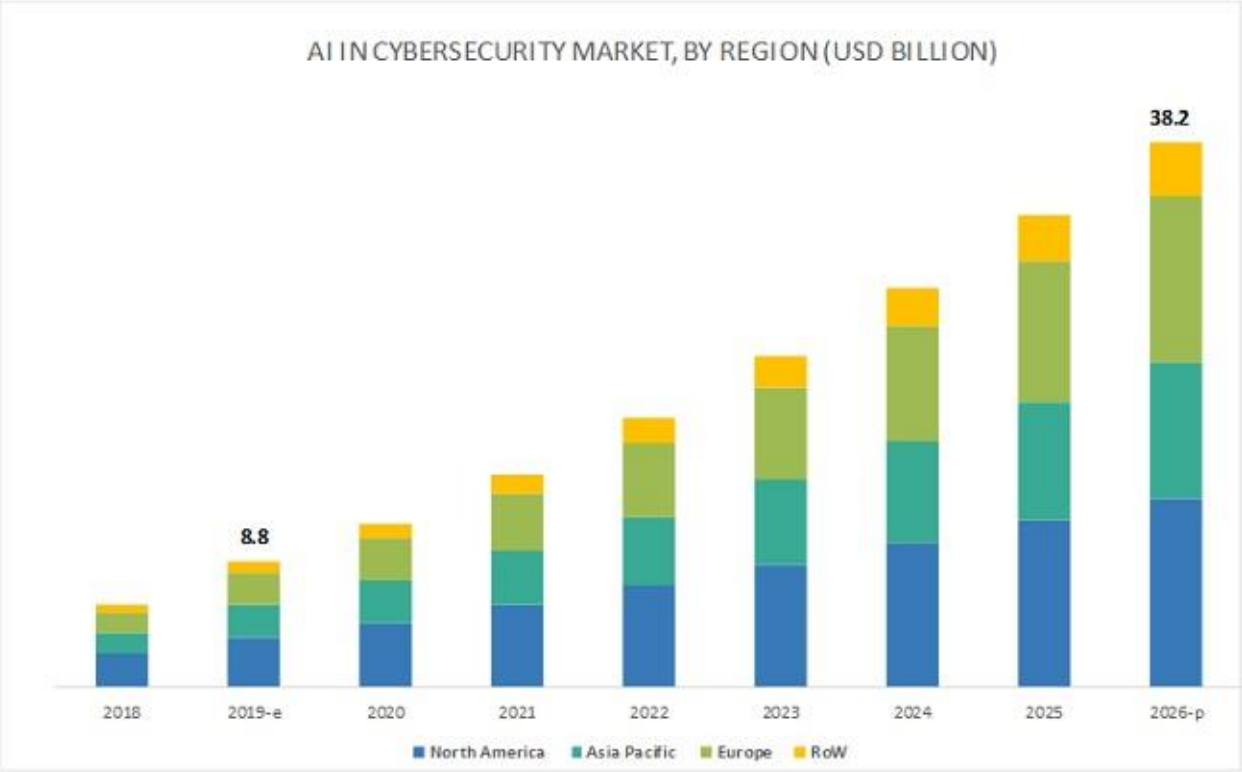
Source: Capgemini Research Institute, AI in Cybersecurity executive survey, N = 850 executives
Average implementation: Share of organizations that have deployed the use cases in quadrant at first level, multiple, or full-scale deployment.

(SOURCE: 10).

- An overwhelming 56% of Cybersecurity Executives claim that their respective staffs are too overworked and overburdened; and that an alarming 23% of these teams cannot even respond to Cyber threats as they occur;
- 48% of the CIOs and CISOs claim that plan to increase their budget for Cybersecurity by at least 29% in 2020.

It is important to note that 850 CIOs and CISOs as well as other security executives were polled in this survey. Further details on this study by Capgemini can be seen here at this link.

Overall, it appears that the spending on Artificial Intelligence in the Cybersecurity Industry will grow exponentially in the coming years, as substantiated by the diagram below:



(SOURCE: 11).

