AI changing the world for Cybersecurity Specialists and Users; Opening Doors for Hackers

Elizabeth Simpkins

IT150G, 15631; 11 AM; Ye, Ziwei

Abstract

This paper is meant to explore the abilities that AI has given to modern-day hackers and the ways that cyber security specialists have had to deal with these new attacks. The process by which hackers have developed over time from curious hackers into sometimes lazy, AI using crackers has changed the way that attacks are developed. AI has flooded the world of cybersecurity with an uprise in cyber-attacks, due to the automated use of AI, like in DDoS attacks that can be replicated and spread over multiple computers and devices in a network. The way that security specialists have defended against attacks in the past is long gone, and the need to upgrade processes and use AI to defend, is vital to being able to keep up with AI used by hackers. Therefore, this research is meant to answer the question of how AI has made unethical hackers' jobs easier and how will it continue to help cyber security specialists solve new threats now and in the future. The prevalent use of AI has also created a demand for AI competence in users, since these new attacks will need to be looked for, and are becoming increasingly difficult to spot. AI has already become a low-level security detection software that is being used by many cybersecurity industries, but the spread to all internet-using businesses and users is important to help mitigate more attacks. AI is not fully operational by itself, however, due to information being received from the internet, it can grab incorrect information, or miss things in a typical phishing email for example, so it cannot fully replace workers in these areas. This paper will go into more detail about how hackers have been able to use AI, how it has benefitted them, and how cyber security specialists have and will continue to defend against AI hackers using AI defenders.

Introduction

Research has shown that the hot topic of AI has made increasing strides in the world of cybersecurity, but it has also helped the wrong side of this world as well, the unethical hackers. This paper is meant to stress the importance of defending against AI-based attacks like the colonial pipeline attack back in 2021, as well as smaller, but still as potentially destructive attacks like phishing attacks. The expanse of everyone that is affected by the use of AI by hackers is also stressed, as well as how much more vulnerable people are today. The progression of hackers' methods is summarized from the development of the first hackers to the hackers today with more resources at their fingertips, like AI based tools that create almost anything they want to use to fool their victims. How AI is used by hackers is also detailed in how it is accessible to them, how they use it unethically, and how they are able to target key infrastructures more often. Ai has created a lazy hacker through the use of automated DDoS attacks that can flood a system without much work done by the hacker, and this is analyzed as to how it lessens the scope of ability that the hacker needs in order to carry out more advanced attacks. How cyber security specialists have used AI to defend is researched through methods of optimized ethical hacking and other AI-based automation tools. AI has made cybersecurity a major component of business structure, because of the scope, advancement, and massive increase in AI hacking. AI is explained to be a work in progress as well, however, since it is still a baby because it has limited scope of abilities and it has to be supervised when completing tasks. It has, however, also reversed a long-standing problem that cybersecurity specialists were having: defenders dilemma. AI may become a common use of technology for protecting systems from penetration, but people will still be in the picture because we are required to analyze the hacker's process, develop new strategies, and supervise AI as it is still new. The use of AI in hacking and

in protecting systems/data has changed the world forever. Therefore, the question that this research intends to answer is how has AI has made unethical hackers' jobs easier and how will it continue to help cyber security specialists solve new threats now and in the future.

Background Information

The term hacker goes back to the 1940s and 1960s, but it was not meant as an evil term, it was meant as more of a new way to use and advance technology (HarishP, 2023). In the 2010's hackers/threat actors/unethical hackers were now a common name and hacktivists were the typical attackers at the time, which involved exposing top secret government information by groups of hackers with a cause to expose injustice or get revenge on a group (Power, 2016). Modern attacks have created limitations, like the ones in Figure 1, on the security measures that have been used to defend against cyber-attacks. With a large increase in attacks on data during the 2010s came more research to fight back against this new type of technology known as AI. Artificial intelligence is a computer that has machine learning abilities to collect data, as well as changing outcomes once it has learned from mistakes, throughout the internet in order to come up with solutions to a problem (Copeland, 2024). Today, there has been a massive spike in cyber-related attacks compared to back then. According to a strategic advisor in AI practices, named Bernard Marr, a leader in the cybersecurity field named "BlackBerry [,] reports that of the 5,200,000 cyberattacks stopped by its security solutions during the three-month period covered by its report, 62 percent of them were against critical infrastructure providers" and that the use of AI is now "being used increasingly frequently to target vital infrastructure" (Marr, 2024). Back in 2016, DEF CON held a competition for finding the best AI based tool for defending against AI based attacks and this opened the eyes Bruce Scheiner, a computer-security expert, at how AI could become a prevalent and advanced tool in the future that would be able to complete tasks

faster and more efficient than any person (Oberhaus, 2023). Cyber security specialists are using AI tools to advance their jobs in defending against hackers and their new uses for AI as well. Sticking with the current security standards will only delay the process of mitigating vulnerabilities and preventing attacks (See Figure 1).

