HIGH SCHOOL EDITION
Journal of Student Research
Volume 13 Issue 2 (2024)

Impact of AI and Generative AI in Transforming Cybersecurity

Kadhir V. Palani[1], Jothsna Kethar[#], Sarada Prasad[#] and Virgel Torremocha[#]

[#]Advisor

ABSTRACT

In the constantly expanding field of cybersecurity, Artificial Intelligence (AI), and more specifically Generative Artificial Intelligence (GenAI) impacts every aspect of the cybersecurity landscape. In today's world, most manual transactions, interactions, and records have become digital, generating vast amounts of valuable data. Many devices are connected by various private or public networks to the Internet known as the Internet of Things(IoT). This has led to many incidents where users and organizations have been targeted for Fraud, data theft, and disruption to businesses among other challenges. AI-based tools play a key role in defending against cyber attacks rapidly and effectively, due to their ability to analyze large volumes of data in real time. GenAI models can continuously learn and adapt, thus proactively assisting with cyber defense. For digital users and entities, this can help protect data, reduce incidents of Fraud, and model threats, keep systems safe, and mitigate other risks. The applications of GenAI however do not extend just to the defense of systems, they can also be used to increase cybersecurity threats. Malicious actors might use covert methods to manipulate data, attack systems, avoid malware detection, and spread harmful or incorrect information. This paper will detail how AI is a double-edged sword in cyber security, providing proactive and increasingly rapid and efficient ways to enhance cyber defense, as well as its use in newer and more damaging threats. It also aims to bring awareness of regulatory and other impacts on society.

Introduction

Cybersecurity is a rapidly evolving area with attacks becoming increasingly more sophisticated and damaging. The integration of Artificial Intelligence (AI) and more specifically Generative Artificial Intelligence (GenAI) emerges as a critical advantage in strengthening digital defenses in the fight against cyber threats. This research looks at the multifaceted role of AI in reshaping the security landscape. The exponential growth of digital data and the interconnected nature of modern systems create a huge challenge for traditional cybersecurity measures. The Internet of Things (IoT) has expanded exponentially in this digital age (Rosencrance, 2021), providing malicious hackers more opportunities to attack critical systems. Thus there is an urgent need for a rapid automated response to cyber attacks. Due to its ability to analyze vast datasets, recognize patterns, and adapt in real time, AI offers a radically new approach to threat detection and mitigation. This paper aims to explore the key applications of AI in cybersecurity, ranging from anomaly detection, and AI-powered Intrusion Detection Systems (Sowmya, et al, 2023), to behavior analysis and threat modeling, and automated response mechanisms (Parmar, 2023).

Overall, this paper aims to serve as a comprehensive guide to the dynamic landscape where AI intersects with cybersecurity. By examining the current state of Generative AI in cybersecurity, exploring its applications, and addressing ethical implications, this paper aims to provide insights into the transformative potential of AI in enhancing cybersecurity applications, while also calling attention to some challenges posed by AI. Various cyber defense and offense mechanisms and other regulatory, legal, and ethical impacts of AI are also discussed to provide a better awareness of the impacts of GenAI and other AI technologies in Cyber security.

Methods

For this paper, I used the exploratory method to get detailed information about different AI technologies and cybersecurity concepts, along with emerging trends in each area. I then explored numerous articles and videos to get a detailed understanding of the current uses of AI to enhance cyber defense or increase malicious threats. Exploring emerging trends in cybersecurity through the use of AI technologies helped with understanding the impact of these advances on society and also the regulatory, legal, and ethical implications that are already beginning to emerge. Throughout this process, I explored advancements in the field of AI in general coupled with the use of Generative AI and other AI tools in cybersecurity to show patterns of increasing AI and GenAI usage in cybersecurity.

Overview of AI in Cybersecurity

Artificial Intelligence has established the critical role it plays in cybersecurity over the past many years. With the recent advent of GenAI, there is now greater effectiveness in proactively identifying threat patterns, quickly detecting the most critical threats, and enabling rapid and automated responses to mitigate the impact of threats. At the same time, there are more opportunities to use these capabilities to cause more damage. Thus, there is a great focus in the Security market on rapidly enhancing the use of GenAI to fortify cybersecurity defenses.