Overall, it is expected that in the United States, the spending on Artificial Intelligence technologies will be at $38.2 billion by 2026. The main catalysts for this growth are as follows:

- The rise of interconnected devices brought on by the evolution of the Internet of Things (IoT);
- The overall growth rate of newer Cyber Threat variants;
- Concerns of information and data leakage;
- The increasing vulnerability of Wi-Fi networks;
- The security posed by the various Social Media platforms (which include the likes of Facebook, Twitter, Linked In, Instagram, Pinterest, etc.);
- The need for secure cloud services in the Small to Medium sized Business (SMB) market.

(SOURCE: 11).

The Advances In AI – ChatGPT

For the most part, we are all familiar with Chatbots. These are the dialog boxes that usually appear in the lower right-hand side of your web browser. Through this, one is able to chat with what is known as a "Virtual Agent" in real time. This is the look and feel as if you are talking to a real human being (and in some cases, you actually are – it's hard to know). But over time, the Chatbot technology has greatly advanced to the point where it can now pull up the profile of an end user, based on previous conversations.

From there, it can provide rather intelligent answers to the end user based upon the questions that are being asked of it. A lot of this is done through Neural Network technology, as reviewed earlier in this whitepaper. For Chatbots, is it "Natural Language Processing", or "NLP" that is most commonly used. Btu just recently, a very sophisticated form of Chabot came out in the marketplace. This is known as "ChatGPT", and it is making waves across all industries.

The Origins of ChatGPT

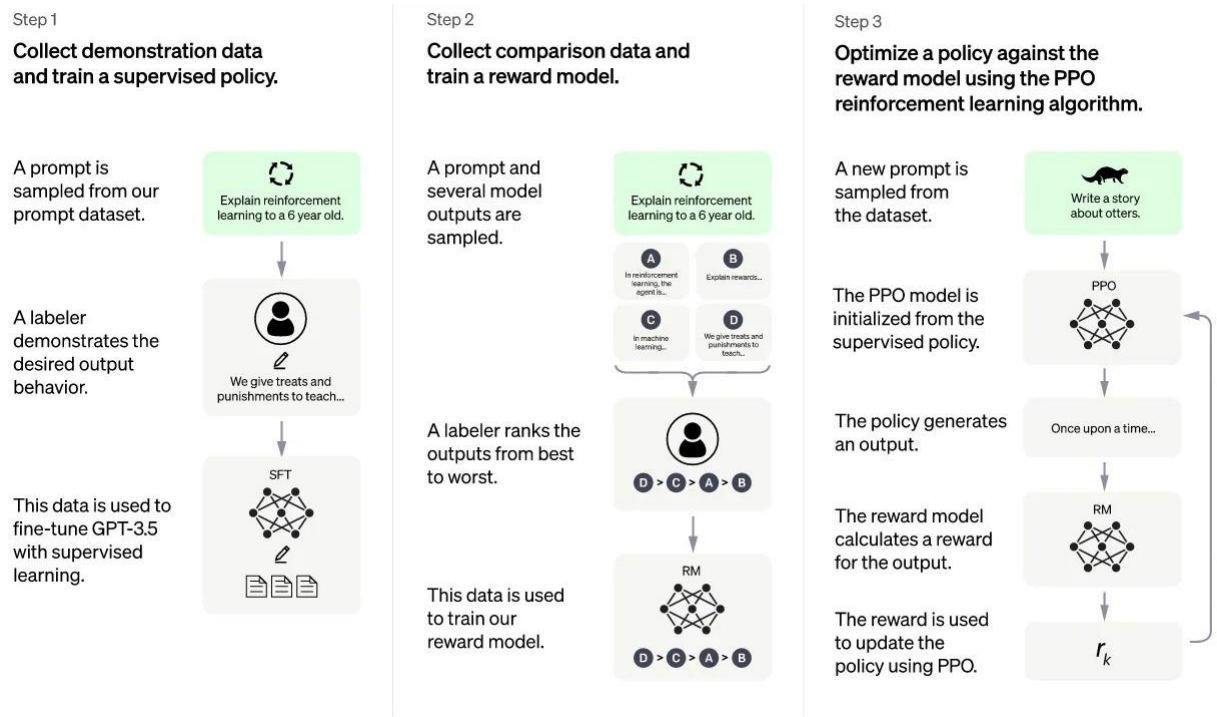
This platform was originally developed by an organization known as "Open AI". It first came out in November 2022, so it is still a fairly new application. Technically, ChatGPT is built upon Open AI's GPT-3.5 and GPT-4 algorithms of what are known as the "Large Language Models", also known as "LLMs". Further, these specific algorithms were optimized using both supervised and supervised AI learning techniques. However, as of March 2023, ChatGPT is now powered by the GPT-4 algorithm, which is the latest release from Open AI.