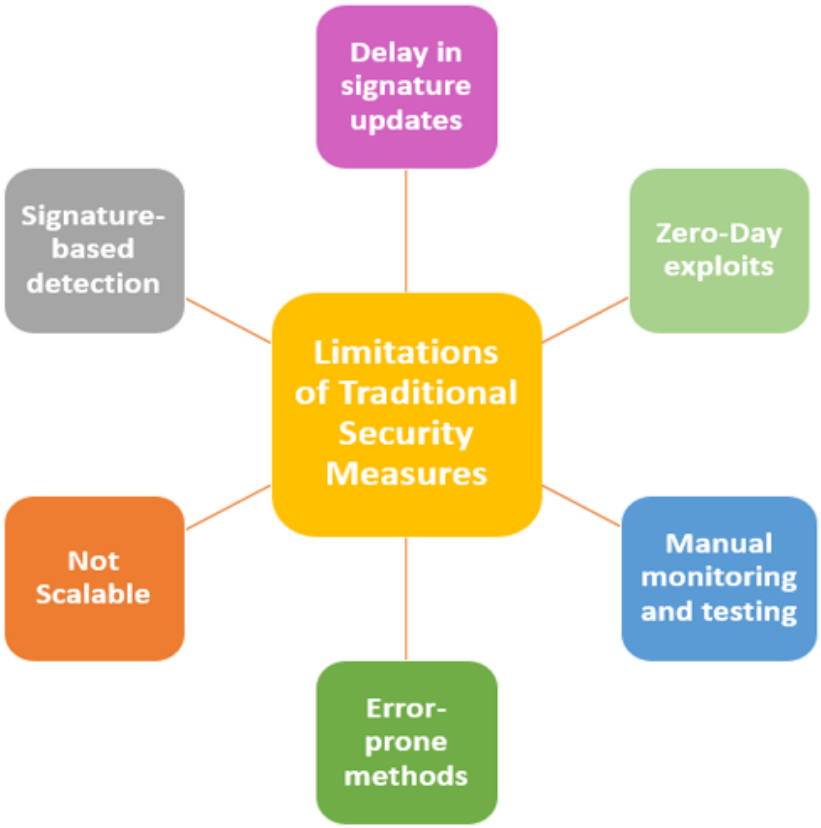

Figure 1: (Muraleedhara, 2024) This diagram shows the limitations of security when AI is not used in security systems

The Enormity Of The Situation

Recent AI based cyber-attacks have opened people's eyes to the expanding threat of AI usage in hacking. In May 2021, the colonial pipeline was hacked through a ransomware attack,

creating a ransom amount to be paid in order to gain back control of the systems. According to a *TechTarget* post, the colonial pipeline attack was a national issue due to the entire country's reliance on the oil that is transferred via this pipeline (Kerner, 2022). This attack targeted a critical infrastructure of the U.S. and therefore affected millions of people. AI was a part in making this attack more effective as described in a blog post by *esed* whom stated that the attackers known as DarkSide were able to use the access of AI and other tools to hack into an encrypt the system (Sardanyes, n.d.). The defense against attacks like this in the future is crucial to keeping other critical infrastructures safe and secure.

More people are becoming vulnerable nowadays to the expanse of AI-based attacks. According to a *ISACA* article, a Deep Instinct's fourth edition report stated that "75% of security professionals have witnessed an increase in cyberattacks this year and 85% were powered by generative AI" (Muraleedhara, 2024). The use of AI has improved the technicality and sophistication of cyber threats including attacks like phishing, malware, ransomware, deepfakes, IoT, and social engineering. Some advanced attacks with the recent addition of AI include one called vishing which is a process that hackers use to clone voices retrieved in order to fool the victim into giving information over to them ("How Hackers and Scammers", n.d.). These sorts of attacks can affect many people, especially those that don't have much knowledge about technology or the recent uses of AI. According to a study on *SageJournals*, people who have little knowledge about cybersecurity awareness, or a hacker's usage of AI, are more susceptible to being attacked online; these people are mostly older, with lower levels of education and privacy protection skills (Wang et al., 2024). With the rapid growth of cyber threats because of help from AI, it is more important, now than ever, for cyber security specialists to understand how hackers use AI so that they can come up with ways to defend using similar tactics. Also

being able to communicate these findings and prevention methods against these new attacks will help people who have little skills or knowledge in their competence with AI (See figure 2).

