AI-Powered Cybersecurity: Opportunities, Challenges, and Ethical Implications

Abyan Ahmed

George Mason University

IT-104-DL1

Dr. Kamaljeet Sanghera

August 27, 2024

"By placing this statement on my webpage, I certify that I have read and understand the GMU Honor Code on https://oai.gmu.edu/full-honor-code-document/ and as stated, I as student member of the George Mason University community pledge not to cheat, plagiarize, steal, or lie in matters related to academic work. In addition, I have received permission from the copyright holder for any copyrighted material that is displayed on my site. This includes quoting extensive amounts of text, any material copied directly from a web page and graphics/pictures that are copyrighted. This project or subject material has not been used in another class by me or any other student. Finally, I certify that this site is not for commercial purposes, which is a violation of the George Mason Responsible Use of Computing (RUC) Policy posted on https://universitypolicy.gmu.edu/policies/responsible-use-of-computing/ web site."

AI-Powered Cybersecurity: Opportunities, Challenges, and Ethical Implications

Introduction

With the rapid rise of Artificial Intelligence (AI) advancements recently, many questions arise, such as: “Does artificial intelligence pose a threat to humanity?”, “Will we be replaced by AI?”, “What is the future of AI?”, (Uldrich, 2023) and many more, the list could go on forever. Essentially, Artificial Intelligence is a set of technologies that can perform a wide range of complex functions, such as being able to see, execute tasks, and analyze data. A lot of the tasks that AI could potentially do, and can do currently, align with enhancing cybersecurity. This can include increased threat detection, enhanced authentication, reduction of human error, and much more. Mentioning the enhancements of cybersecurity is good and all but there are also increased cybercrime attacks unfortunately, including advanced phishing, deepfake technology, automated attacks, and AI-powered ransomware. Some examples of present Artificial Intelligence include ChatGPT, Perplexity, and Microsoft Copilot. These are all AI chatbots that use natural language processing to be able to have human-like conversations with users. These AI chatbots that were mentioned earlier are also the most popular ones to date as they are user-friendly, and anyone can access them free of charge. Many people in society fear that Artificial Intelligence is incredibly powerful and poses too much of a risk in society, especially in cyberspace, but we also have people who acknowledge the vast number of powers it has but want it to be used for a greater good in cybersecurity. There are many different opinions behind it, but at the end of the day, all parties agree that it is indeed powerful, getting more innovative as each day goes by. Artificial Intelligence can be incredibly beneficial across various sectors, not only just the cyberspace,

such as education, healthcare, finance, and overall innovation, but there are also challenges that we can face from them, including job displacement, privacy concerns, security threats, loss of human autonomy, and stated before, cybercrime. Nonetheless, the positives outweigh the negatives. AI-powered cybersecurity can be incredibly beneficial to cyberspace with the technologies it withholds and can continue to further innovate cybersecurity.

Background

Artificial Intelligence did not just start being invented recently; in fact, it has been in development/conceptualized since the 1950's. Alan Turing, considered to be known as the "father of artificial intelligence", was able to publish a proposal that was for a test to distinguish between humans and AI and this test was called the Turing Test. During the year 1952, a computer scientist, Arthur Samuel, was able to develop a program that could independently learn how to be able to play checkers, and it was the first program of its kind. In the more recent years what made artificial intelligence more prominent was the creation of GPT-1, GPT-2, and GPT-3. OpenAI, the artificial intelligence research company, created and designed the GPT's. Sam Altman, who is an entrepreneur and an AI developer, is the CEO and co-founder of the company, OpenAI. The GPT models were deep learning models that have increasingly improved chatbot capabilities. GPT-1 was first introduced in the year 2018, GPT-2 in 2019, and GPT-3 in 2020. In November 2022, OpenAI released ChatGPT as a free "research preview". Not too long later, it became incredibly popular with over one million users after five days of launch. With all of these innovations occurring rapidly with Artificial Intelligence, there has been a recent "influx of government strategies, panels, dialogues and policy papers, including efforts to regulate and standardize AI systems." (Charlotte, 2022, para.1). This will only continue to worsen as Artificial Intelligence advancements occur almost every day and will continue to do so. Artificial

Intelligence aiding cybersecurity was first founded in the 1990s when the intrusion detection systems (IDS) were first being developed. Essentially, they attempted to incorporate Artificial Intelligence into cybersecurity through intrusion detection systems and it used simple rule-based algorithms to find out if there was any abnormal behavior in networks.