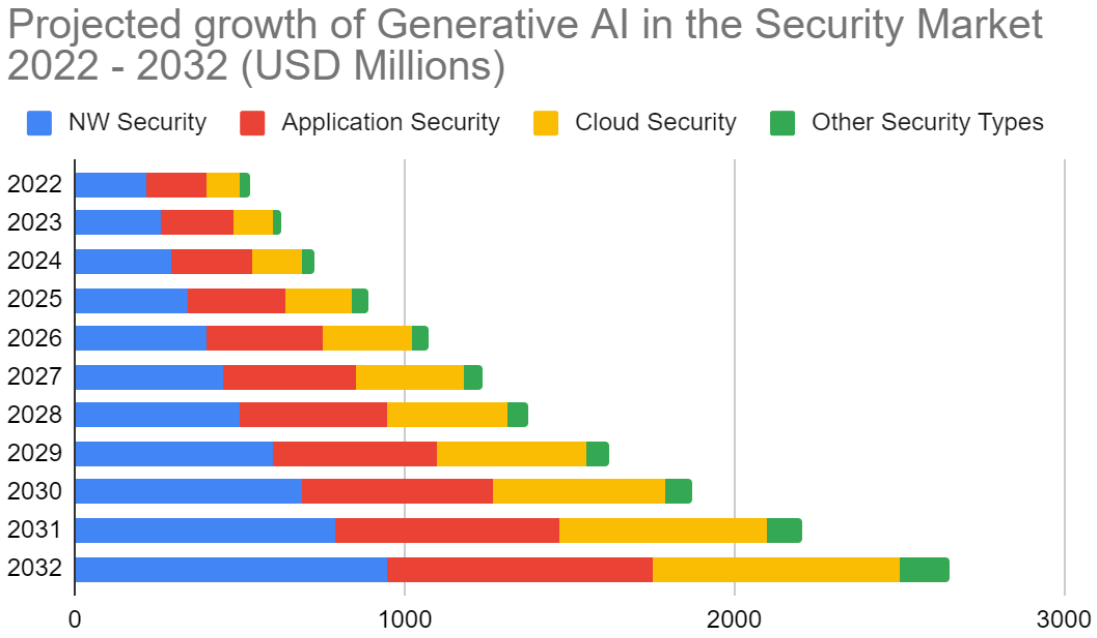

Figure 1. Generative AI in the Security Market (Kadhir, 2024).

This figure shows the projected growth of Generative AI in cybersecurity in the period 2022-2032, it also shows where Generative AI is going to be used the most in the various areas of cybersecurity such as Network Security, Application Security, Cloud Security, and other Security types (Security data obtained from Lea, 2023).

Under the broad umbrella of Artificial Intelligence, Generative Artificial Intelligence (GenAI) and Large Language Models (LLMs) like ChatGPT, LLama, Gemini, etc. have enabled a variety of advanced capabilities in cybersecurity. However, this has also enabled greater sophistication and an increase in the type and scale of cyber threats. AI in cybersecurity is indeed a double-edged sword (Ali, et al., 2023). The very nature of GenAI and its need for large quantities of data is also driving the need for a variety of social, ethical, and legal considerations.