The Technicalities Behind ChatGPT

ChatGPT comes from the family of generative pre-trained transformer language models (This is where the "GPT" part of the name comes from). As just mentioned, it uses both supervised and unsupervised learning. It should be noted that human intervention was needed to help optimize the performance of ChatGPT. In terms of the former, the model was given real life conversations in which the developers played both sides of the fence: the end user as well as the Virtual Assistant.

With the latter, In the developers created ranked responses that the model had formulated based upon previous conversations. From here, these quantitative based rankings were then used for the development of the "reward models". These were eventually used to further optimize the model by making use of Proximal Policy Optimization algorithms, also known as the "PPO".

These processes are illustrated below:



(SOURCE: 12).

It is interesting to note that the launching pad for the ChatGPT platform was the Microsoft Azure infrastructure, which was powered by Nvidia based GPUs These algorithms were developed by Microsoft for OpenAI, at a rather huge financial cost.

At the present time, OpenAI collects information and data from the many ChatGPT end-users as feedback. This is then used to train and optimize the back-end algorithms even more. With this mechanism, the end user can either "upvote" (positive) or "downvote" (negative) the responses they receive from ChatGPT, and how useful it was for them in the project that they were trying to accomplish.

The Advantages And The Disadvantages Of ChatGPT

The Advantages

The primary thrust of ChatGPT is to provide a Chatbot that is much more sophisticated that the others that are currently being used right now. In other words, rather than appearing to display canned answers, Open AI wants their Chatbot to be as conversational as possible, with having the same experience as you would with having a conversation with a real human being. But given how sophisticated this platform has become, ChatGPT can now serve an entire host of other applications, some of which they include the following:

- It is used quite heavily for content generation. For example, rather than taking the time to create their own content, many writers are now using ChatGPT to compose an entire book for them. The publishing industry is quite aware of this, and in fact are now cracking down on authors that use this method. In fact, Kindle Direct Publishing (KDP) of Amazon (the largest self-publishing platform) has taken a harsh stance against this.

- Create and compile source code for a web-based application.
- Can emulate heavy gaming applications.
- The Financial Sector:

  *Providing financial advice;

  *Detecting any sort of fraudulent transactions;

  *The creation of Legal Documents and Contracts between banks, brokerage firms, etc.
- Sales and Marketing:

  *SEO;

  *Keyword Research;

  *Creating customer feedback forms.
- The Healthcare Industry:

  *Medical Transcription;

  *Triaging of patients in the ER;

  *Creating Virtual Agents for the purposes of scheduling medical appointments.
- It is now becoming a strong alternative to the Google Search Engine.
- It can also be used for Language Translation, for example converting an English book into Spanish, and many other languages.
- The Educational Sector:

  *Resume writing/proofing/editing;

  *Recruiting and even interviewing candidates.

But of course, as the sophistication of the algorithms in ChatGPT grows even more sophisticated, the applications it will serve will also explode.

<u>The Disadvantages</u>

Despite the advantages of ChatGPT, it also suffers from a number of limitations as well, some of which are as follows:

*The output is not what the end user is expecting (but this is true of all AI apps - a lot of this depends upon the data that is fed into it). In technical terms, with regards to Large Language Modeling, this is also known as “Hallucination”.

*It is also the case that in the efforts to make ChatGPT has human like as possible, it is possible that it can become too overtrained, and not give the correct, or expected out. In technical terms, this phenomenon is also known as “Optimization Pathology”, which is also known more commonly as Goodhardt’s Law.