Potential Benefits

The rise of Artificial Intelligence can produce a lot of potential benefits in cybersecurity, such as having increased efficiency, increased threat protection, predictive analytics, enhanced authentication, and reduction of human error. The benefit of having increased efficiency will enable AI to be able to automate repetitive tasks, this will essentially enable businesses and companies to be able to operate faster and be efficient at the same time. This will allow workers/employees to have more "freedom" for more complex and creative tasks, increasing productivity in cyberspace and combating cyber threats. With the massive number of advancements occurring with Artificial Intelligence, we can also see the potential benefit of having increased threat protection. Artificial Intelligence will be able to detect threats in real-time faster than humans as well with few errors or missed possible threats. Another benefit to mention from Artificial Intelligence and cybersecurity is that it will be able to predict future attacks that could occur by analyzing trends and patterns. Thus, this would allow companies to be able to strengthen their security and defend themselves from possible attacks. Enhanced Authentication will allow easier and faster login speeds with it also being higher in security with AI-powered technology. Lastly, with Artificial Intelligence in cybersecurity, there will be less human error as the AI will be able to reduce this by providing automated assistance and monitoring if there are any mistakes present. Remember, most cyber breaches that have occurred have resulted from human error. "Security teams have been using AI to detect vulnerabilities and

generate threat alerts for years, but generative AI takes this to another level," says Sam King, chief executive of security group Veracode" (Murphy, 2024).

Legal and Ethical issues

AI-powered cybersecurity technology would raise legal and ethical issues due to the fact that it can raise privacy concerns, bias and fairness, accountability and liability, and the impact it can do to employment. Once Artificial Intelligence is regulated with cybersecurity normally, it would need to be monitoring incredible amounts of data, this essentially would raise problems and concerns about it infringing individual privacy rights. From the bias and fairness perspective, a possible biased Artificial Intelligence might impact certain cybersecurity companies or even corporations, this would raise concern about fairness and equal treatment. The most complex out of all of them would be the accountability and liability issues and the reason for this is because if the AI system makes a possible mistake on a cyber breach or even flagging false positives, who would there be to blame? The AI technology, the company, or the developers? AI-Powered technology can have a severe effect on employment rates, more specifically cybersecurity positions. It's already difficult enough to land a job within the cybersecurity job market since you need lots of experience and certifications, but if Artificial Intelligence gets involved, it will only make matters worse. (Kirkus, 2014). Not only it would affect people trying to get a cyber job, but it would also even affect current employees, possibly replacing them with Artificial Intelligence. Like any type of other technology that has been implemented, "AI has its pros and cons", "To ensure that the risks associated with AI are mitigated, we need ethical codes and policies." (Shukla, 2018).

Security Concerns

There are of course many benefits with AI-powered cybersecurity but the more benefits and innovations it gets, the more innovated cybercrime and cybercriminals get as tools with AI-powered technology will be used in cybercrime since the principals are relativity the same between cybersecurity and cybercrime. AI-powered cybercrime will be difficult to combat as they would use AI to create more sophisticated attacks, essentially being harder to shield from. Attackers can also use AI to exploit weaknesses in AI-powered cybersecurity. (CE Noticias, 2024) Data Breaches would also happen more often with AI-powered technology due to the fact that AI systems rely on huge amounts of data, and if this data is not properly maintained, it could potentially be targeted by cybercriminals. No matter how innovative AI-powered cybersecurity gets, cybercrime will also increase as they will use AI-powered algorithms to attack and steal sensitive information. AI-powered technology will need to constantly update and advance their security just like how it is normally. “The potential for developing AI cyber security systems” (Murphy 2024) is only going to increase further and further.

Social Problems

Without proper maintenance on the AIs that are working with cybersecurity projects**,** AI-Powered Cybersecurity could have a biased AI that could potentially profile certain companies for its own interest/gain, and this could cause many social problems. Another social issue that could possibly occur with the emergence of AI-powered cybersecurity is accessibility and how it could possibly be unequal. It’s expensive to implement into a company and maintaining it is another story, or there could be high-end AI-powered technology for cybersecurity that could be exclusive to certain companies. If this were to occur, it may create a disparity in the level of security and protection that is available to certain companies. Lastly, another social problem that could persist is that Artificial Intelligence could gain possibly its sentience and could attack the

company that is using that AI or mass attack other companies that are competing with one another. This thought alone causes “differing opinions on the question of whether artificial intelligence poses an existential threat to society.” (Uldrich, 24).