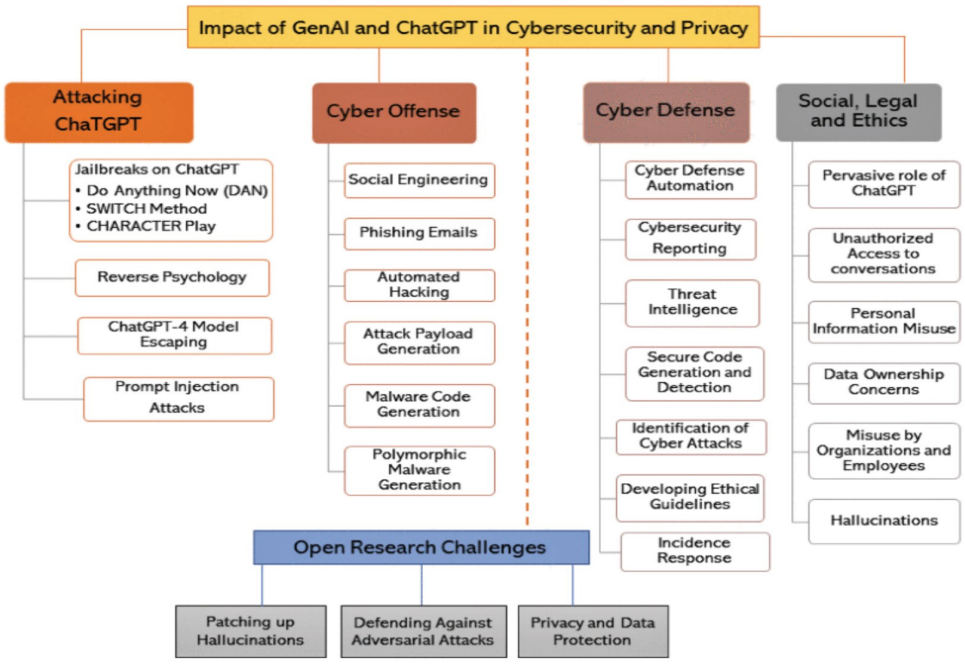

Figure 2. Cybersecurity and Generative AI

This image shows how Generative AI tools like ChatGPT can be used in various applications to achieve different goals such as in cyber Offense and cyber Defense while also showing the social, legal, and ethical problems with GenAI tools such as ChatGPT(Gupta et al., 2023).

Advantages of AI and Generative AI in Cybersecurity

Enhanced Cyber Defense Mechanisms - Threat Modeling

Before the use of AI, traditional cyber defense mechanisms were primarily reactive and limited in their ability to anticipate and prepare for different types and scales of attacks. Integrating Generative AI into cyber defense mechanisms to simulate various attack scenarios allows for enhanced threat modeling. Threat modeling is a term used to describe how risks and threats can be analyzed and detected and how the administrators should react to the threat if it happens, to mitigate the damage (Drake, n.d). This approach enables the identification of

vulnerabilities proactively by simulating advanced and evolving cyber threats. Some practical applications of threat modeling are in addressing phishing attacks, which are a continually evolving threat. Some other practical applications of AI in threat modeling could be to model Distributed Denial of Service (DDoS) attacks on systems to enable AI to detect patterns preceding these attacks, thus allowing for rapid response. Ashwin Krishnan(2023) illustrates how an AI model can be trained to generate phishing emails in a controlled environment, enabling cybersecurity systems to learn and recognize the changing characteristics of phishing emails. This dynamic learning process enables cybersecurity systems to be better prepared to rapidly identify and neutralize threats posed by malicious hackers. Another application is in safeguarding LLMs themselves from being exploited by employing data poisoning. This would cause them to generate and share incorrect information with users. By constantly monitoring large volumes of data in real-time, AI can identify patterns that are indicative of potential or future threats, and also by studying large volumes of past data around cyber incidents, AI can help forecast emerging patterns of threats (Goundar, 2023).

The strategic shift in cyber defense methodology is moving towards the concept of using AI to "fight fire with fire". This involves leveraging advanced technologies similar to those used by cyber attackers, thereby better understanding and counteracting their methods. Ambika Choudhary (2023) also emphasizes the potential reduction in successful cyber attacks through the use of Generative AI-driven simulations and threat modeling. Organizations can develop a nuanced understanding of potential threats, leading to the creation of more effective defense mechanisms tailored to counter specific types of attacks.