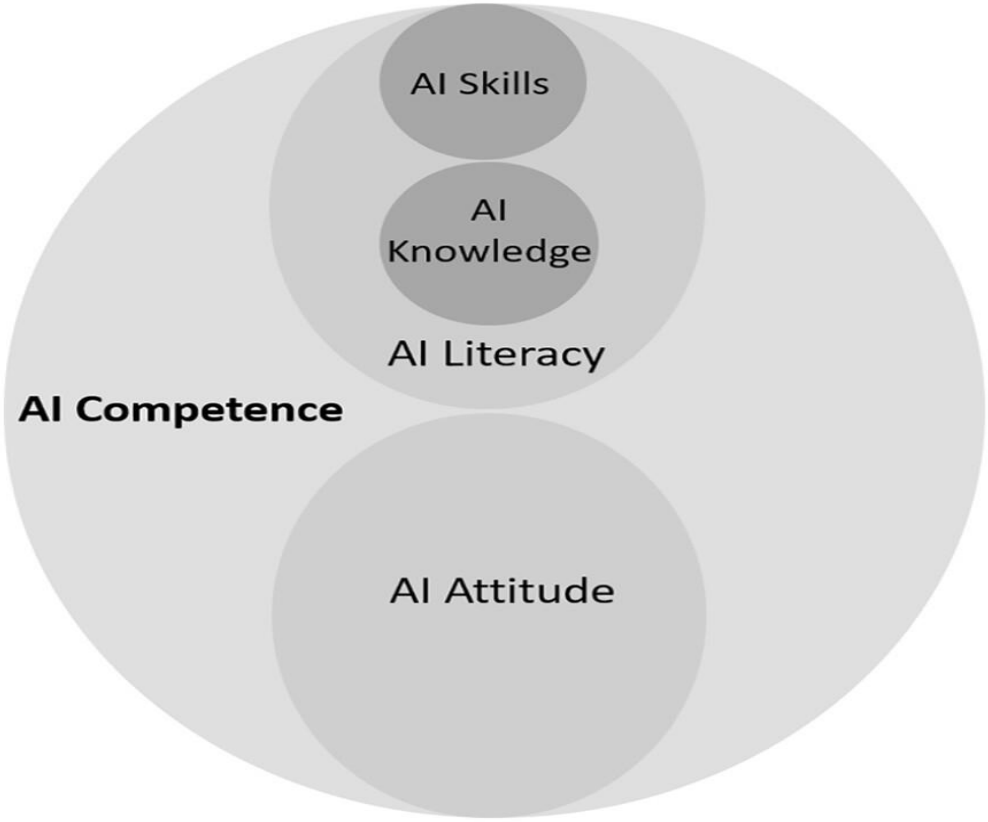

Figure 2: (Wang, et al., 2024) This diagram represents the abilities that people have relating to AI and their abilities in mitigating or protecting themselves against cyber attacks

How hackers use AI/how it has changed hackers

With AI sources creating more efficient and better execution-based outputs, comes the unethical use of hackers that have used these tools to make their plots easier. The sped-up process of using AI can help a threat actor automate their attacks by having AI repeat a process until a successful outcome is achieved, and this makes it to where the hacker has to put little effort into their attack (Seeing AI to AI, n.d.). This also creates a massive increase in the number of threat actors, since low-level hackers now have access to technology that can continuously

attempt infiltrations, with little effort from the hacker themselves. Hackers use a wide range of AI tools but according to a study about how hackers commit these attacks, hackers will use the part of AI that includes machine learning in order to avoid defenses which simply involves the hacker training the AI to repeat and process certain processes and data (Gabrian, n.d.). The whole idea of a hacker using AI technology is for them to easily move through a system through an automated process available through what AI has learned, including the commands that the hacker adds, in order to execute their mission.