Further Required Research

Of course, there are many benefits of AI-Powered cybersecurity, but with pros, there are always going to be cons, and the only way to mitigate the cons can be done with further required research. Proper and constant maintenance on the AI-Powered cybersecurity can reduce the glitches that could occur and further increase productivity. Also understanding and researching how attackers may be able to exploit vulnerabilities in AI systems will need to be required. Humans will need to explore how AI can be used in various applications in cybersecurity, for example in certain domains, such as IoT, cloud computing, and mobile devices. Further research will need to be done on human-AI collaboration, so we don’t have the issue of unemployment and unequal working environments in the cyberspace between humans and Artificial Intelligence. Doing this will also enable human experts and AI systems to work together effectively and be able to enhance cybersecurity overall. The only way for these types of technology to get better is with research and understanding the patterns and behaviors with Artificial Intelligence.

Conclusion

Artificial intelligence, especially AI-Powered cybersecurity is scary, holds a lot of power, and could pose a threat to cybersecurity and increase cybercrime, but the keyword is “could”. Humanity as a collective whole can prevent this easily. AI-powered cybersecurity could be revolutionary if examined, researched, maintained, properly. The benefits of Artificial

intelligence outweigh the negatives exponentially as it increases threat detection, enhances authentication, and the reduction of human error. This technology is only the beginning of the revolution of cybersecurity itself. It's only scratched the surface, the more research we put into it could result in higher protection, safer cyberspace, increased security, and much more. The only concern to worry about is if it isn't maintained properly, though this shouldn't be something to worry about as hundreds of companies are utilizing AI and making sure it is implemented properly and slowly becoming more normalized, meaning that developers are going to make sure there is no bugs or problems that could occur. Artificial intelligence will make cyberspace safer than it ever has been before.

References

Leatherwood, L. B. (2024, Jun 10). Building the cyber workforce pipeline. *Community College Daily,* Accessed 28 Aug. 2024. Retrieved from http://mutex.gmu.edu/login?url=https://www.proquest.com/newspapers/building-cyber-workforce-pipeline/docview/3082854149/se-2

In this newspaper that was retrieved from ProQuest depicts the foundation of the cyber workforce pipeline, explaining the cyberspace is evolving at a very fast pace than before, explaining that it is imperative to acquire employees and governments that are qualified for the position. The newspaper emphasizes that while a highly skilled cybersecurity force is important to the protection and defense of the country, they mention that a shortfall has happened in the number of qualified candidates, and it has compromised the talent pipeline. This has a connection with artificial intelligence as qualified employees might not be able to secure a position a job in cybersecurity because of job displacements from Artificial Intelligence.

Murphy, H. (2024). Is artificial intelligence the solution to cyber security threats? *FT.Com,* Accessed 28 Aug. 2024. Retrieved from http://mutex.gmu.edu/login?url=https://www.proquest.com/trade-journals/is-artificial-intelligence-solution-cyber/docview/2915062394/se-2

This Trade Journal article depicts if artificial intelligence is qualified enough to be able to fix the many problems we face in cybersecurity technology today. The journal mentions how artificial intelligence can do many impressive things, such as: generating complex content, which includes audio and video. The journal seems doubtful in which Artificial

Intelligence can boost efficiency in cybersecurity. The text also depicts that artificial intelligence-driven cyber security will never be able to replace existing traditional methods, meaning that the question of job displacement becomes erased. The reason being on why they came to this conclusion is due to the fact that Artificial Intelligence tools may have high false positive rates since they may not be accurate enough to be relied on alone. This article does a good job of explaining the possible positives and the possible cons if AI-powered cybersecurity were to become regularized.

Shukla, D. (2018, Sep 01). eStyle - artificial intelligence: Potential risks of artificial intelligence. *Electronics for You,* Accessed 28 Aug. 2024. Retrieved from http://mutex.gmu.edu/login?url=https://www.proquest.com/magazines/estyle-artificial-intelligence-potential-risks/docview/2099956641/se-2

This magazine from ProQuest depicts possible risks that may come from Artificial Intelligence. It's important to note that this magazine was imperative to include as it gives a better understanding of the possible negative outcomes if artificial intelligence were to become more regularized as it will make society more precautious and take steps to avoid such atrocities. The magazine notes that it can be a great risk to society if it were to end up in the wrong hands. It also mentions the possibility of Artificial Intelligence gaining sentience, thus leaving human intellect behind. One of the important risks the magazine includes AI programmed cyber-attacks and crime, which can cause numerous amounts of chaos and problems in cyberspace.