Automated Threat Detection and Response

Enhanced threat detection is important for organizations that have valuable online assets because of its ability to quickly respond to cyber threats of various types, which maintains trust among stakeholders, clients, and the public. Generative AI serves as a mixed cybersecurity tool with the capability to automate both threat detection and response mechanisms as well as threat modeling. Using advanced algorithms, AI conducts real-time analysis of extensive network data, focusing on identifying anomalous behavior indicative of potential breaches. This analytical ability extends to various threat categories, including Distributed Denial of Service (DDoS) attacks, malware infections, and unauthorized access attempts. In the realm of network traffic analysis, Generative AI algorithms play a pivotal role by continuously analyzing data flows. The system's ability to discern abnormalities by the identification of subtle indicators through real-time analysis enhances the detection of potential threats (Ali & Ford, 2023), contributing to a proactive defense against emerging cyber risks. AI-based Intrusion Detection Systems (IDS) enable improved threat detection accuracy, reduce false positives, enable faster response, and have the advantage of enhanced adaptability to emerging threats (Utilities One, 2023).

In the event of a threat being detected, GenAI is instrumental in generating rapid responses to mitigate the impact of the attack. For instance, in the case of a DDoS attack, the AI system can swiftly redistribute network traffic, minimizing downtime and preserving operational continuity. This automated response extends to other scenarios, wherein AI can autonomously block malicious traffic or isolate infected systems, curbing the progression of the attack and preventing further damage. These abilities are especially emphasized in Sowmya, T. and Mary Anita's (2023) article, detailing how AI, deep learning, and machine learning can be used to protect various systems, cloud infrastructure, and more because of the intrinsic ability of many different algorithms of AI to learn from large inputs of varied data and generate new tailored responses to cyberattacks. One of the key strengths of Generative AI, however, lies in its capacity to tailor security solutions to the specific needs of an organization. This entails leveraging AI to innovate new malware detection techniques, enhancing the organization's ability to identify and neutralize evolving threats.

Additionally, AI-driven efforts in creating more robust authentication systems contribute to fortifying access controls, reducing the vulnerability surface. This tailored approach to cybersecurity is particularly advantageous in navigating the dynamic threat landscape. By continuously adapting and evolving security

measures, organizations employing Generative AI can significantly reduce the risk of successful cyber attacks. The automated detection and response capabilities of AI not only enhance overall security postures but also minimize the potential impact of attacks, showcasing the strategic importance of GenAI in modern cybersecurity paradigms.