*It is prone to “Algorithmic Bias”. This is where the algorithms that drive ChatGPT cerates unfair outcomes, in which one output is highly favored over the alternatives.

*ChatGPT cannot connect to the Internet, thus it is unable to provide answers on a real time basis. For example, if you ask it to give you the temperature and weather conditions at this very moment, it will not be able to do it.

*It can only accept inputs from the end user in a text only version. It cannot pull in resources from other areas, such as websites, videos, and images.

*It is unable to multitask. This simply means that you can only present one query at a time to it.

*Because of the sophistication of its algorithms, it takes a lot of overhead in terms of both computing and processing power in order to come with answers to the queries that it is posed with.

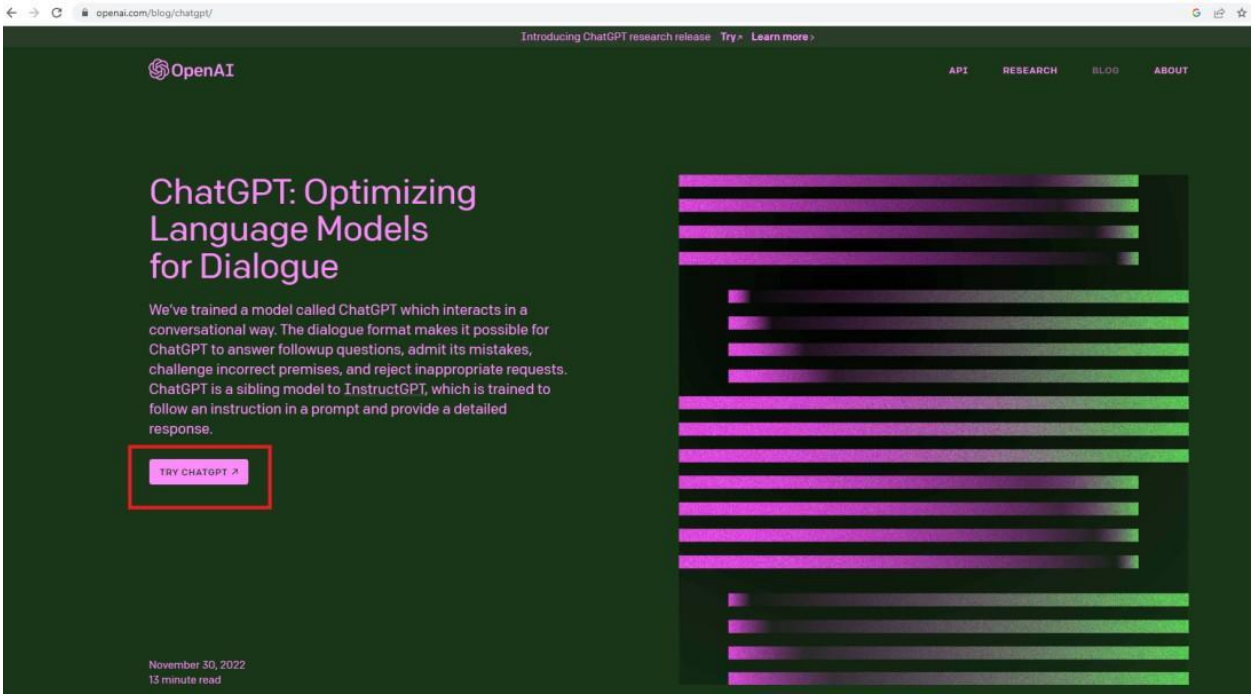
*AI algorithms can go “stale” quickly over a short period of time. Therefore, there is the constant need to keep them updated, refined, and optimized at all times.

*There have been complaints that ChatGPT can be very wordy in terms of its answers, and usually not enough detail is provided, especially for complex queries.