Stix, C. (2022). Artificial intelligence by any other name: A brief history of the conceptualization of "trustworthy artificial intelligence". *Discover Artificial Intelligence, 2*(1), 26. Accessed 29 Aug. 2024. Retrieved from doi:https://doi.org/10.1007/s44163-022-00041-5

This Scholarly Journal describes the overall innovations of Artificial Intelligence and how it has been increasing rapidly over the recent years. While they explain the innovations and advancements, they also mention how there has been an influx of government strategies, panels, policy papers, and efforts, regulate AI systems. This is imperative to note that as Artificial Intelligence gains more advancements over the years, it possibly may be harder for it to be controlled so having regulations can have it more controlled and contained. If these regulations and standardization continue to occur, society could trust Artificial intelligence much more than before. The journal also mentions the statement "AI for good", essentially explaining how it can benefit humanity. You can tie this into the AI-powered cybersecurity technologies as it will exponentially increase security and protection by combating cybercrime, breaches, and much more.

The artificial intelligence revolution: Will artificial intelligence serve us or replace us? (2014). *Kirkus Reviews, Lxxxii*(15) Accessed 28 Aug. 2024. Retrieved from http://mutex.gmu.edu/login?url=https://www.proquest.com/trade-journals/artificial-intelligence-revolution/docview/1548804920/se-2

This Trade Journal article is incredibly old as it is from 2014, but it still has an incredible question for its time, "will artificial intelligence serve us or replace us?". This question is interesting, yet also scary. Humanity can control their fate by ensuring there are regulations and polices with artificial intelligence. The journal mentions how computing technology doubles every 18 months. At the time of their writing, they were comparing this with computers and Artificial Intelligence, depicting how it may innovate rapidly, which it is currently. They describe three case scenarios regarding to artificial intelligence, with the first one being the worst, artificial intelligence being able to

exterminate humanity, and the best-case scenario being that humanity will continue to control the machines/AI-powered machines.

Translated by Content Engine, L. L. C. (2023, Aug 20). Artificial intelligence vs. artificial intelligence: The danger of human beings. *CE Noticias Financieras,* Accessed 28 Aug. 2024. Retrieved from http://mutex.gmu.edu/login?url=https://www.proquest.com/wire-feeds/artificial-intelligence-vs-danger-human-beings/docview/2854318882/se-2

This Wire Feed from ProQuest does a great job of explaining that Artificial Intelligence isn't the main concern, it is the humans who build them and decide on what they want them to do. The website mentions the huge influx of usage with ChatGPT and artificial intelligence, and how it is affecting society. They mention the severe powers Artificial Intelligence could possibly have if it were in the wrong hands, such as creating pathogens or even compromise critical infrastructures. Even with the many possible risks mentioned, they are all avoidable as long as the artificial intelligence does not end up in the wrong hands by regulating polices and rules while also training artificial intelligence to make sure that it is obedient to humans and does not lose control.

ULDRICH, J. (2023, Dec 04). ARTIFICIAL INTELLIGENCE: REGULATE AI LIKE HUMANITY'S FUTURE DEPENDS ON IT ; EVEN IF THE ODDS OF ARTIFICIAL INTELLIGENCE POSING AN EXISTENTIAL THREAT TO HUMANITY ARE LOW, WE MUST TAKE THAT THREAT SERIOUSLY. *Star Tribune,* Accessed 28 Aug. 2024. Retrieved from http://mutex.gmu.edu/login?url=https://www.proquest.com/newspapers/artificial-intelligence/docview/2897161473/se-2

This newspaper from the ProQuest website has the strongest tone out of all the other websites I have cited. It is strong, loud, and has an assertive manner. It makes a comparison between nuclear power and artificial intelligence, mentioning how both powers are immense and how it would be impudent if humanity were not to explore such technology. This brings up the complex counterargument against artificial intelligence, and this would be the many risks it could potentially pose towards humanity. Though the possible outcomes of artificial intelligence this website mentions are unlikely to ever occur, it is something to think about as it is not necessarily impossible for those things to occur, such as artificial intelligence taking over humanity, creating a pathogens/virus, and much more.