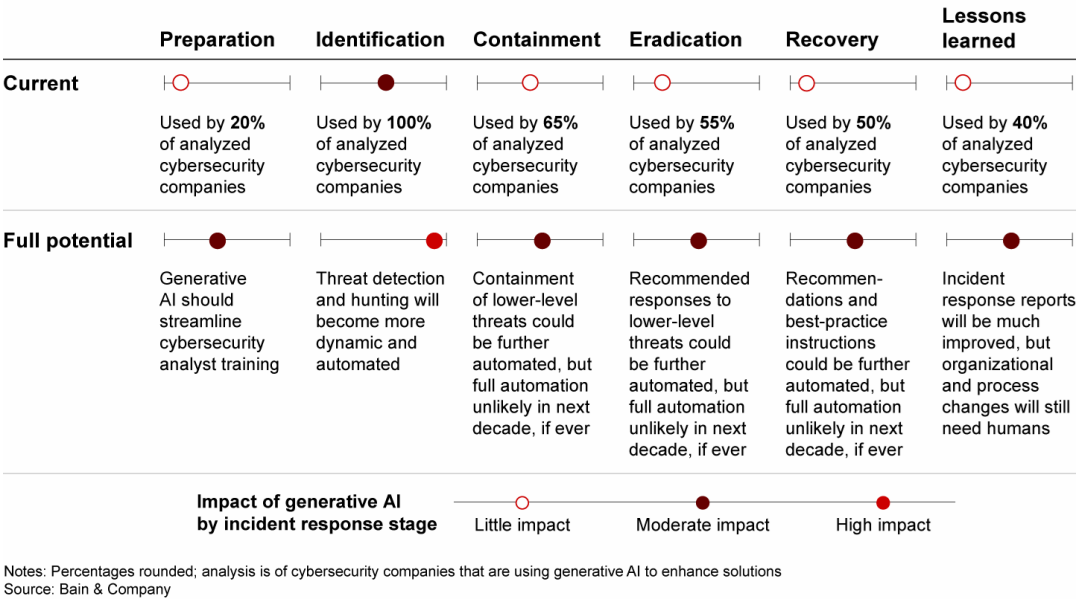

Figure 3. Threat identification holds the most potential for Generative AI to improve cybersecurity—and that's where industry adoption has been strongest so far (Ali, et al., 2023).

Personalized Security Protocols

Based on their requirements, users use digital tools and websites differently. AI can be used to customize security protocols for different user requirements thus minimizing risk. Machine learning (ML) is used to understand basic user behavior patterns. This training process involves ML algorithms being trained using historical user and network data to recognize and adapt to the regular activities of users. The acquired knowledge is then utilized to tailor security protocols to the specific needs of each type of user. For instance, a user with frequent access to sensitive data might be mandated to use two-factor authentication. In contrast, a user with less sensitive data access may not require such stringent measures. As detailed in Ilia Tivin's (2023) article, having personalized security protocols can be more effective in preventing threats.

Moreover, AI can detect anomalies or deviations from normal user behavior. This involves continuous monitoring of user actions, and if there is a sudden and significant change, it could be an indication of a potential security threat. For example, a sudden increase in accessing sensitive data might signal a security breach. AI plays a crucial role in monitoring and flagging such suspicious activities. Another example is using AI for Fraud detection in credit card usage (Digitalocean.com, n.d.). Unlike traditional one-size-fits-all security measures, AI allows for adaptability and responsiveness to individual user behaviors. This dynamic approach is particularly beneficial in enhancing overall cybersecurity, as it tailors security measures to the specific needs and activities of users, providing a more effective defense against potential threats.

AI Threats and Challenges in Cybersecurity

Data Privacy, Deepfakes, and Information Manipulation

The use of extremely large volumes of data to train various GenAI models has heightened concerns regarding data privacy within the cybersecurity domain. These large datasets frequently encompass sensitive information, including personal, financial, and health data. This data is often collected and used without the knowledge or consent of users. The inadequately protected nature of this data renders it susceptible to exploitation for malicious purposes, including identity theft, fraud, and financial scams. In addition to the potential for data misuse, another formidable risk is the creation of 'Deepfakes'. Deepfakes are crafted through advanced AI methodologies such as Generative Adversarial Networks (GANs) and pose a significant risk due to their ability to fabricate highly realistic videos, images, or audio content. This manipulated content can be exploited to spread misinformation, fuel propaganda, financial fraud, and geopolitical tensions, and impersonate and tarnish the reputations of targeted individuals. An example is a deepfake of Volodymyr Zelensky which portrayed him telling his soldiers to surrender and lay down their arms (Allyn, 2022). If such misinformation is allowed to spread without proper regulations or laws, it could lead to mistrust in society due to a lack of reliable sources of information. Central to this technology is its ability to reproduce human expressions and speech nuances that make it challenging to differentiate it from authentic content. Here, the threat landscape expands beyond conventional cybersecurity domains and extends to data privacy, information integrity, and digital identity verification.

In order to mitigate this risk, sophisticated AI-driven systems specifically designed to detect subtle anomalies within digital media that may signify manipulation, will need to be integrated into existing cybersecurity frameworks. This defense strategy will need to be supplemented by organizational preparedness, requiring comprehensive employee training on the intricacies and risks associated with deepfakes. The adoption of such comprehensive measures is indispensable not only for fortifying information security but also for upholding the credibility of digital communications in an era increasingly dominated by the proliferation of AI-generated content (Chukwube, 2023).