A Preview Into ChatGPT

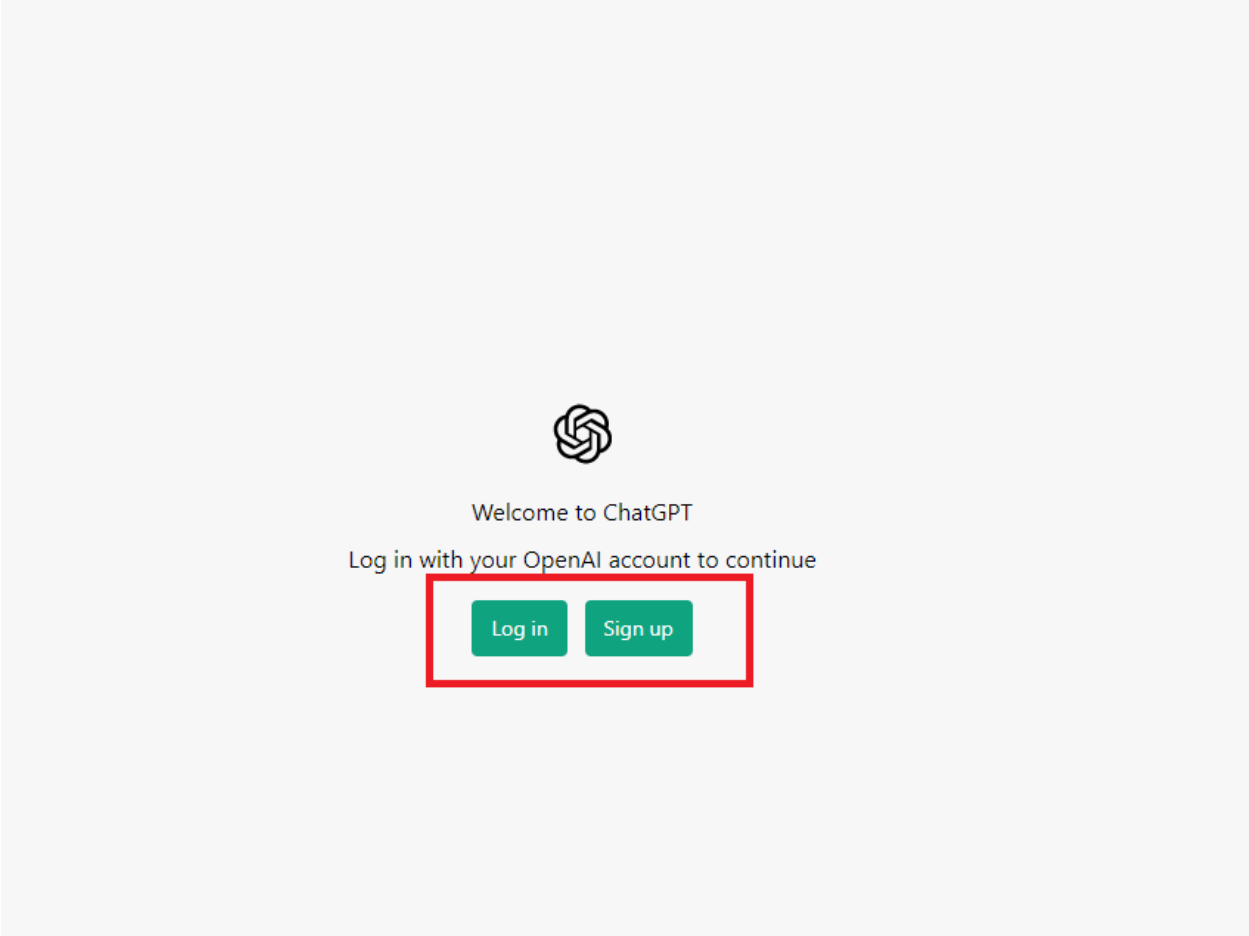
In this section of the whitepaper, we take a look at how to launch a simple application using ChatGPT.