The concept of a lazy hacker is created from the use of AI because automation is used for the majority of the attacks today, and only minimal execution is done by the hacker. In an interview posted on *Fierce Network,* Max Clauson states that bot-attacks are becoming more prevalent with the use of AI to create these attacks, because they are simpler to create and provide the widest attack spread with little effort (Abarinova, 2024). Low level hackers are able to infiltrate harder systems to crack because AI has created an automated process to get past security measures. According to an article on the *Georgia State University* site, AI has also created a way for hackers to make malware that can get past defenses (How Can Hackers Use, 2019). A lazy hacker is created by having automated tools like WormGPT and Chat GPT (Aash, 2024). These create an easy access for hackers to bypass security measures, and put little effort into their attacks.

How To Defend Against AI And Its Spread In Cybersecurity

In order to defend against security threats using AI, cyber security specialists have to be able to use these tools as well and be able to use what the AI gives them to determine how to handle a vulnerability, analyze whether something harder to determine, like an advanced

phishing email, is it real or not, or just make processes go faster. In an article on *Forbes*, a corporation called IBM, "is already demonstrating how AI can replace manual processes by automating incident responses—accelerating alert investigations and triage by an average of 55% as well as simplifying access for verified users and reducing the cost of fraud by up to 90%" (See Figure 3). AI based tools for cyber specialists automate the old methods of searching through data and finding vulnerabilities, or enabling things on systems to make them more secure, everything would now be automatic and more efficient due to these tools. According to a post on *GeeksforGeeks*, some of these tools include Darktrace, Cylance, Vectra AI, SentinelOne, Cybereason, McAfee MVISION, and FortiAI (Writingsnler, 2024). By looking at what a threat hacker uses and how they go about creating/executing an attack, generative AI can be used by cyber specialists to find new ways to defend against the increase/advancement in attacks by providing efficient defense.

Since cybersecurity is a very large and is interdisciplinary in nature: involving two or more academic, scientific, or artistic disciplines (interdisciplinary, n.d.), it effects a lot of people, businesses, and governments when things go wrong. The spread of AI based attacks has increased drastically and hackers are not just targeting high-risk targets, according to an article on *ceo monthly*, attacks are occurring in every industry all across the U.S. (The Role of AI in DDoS, 2024). This is because AI tools can allow hackers to repeat a step/direction until it is able to succeed by using a new tactic made by either the hacker or one created by AI through trial and error. The attacker can then flood a system with a DDoS Bot attack (See figure 3) and if it is not a known attack to the system, the cyber specialists may not be able to defend against it, which is why defensive AI is needed in order to mitigate against new types of attacks driven with AI. Since recent AI hacks have been executed and critical infrastructures have been targeted, like

power grids, food supplies, or energy sources, defensive uses of AI are needed in order to protect things that not only people in the U.S. rely on, but also products/goods/data that other countries rely on the U.S. for as well, and need protecting, creating a global issue and need.

