Artificial Intelligence: The Context of the current stage regarding usage of the AI and its applicability.

Ailton Macupe Feliciano Baúque (**0x3**),

0x Team, Security Operation Center, ATHSec, Mozambique

ABSTRACT

In this article, I talk about AI plus its impact on our society, focusing on what it brings to our digital environment and CS. AI has been around for a long time since automation. But as the technology evolved, so did it, and today it generates a lot of discussion about its direction.

One of the main challenges of AI is its potential to make people sluggish. With machines performing more advanced and automated tasks, we are becoming less engaged and less willing to learn.

Another challenge is the threat to our digital security, as cybercriminals can exploit AI systems to carry out cyberattacks. AI also has some benefits that can help us in our security systems, allowing us to identify patterns and analyze large volumes of data quickly and accurately.

To ensure the responsible as well as safe development and use of AI, ground rules with regulations are needed. Without proper regulations, there is a risk that AI will be developed and used in ways that are unsafe and unethical. Therefore, it is fundamental that we establish clear norms in addition to standards for its development and use, in order to extract the benefit of its potential and minimize its risks.

Keywords: Artificial Intelligence, Digital Security

Email Address: ***ailtonbauque@outlook.com***

Submitted to ATHSec May 13, 2023

INTRODUCTION

The concept of artificial intelligence has been around for centuries, with humans using various forms of automation to make tasks easier and more efficient long before the advent of computers and machines. From the water clocks of ancient Greece to the spinning jenny of the Industrial Revolution, humans have been seeking ways to automate tasks and replace manual labor for millennia.

However, it wasn't until the mid-20th century that the term "artificial intelligence" was coined and the field began to take shape as we know it today. With the development of computers and advanced algorithms, the potential for AI to revolutionize industries and transform the way we live and work became increasingly clear.

But with these exciting possibilities come new challenges and ethical considerations. As AI becomes more advanced and autonomous, questions about its impact on society, its potential biases, and the potential for misuse have come to this world.

AI: DEFINITION

The term AI has a lot of definitions used over the decades. According to John McCarthy in his paper from 2004, he says AI “It is the science and engineering of making intelligent machines, especially intelligent computer programs. It is related to the similar task of using computers to understand human intelligence, but AI does not have to confine itself to methods that are biologically observable.”

AI, or artificial intelligence, refers to the development of computer systems and algorithms that are designed to perform tasks that typically require human intelligence, such as visual perception, speech recognition, decision-making, and natural language processing. In other words, AI involves the development of machines that can "think" and perform tasks that would normally require human intelligence.

Artificial Intelligence is the ability of a computer to perform tasks that require some understanding, knowledge, and inferring of information from machines to successfully accomplish certain tasks that require intelligence, or reason on human beings.

CHALLENGES BROUGHT BY AI

One of the potential downsides of AI is that it could make people more reliant on machines to perform tasks, which could lead to increased laziness and reduced engagement in daily activities. As AI becomes more advanced and capable, it may be able to perform tasks that were previously done by humans. However, if people become too reliant on them, they may begin to neglect important tasks or become less engaged, sometimes unable to do certain tasks.

Another concern is the potential for AI to be used in the development of advanced malware. With its ability to analyze and adapt to its environment, AI can be used to create highly sophisticated malware that is difficult to detect and remove.

AI can also be used to create highly effective phishing attacks. If enough data is given, it can generate highly targeted phishing emails that are much more likely to be successful than traditional phishing attacks.

Finally, AI can be used to automate attacks, making them faster and more efficient than ever before. As an example of that, the tool “**PentestGPT**” powered by the latest model of GPT-4, is just the beginning of it.

IMPACT OF ARTIFICIAL INTELLIGENCE

Rapid advances in artificial intelligence have the potential to significantly disrupt labor markets. While AI based tasks can augment the productivity of some workers, they can replace the work done by others and will likely transform almost all occupations at least to some degree. This is the impact of AI, which is significant especially in the community, where it can be used to improve public services such as healthcare, transportation, and emergency services. However, AI can also result in job displacement and privacy concerns.

In another perspective, AI can be used to detect and prevent cyber attacks. However, AI can also be used by hackers to develop more advanced and sophisticated attacks. As such, there is a need for cybersecurity professionals to stay tuned and implement measures to protect against AI-powered attacks.

BENEFITS EXTRACTED FROM THE USE OF AI

It is not just a concern, AI also brings a ton of things to be happy about, for instance it gives us the ability to be more precise in some cases. Using AI we can help our security systems to scale the pattern of attacks used in the incredible speed and precision that a regular SOC Analyst wouldn't, analyze large amounts of logs seeking for patterns and a lot of other anomalies.

So some of the benefits of AI are: Increased precision, Efficiency, Personalization, Innovation and sometimes Improved safety.

CONTINGENCY PLAN

As it suggests, currently in this rush to build AI systems we are going blinded. As the development and use of AI systems continue to accelerate at a breakneck pace, it is important to consider the long-term perspective of where we will be in 50 years. With a focus on security, it is critical to double-check whether the systems being developed and implemented are secure or not.

Unfortunately, the absence of a regulatory entity to oversee the creation of AI systems in terms of security presents a significant challenge. While a minimum level of safety is often prioritized for the system itself, the safety of the people involved around the system is of paramount importance. The lack of legal conditions to ensure the security of AI systems creates the potential for abuse and misuse.

To address these concerns, guidelines and standards should be established to provide a framework for AI development. While developers have the freedom to create what they wish, there must be a set of fundamental rules to ensure that the technology is used ethically and with consideration for the safety of all parties involved. By establishing these standards, we can help mitigate potential risks and ensure that AI systems continue to bring benefits to society and by extension our digital security.

REFERENCES

John McCarthy, WHAT IS ARTIFICIAL INTELLIGENCE? (2004).

https://www-formal.stanford.edu/jmc/whatisai.pdf

https://www.ibm.com/topics/artificial-intelligence

Artificial Intelligence: A Modern Approach (https://aima.cs.berkeley.edu/)

https://www.britannica.com/technology/artificial-intelligence

https://www.britannica.com/question/What-is-the-impact-of-artificial-intelligence-AI-on-society

https://www.procon.org/headlines/artificial-intelligence-ai-top-3-pros-and-cons/