1) First log into the ChatGPT website, and create your own account:



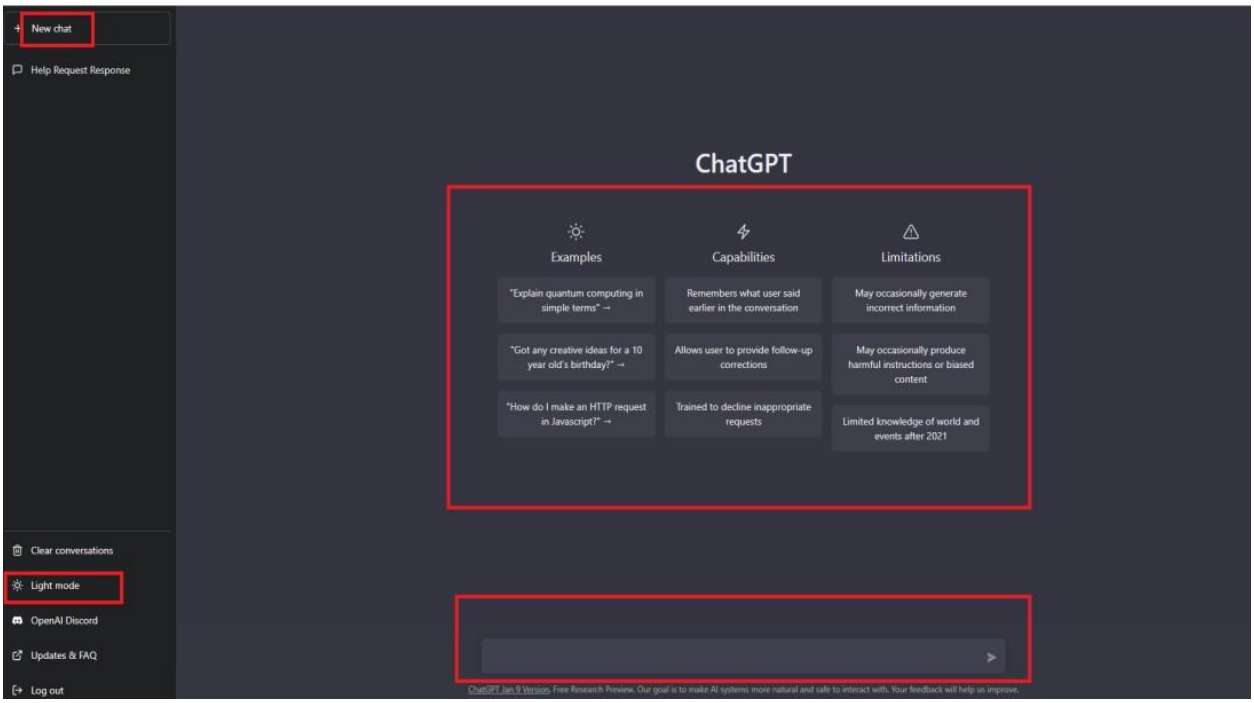
(SOURCEL 13).

2) Log into your newly created account:



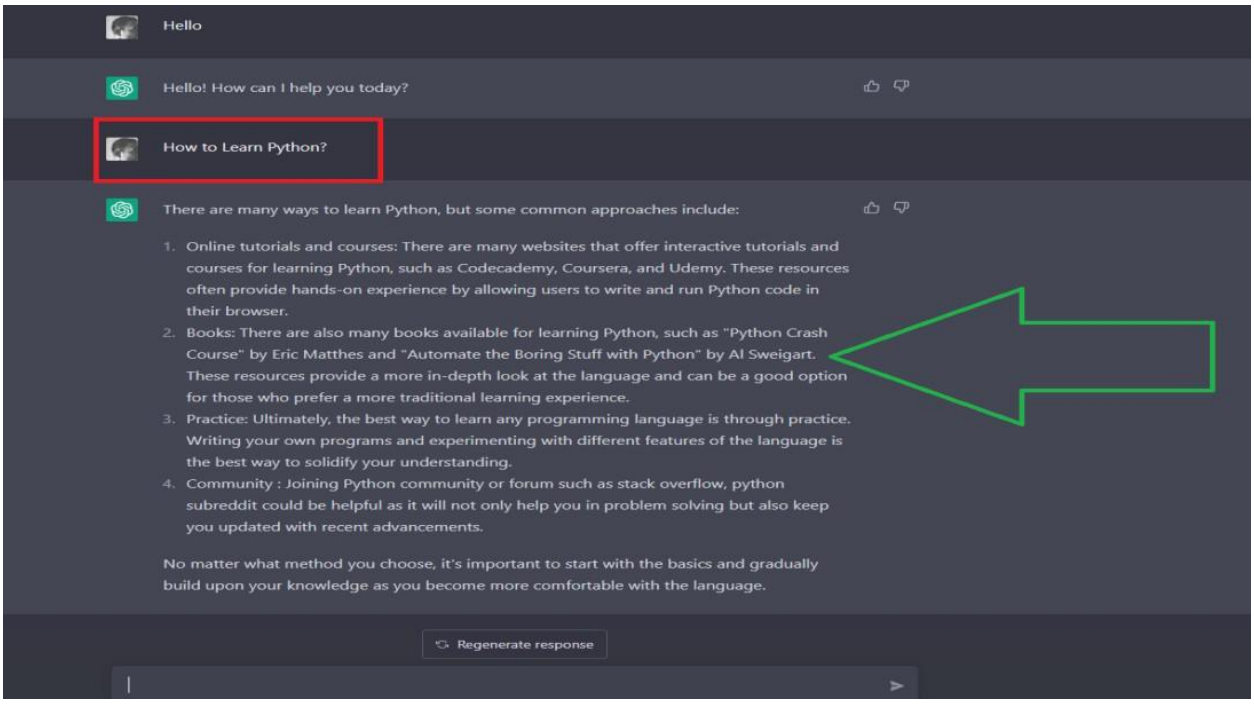
(SOURCE: 13).