AI in Cyber Warfare

Perhaps one of the earliest cyberweapons in history (Fruhlinger, 2022), the Stuxnet attack which successfully infiltrated Iranian nuclear facilities, caused over $500 billion in damages according to Kenneth Okereafor & Co. (2020). This example shows the huge potential for damage by cyberattacks which can grow and expand past their original purpose. Stuxnet showcased how a meticulously crafted malicious software entity could infiltrate and inflict substantial damage upon an industrial control system. With the integration of advanced AI capabilities, newer cyberattacks may have heightened sophistication with the potential to elude detection more effectively and dynamically adapt to defensive measures in real time. In the age of cyber warfare, AI emerges as a potent tool, due to its capacity for algorithmic sophistication and pattern generation.

DeepLocker, Mirai, and Mylobot are examples of sophisticated, resilient, and persistent AI-powered malware (Armin, 2023). Mylobot is a very resilient malware that adapts its attack and evades detection by using AI techniques to analyze system behavior. Mirai created a massive botnet by utilizing AI techniques to detect and infect vulnerable IoT devices like Routers and Cameras. It then used them to launch Distributed Denial of Service attacks (DDOS) attacks. These attacks overwhelm websites with huge volumes of traffic and bring them down. The potential impact of AI-driven attacks on critical infrastructure and systems crucial for society to function is a huge concern. These could be power grids, water supply systems, communication networks, and financial systems. Cyber-attacks on such critical infrastructure can cause widespread disruptions, economic ramifications, and, in extreme cases, potential loss of life depending upon the severity and scope of the assault.

An even bigger concern is the potential ability of these cyber weapons to learn and evolve independently using advances in AI. In this scenario, these weapons would be able to identify new targets, devise

novel methods of attack, and modify their code autonomously to evade detection, all without human intervention. Such autonomous and adaptive AI-driven cyber-weapons make it more challenging for nations to counter these evolving threats.

Need for Robust Security of AI/ML Systems

As our dependence on AI increases, the security associated with AI systems emerges as a major concern, necessitating a deep understanding of potential threats and vulnerabilities. Adversarial attempts to manipulate AI algorithms through sophisticated techniques such as data poisoning and model evasion pose substantial risks. There is thus a critical need to strengthen the integrity of AI models to prevent them from becoming a vulnerability in cybersecurity defenses. Data poisoning, a form of attack, involves the introduction of malicious data into training datasets to induce the AI model to learn incorrect or biased patterns (Menon, 2023). This covert manipulation can lead to the AI model making erroneous predictions or undertaking actions detrimental to users. Adversaries leverage data poisoning to exploit vulnerabilities within AI systems, causing potential havoc in applications like facial recognition or fraud detection, where compromised models may misidentify individuals or overlook fraudulent transactions.

Additionally, model evasion represents a distinct threat vector wherein adversaries craft inputs with the intent to deceive the AI model into making inaccurate predictions (Ivezic, 2023). This is achieved by meticulously constructing inputs that closely mimic legitimate data but incorporate subtle variations avoiding detection by the AI model. The malevolent utilization of model evasion could enable adversaries to bypass AI-powered security systems or induce errors in AI-powered autonomous vehicles, potentially leading to hazardous situations.

To strengthen the integrity of AI models and mitigate these sophisticated threats, a multifaceted approach is required. Safeguarding training datasets from tampering is critical, necessitating robust mechanisms to detect and neutralize any attempts at data poisoning. It is also critical to develop AI models resilient to evasion attacks. This involves the implementation of advanced techniques such as adversarial training and robust optimization to enhance model robustness. By guarding against these kinds of attacks, the security of AI systems can be significantly improved, reducing the risks of misidentification, erroneous predictions, and potential exploitation of AI-powered applications within the cybersecurity landscape. This in turn helps generate trust among users and stakeholders (Waller, 2023).