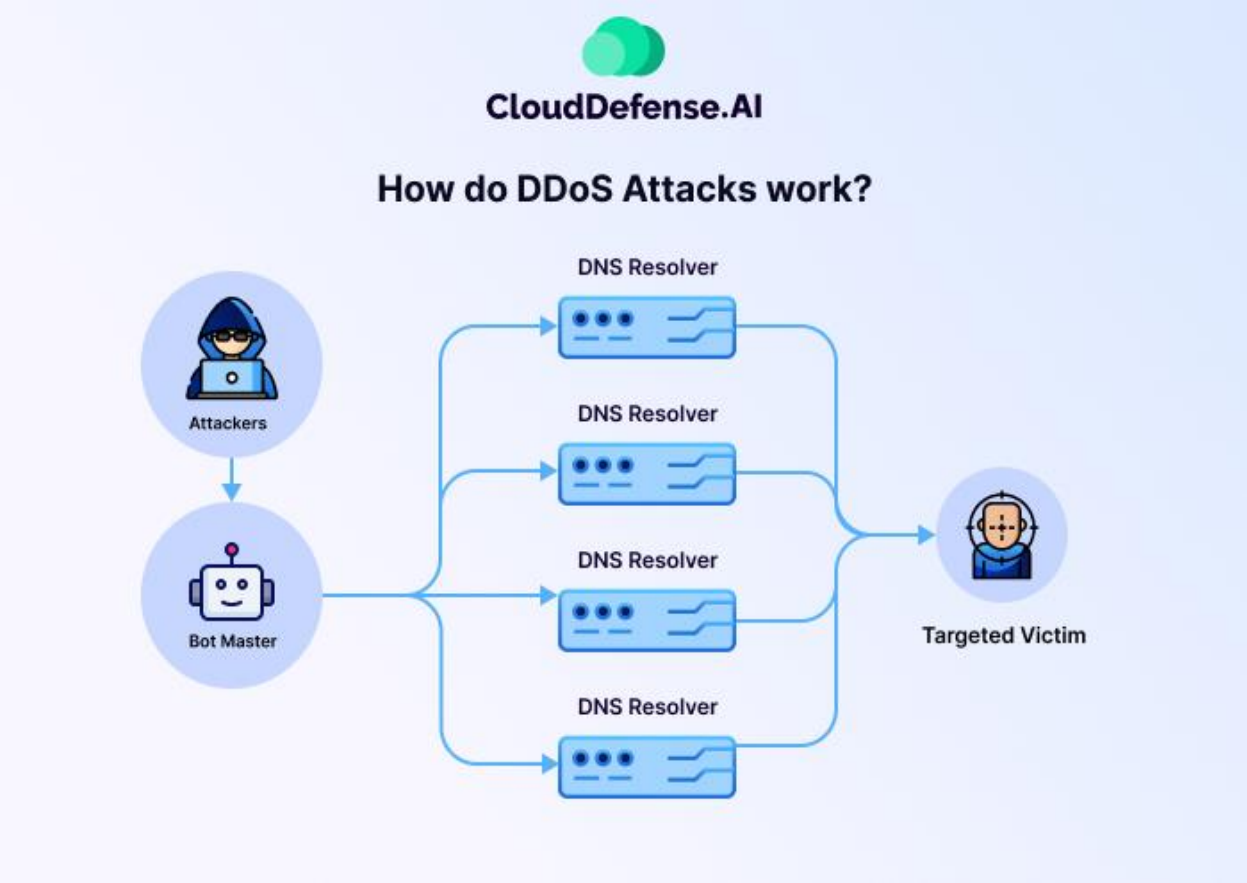

Figure 3: (Bansal, n.d.) This image is a visualization of a DDoS Bot attack that shows how the AI Bot's created can flood a system and then effect the targets who now cannot access any of their data.

AI Limitations And Accomplishments

While AI has had a lot of advancement in its usage of tools to defend against attacks, it also has limits to what it is able to do. Since AI is still fairly new, and it is not able to complete the human aspects of a cyber specialist's job, there are limits to what AI can be relied on in an industry. As discussed in an article on *towerwall,* AI used by cyber specialists will need people

to supervise the systems because AI can still get things wrong, due to pulling information from the internet, it can pull other things like generalizations or just incorrect data (Drolet, 2023). Foundational things in a company or in the public, like making sure that everyone understands how to avoid click-bait or phishing emails is also essential in order to reduce the increasing number of attacks that come into an AI defensive machine. Too much reliance on AI can also create issues like the ones listed in an article on *Relevant Software* which stated that AI cyber systems are not reliable since they do still get things wrong, they can be hacked into, changed, or not be able to solve an issue that requires a person to evaluate (Burak, 2024). A technology dominant world where AI is predominantly used to create attacks is a world where people need to know more about how they can prevent AI attacks themselves as well, so education is something that people have to disburse.

Before AI was used by cyber specialists, defenders faced an increasing problem of not being able to keep up with and defend against the attacks that people were facing. Defenders often face criticism as well for not being able to mitigate against every attack or slow the spread of them, and this is where the defender's dilemma was created. In order to solve this issue, AI can reverse the rabbit hole by helping defenders mitigate against attacks and process data quicker than any person would be able to (Walker, 2024). Since AI has been used to automatically process data, the cyber security field has had a decrease in the defender's dilemma because AI can handle the bulk of the flow of attacks while security specialists supervise and make the decisions that AI tools can't.