3) After logging in, you will be given a brief tour of ChatGPT:



(SOURCE: 13).

4) You can now start asking ChatGPT your queries, and in this example, the end user is asking it how to learn Python:



(SOURCE: 13).

Conclusions – The Implications Of ChatGPT

ChatGPT, and all other forms of AI and ML will be around with us for a very long time. The way technology is going is that it is going to become much more sophisticated as time goes on. While there are the many strategic benefits of AI, there are also a lot of societal impacts that we have not even fathomed yet. One huge concern is its use in replacing jobs currently being done by humans.

Another big concern of this platform is that it can also be used for nefarious purposes as well, especially when it comes to Cybersecurity. There is a great amount of both fear and apprehension in the industry that the Cyberattacker can create malicious code with it, and launch massive Ransomware attacks with it. This is even despite the fact that Open AI has pledged that there are safeguards with respect to this.

In fact, there now have been cries amongst business leaders to slow or even halt the pace of the growth of AI, until we as a society, can truly understand its repercussions, both for good and bad. But in the end, ChatGPT and AI is just another tool – it can never, ever come close to fully replicating the thoughts and reasoning power of the human brain.

Sources

1) https://www.forbes.com/sites/cognitiveworld/2019/06/19/7-types-of-artificial-intelligence/#301ec3a6233e
2) https://www.brainfacts.org/brain-anatomy-and-function/anatomy/2012/the-neuron
3) http://webspace.ship.edu/cgboer/theneuron.html
4) https://www.youtube.com/watch?v=YcedXDN6a88
5) https://medium.com/@chethankumargn/artificial-intelligence-definition-types-examples-technologies-962ea75c7b9b
6) https://www.ibm.com/security/artificial-intelligence
7) https://www.forbes.com/sites/louiscolumbus/2019/07/14/why-ai-is-the-future-of-cybersecurity/#187aab24117e
8) https://www.marketsandmarkets.com/Market-Reports/artificial-intelligence-security-market-220634996.html
9) https://www.plugandplaytechcenter.com/resources/how-artificial-intelligence-transforming-cybersecurity/
10) https://www.entrepreneur.com/article/339509
11) https://www.cs.bham.ac.uk/~jxb/IAI/w2.pdf
12) https://levelup.gitconnected.com/what-is-chatgpt-openai-how-it-is-built-the-technology-behind-it-ba3e8acc1e9b
13) https://www.geeksforgeeks.org/what-is-chatgpt/
14) http://technoitworld.com/5-artificial-intelligence-fields-changing-way-things-work/
15) https://aboutssl.org/role-of-artificial-intelligence-in-cyber-security/
16) https://www.cncs.gov.pt/content/files/cybersecurity_and_the_role_of_artificial_intelligence-_arlindo_oliveira.pdf
17) http://techgenix.com/cybersecurity-ai/