Other Impacts of AI on Cybersecurity

Training and Education for AI in Cybersecurity

This rapid change in technological capabilities necessitates revamping the required skills for cybersecurity professionals with an additional key focus on AI technologies. Significant changes will be required to educational curriculum and other training programs for all individuals, institutions, and organizations associated with Cybersecurity. In addition to teaching technical proficiencies in AI, such as Machine Learning(ML) and Natural Language Processing(NLP), any training must ensure a good comprehension of the ethical and legal challenges specific to AI applications including compliance with data privacy regulations. AI can itself be used to tailor training programs to be most effective based on the user (Pires, 2024). Students must be aware of the potential scenarios where it can be exploited for malicious purposes, such as the creation of deepfakes or the development of autonomous weapons systems. Active hands-on engagement in real-world projects becomes critical (Hughes, 2024), involving the development of AI-powered security tools or the execution of comprehensive security

audits on AI systems. Adopting a multifaceted educational approach that integrates technical, ethical, and practical dimensions of AI cybersecurity, will create a cadre of well-trained cybersecurity professionals who can confront the wide variety of challenges inherent in the AI-centric landscape. Various government organizations are already investing in such training programs (Bracken, 2023).

Challenges in Legal and Ethical Frameworks

The use of GenAI in the realm of cybersecurity leads to many legal and ethical dilemmas. Conventional legal frameworks, which are tailored for human actors, are not equipped to deal with AI-executed cyber attacks. Determining the culprit becomes more difficult when AI operates autonomously and generates legal ambiguity surrounding these attacks. The ethical responsibilities of creators and users of GenAI are now coming under scrutiny (Prasad, 2024). In order to deal with these challenges, the legal framework will need to be modified to include new regulations and standards governing AI development and deployment in cybersecurity. Guidelines for data usage, defining AI training methodologies, and delimiting the scope of autonomous decision-making will be necessary. Given the inherently global nature of cybersecurity threats, international collaboration is critical in the development of these legal frameworks. To stay relevant, the legal system will need to adapt and continuously evolve to effectively address any new challenges introduced by GenAI in the domain of cybersecurity.

At the same time, ethical considerations in deploying GenAI for preemptive cyber defense measures require close attention. Utilizing AI for monitoring and defense introduces the potential for invasive surveillance, causing substantial privacy concerns. Ethical concerns arise from the autonomous response capabilities of AI systems, including the risks associated with false positives and unintended consequences. Robust ethical guidelines and accountability mechanisms will need to be established to govern AI behavior in the realm of cybersecurity. Striking a balance between the need for security and the preservation of individual privacy rights while mitigating the potential for AI overreach becomes critical. Strong ethical regulations from regulatory bodies will be required to create ethical and safe Cybersecurity applications using AI (Limaj 2023).

The Role of Government and Regulatory Bodies

Given that AI impacts not just technology, but also society, politics, industry, and economies, governments and international regulatory entities are already paying close attention to the extensive new capabilities unleashed by AI (including ChatGPT and other new GenAI models). The US and Europe have started to explore regulations to manage both the positive and the negative impacts of AI, proactively. The White House has recently announced an executive order to examine and address the current and long-term risks of AI. Individual governments, while addressing local requirements, must also join together to come up with a global, multifaceted approach to manage the use of AI technologies with a focus on responsibility and ethics to ensure their safety for public use. Key issues such as data privacy, security protocols, and the ethical deployment of AI must be addressed by these regulatory bodies (Conference-board.org, 2023). There need to be mechanisms in place to not only ensure compliance with established standards but also that are actively diligent against any potential misuse or discrimination. Specifically, there needs to be robust mechanisms for auditing and verifying AI systems at various stages of AI development, to avoid discrimination against individuals or groups (Farley, 2024).

Conclusion

Advances in AI and GenAI are causing a paradigm shift in all aspects of our lives today and the impact on society is tremendous. While AI is being used to exponentially enhance cybersecurity defense, malicious actors

also leverage it to generate even more damaging threats and challenges. Online data generated by individuals and businesses in a variety of ways both directly and indirectly is used to power GenAI, which is then used as a double-edged sword to impact society at large. As digital citizens who are directly or indirectly impacted by these malicious actions, having a good understanding of AI, understanding risks and its capabilities and a general idea of future trends is essential for everyone.