The future of AI

Due to the increasing use of AI in attacks and defensive tactics, it is more than likely that AI will become a common use in all cyber-related tactics for the future. The goal is for all of the cyber industry to use AI for more efficient data collection and lower-level defense. AI used across the board means that it can be implemented instead of having to pay an employee to do the same work and it can be replicated to be used for different tasks ("Seeing AI to AI", n.d.). Just because AI would be able to do these jobs, does not mean that people are completely out of the picture, however. As long as AI still has a limit on how it can interpret data/attacks, based on the fact that it can't determine things that only a human would be able to decide upon, it will always need a supervisor to watch it work. This is why people will be needed to solve the problems that AI can't determine. In a Forbes article, the author says that they "predict that AI will heavily support (if not replace) manual work in areas like data collection, analytics, risk assessment, audits, cybersecurity operations and even the design of cybersecurity architectures" (Dimitriadis, 2024). This is because AI can do all of the manual sorting/collecting of data points and industries won't need to hire someone to do these jobs anymore because AI can do it faster without human error, but AI still requires supervision for things like human factors that the computer can't determine. Human factors can include determining why a hacker would use a certain type of attack, or decide to attack at all, deciding whether something should be flagged or not based on other circumstances that AI may not be able to see, and AI can be tricked and therefore does get things wrong from time to time, so people have to be present in order to catch things like this (What AI Can, 2023). This is why AI can't be fully reliant upon now or in the future because of this human element, but it can be expanded upon to make industries more efficient.

The advances of AI in attacks and in the security, sector have changed the way the world sees cybersecurity, as an absolute need for industries and companies for protection. Attacks using AI have, alone, created a major concern for world-wide industries. U.S. companies have to deal with ransomware that is now more frequent and more expensive due to the technical achievements of AI attacks. According to a technology company interviewed on an article form *Fierce Network*, the "average cost of an attack in the first half of 2024 was *$6,000* per minute, while the average attack lasted 45 minutes" (Abarinova, 2024). The security sector has seen a massive increase for the need to use AI in order to defend against these attacks as well. Without using AI, defenders would not be able to keep up with the ever-changing attacks that today's hackers use.

Conclusion

In response to the beginning question, AI has made a hacker's job much easier through several resources provided to them. An unethical hacker is able to use AI tools to replicate attacks until they are extremely advanced and hard to even detect that they are there, even by other AI systems. The use of AI for attacks has also increased the sophistication and number of attacks that are seen every day. Through this use, however, hackers can be seen as lazy, to a point, because many low-level hackers with little knowledge in hacking are able to use AI for harder processes and apply minimal effort in their attacks. This also increases the number of attacks that people are seeing as well. While this would create an overflow of data that is being sent to cybersecurity specialist to sort through, the defensive team is now using AI as well to combat these large amounts of information. It is used as a tool to defend against the large number of attacks and it takes over certain data collecting/analyzing positions, but does not replace them since it must be supervised in order for people still apply the needed human-based decision

making, like determine whether there may be other factors outside of what a computer can see. Of course, AI having faults does not mean that it can't improve them since it has machine learning, meaning that even if it gets things wrong one time, it learns from itself and other AI programs on what to look for in attacks/data. For the future, AI will more than likely become a general automated tool for sorting through data and solving low-level attacks. It may even become something that people can install on their computers to defend against viruses, malware, and phishing attacks. Just like the example from the DEF CON AI battle, the future may be just that, AI vs. AI, which one can infiltrate or defend the best, and possibly not need to be supervised?

References

Aash, P. (2024, March 11). *Dark AI: Top 7 AI tools assisting hackers*. ciso platform. Retrieved October 25, 2024, from https://www.cisoplatform.com/profiles/blogs/dark-ai-top-7-ai-tools-assisting-hackers

Abarinova, M. (2024, August 16). *AI is the latest weapon for DDoS attacks*. FIERCE Network. Retrieved October 25, 2024, from https://www.fierce-network.com/cloud/ai-latest-weapon-ddos-attacks

Bansal, A. (n.d.). This image is a visualization of a DDoS Bot attack that shows how the AI Bot's created can flood a system and then effect the targets who now cannot access any of their data. [Image]. https://www.clouddefense.ai/ddos-attacks/

Burak, A. (2024, July 30). *AI in cybersecurity examples: How technologies can protect the digital world*. RELEVANT SOFTWARE. Retrieved October 25, 2024, from https://relevant.software/blog/ai-in-cybersecurity-examples/

Copeland, B.J. (2024, October 25). *Artificial intelligence*. Britannica. Retrieved September 21, 2024, from https://www.britannica.com/technology/artificial-intelligence

Dimitriadis, C. (2024, July 3). *The Future of The Cybersecurity Profession with The Rise Of AI*. Forbes. Retrieved September 20, 2024, from https://www.forbes.com/councils/forbestechcouncil/2024/07/03/the-future-of-the-cybersecurity-profession-with-the-rise-of-ai/#:~:text=AI%20will%20reshape%20many%20cybersecurity,of%20AI%20itself%20while%20applying

Drolet, M. (2023, September 10). Will AI rib the need for cybersecurity experts and service providers? t*owerwall*. Retrieved from https://towerwall.com/will-ai-rid-the-need-for-cybersecurity-experts-and-service-providers/

Gabrian, C.A. (2024). Unveiling the dark side: How hackers exploit Artificial Intelligence for cyber warfare. *Euro-Atlantic Resilience Journal 2*(3). https://resiliencejournal.e-arc.ro/wp-content/uploads/2024/06/EARJ-3-2024-Gabrian.pdf

HarishP, A. (2023, March 5). *The history of hacking and evolution of hacking*. LinkedIn. Retrieved October 24, 2024, from https://www.linkedin.com/pulse/history-hacking-evolution-ashwin-harish-p

How can hackers use machine learning? (October 24, 2019). Georgia State University. https://ebcs.gsu.edu/2019/10/24/how-can-hackers-use-machine-learning/

How hackers and scammers use AI (Artificial Intelligence). (n.d.). Cyber Seniors. Retrieved October 25, 2024, from https://cyberseniors.org/uncategorized/how-hackers-and-scammers-use-ai-artificial-intelligence/

interdisciplinary. (n.d.). In *Merriam Webster dictionary*. Retrieved from https://www.merriam-webster.com/dictionary/interdisciplinary

Kerner, S.M. (2022, April 26). *Colonial pipeline hack explained: Everything you need to know*. TechTarget. Retrieved October 25, 2024, from https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know

Marr, B. (2024, May 17). *How AI is changing the world of cybersecurity*. LinkedIn. Retrieved September 21, 2024, from https://www.linkedin.com/pulse/how-ai-changing-world-cybersecurity-bernard-marr-aso2e

Muraleedhara, P. (2024, April 23). *The need for AI-powered cybersecurity to tackle AI-driven cyberattacks*. ISACA. Retrieved September 20, 2024, from https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2024/the-need-for-ai-powered-cybersecurity-to-tackle-ai-driven-cyberattacks

Oberhaus, D. (2023, March-April). *Prepare for AI hackers*. HARVARD MAGAZINE. Retrieved September 20, 2024, from https://www.harvardmagazine.com/2023/02/right-now-ai-hacking

Power, K. (2016, August 17). *The evolution of hacking*. FORTRA Tripwire Integrity Management. Retrieved October 25, 2024, from https://www.tripwire.com/state-of-security/the-evolution-of-hacking

Sardanyes, E. (n.d.). *Examples of cyberattacks launched with Artificial Intelligence*. esed. Retrieved October 25, 2024, from https://www.esedsl.com/en/blog/examples-cyberattacks-launched-with-artificial-intelligence

Seeing AI to AI: Artificial Intelligence and its impact on cybersecurity. (n.d.). NEW JERSEY CYBERSECURITY & COMMUNICATIONS INTEGRATION CELL. Retrieved September 21, 2024, from https://www.cyber.nj.gov/guidance-and-best-practices/artificial-intelligence/seeing-ai-to-ai-artificial-intelligence-and-its-impact-on-cybersecurity

The role of AI in DDoS detection and mitigation. (2024, June 3). ceo monthly. Retrieved October 25, 2024, from https://www.ceo-review.com/the-role-of-ai-in-ddos-detection-and-mitigation/

Walker, K. (2024, April 24). *Cybersecurity: Past, present, and the AI future*. LinkedIn. Retrieved September 21, 2024, from https://www.linkedin.com/pulse/cybersecurity-past-present-ai-future-kent-walker-s3idc

Wang, C., Boerman, S.C., Kroon, A.C., Moller, J., & Vreese, C.H. (2024). The artificial intelligence divide: Who is the most vulnerable? *New Media & Society 26*(11). https://doi.org/10.1177/14614448241232345

What AI can-and can't-do for cybersecurity. (2023, November 20). digital silence. Retrieved October 25, 2024, from https://digitalsilence.com/what-ai-can-and-cant-do-for-cybersecurity/

writingsnler. (2024, March 3). *Top 7 AI tools for cybersecurity in 2024*. GeeksforGeeks. Retrieved October 25, 2024, from https://www.geeksforgeeks.org/ai-tools-for-cybersecurity/