This paper serves to provide an overview of AI technologies in cybersecurity and emerging trends in this area. Awareness of the various other current and potential impacts on society - government regulations, legal and ethical aspects is also important as they could impact everyone. In addition to cybersecurity initiatives in organizations, it is also important for individuals to understand these emerging trends. With greater awareness and training, individuals will learn to use the internet securely and keep their data safe, while also learning to safeguard themselves against threats and manipulations of different types like phishing, deepfakes, scam calls, and more. Readers should additionally make every effort to keep up with advances in this field to ensure they can take action to minimize risk to themselves, their businesses, and society at large.

Acknowledgment

I would like to thank Dr. Sarada Prasad for his guidance during my research and for helping me get a better understanding of the vast field of cybersecurity. I also thank Prof. Virgel Torremocha and Ms. Jothsna Kethar for their overall support and guidance in writing my first research paper.

Limitations

While this paper encompasses many different aspects of AI and Generative AI in cybersecurity, this is a fast-developing field and there are new tools and capabilities powered by AI that are emerging every day. Because of this, much of the data and parameters used in constructing this research paper could change in the near future. The focus of this research paper is to provide a general overview of various key impacts of the use of AI in cybersecurity. Due to the vastness of this area and the speed of technological advances, a reader interested in understanding in-depth any of the topics referenced in this paper, will need to use this as a starting point to do additional research on the desired topic. However, this paper still serves as a comprehensive guide to novices exploring the digital landscape of AI in Cybersecurity.

References

Ali S, Ford F. (2023, Sept18) bain.com Generative AI and Cybersecurity: Strengthening Both Defenses and Threats https://www.bain.com/insights/generative-ai-and-cybersecurity-strengthening-both-defenses-and-threats-tech-report-2023/

Allyn, B. (2022, March 17). Deepfake video of Zelenskyy could be “tip of the iceberg” in Info War, experts warn. NPR .https://www.npr.org/2022/03/16/1087062648/deepfake-video-zelenskyy-experts-war-manipulation-ukraine-russia

Armin J. (2023, Sept 24) AI Malware https://www.linkedin.com/pulse/ai-malware-jart-armin/

Balbix. (2022, April 22). Using artificial intelligence in Cybersecurity. Balbix. https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity.

Bracken M. (2023, Dec 01) Bipartisan House legislation calls for two new federal cybersecurity training programs https://fedscoop.com/federal-cybersecurity-workforce-expansion-act/

Choudhury, A. (2023, October 31). 8 ways generative AI can enhance cybersecurity. Hire the World's Most Deeply Vetted Developers & Teams. https://www.turing.com/resources/generative-ai-enhances-cybersecurity

Chukwube, M. (2023, June 24) How the application of AI in threat detection will revolutionize Cybersecurity https://readwrite.com/how-the-application-of-ai-in-threat-detection-will-revolutionize-cybersecurity/

CISA. (n.d.). Artificial Intelligence: CISA. Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/ai

Conference-board.org (2023, Nov 01) AI: Regulations Rising https://www.conference-board.org/publications/AI-regulations-rising

Crume, J. (2023, November 7). How to secure AI business models. YouTube. https://www.youtube.com/watch?v=pR7FfNWjEe8

Devoteam.com (2023, Feb 28) Dangers and Challenges of AI in cybersecurity. https://www.devoteam.com/expert-view/dangers-and-challenges-of-ai-in-cybersecurity/

Devoteam.com (2023, May 9) Cybersecurity and ChatGPT. https://www.devoteam.com/expert-view/cybersecurity-and-chatgpt/cybersecurity-roles-of-generative-ai-entities-companies-agencies-and-government-in-enhancing-cybersecurity.

Dhoni, P., & Kumar, R. (2023, October 31). Synergizing generative AI and cybersecurity: Roles of Generative AI entities, companies, agencies, and government in enhancing cybersecurity. Authorea. https://www.techrxiv.org/users/691566/articles/682788-synergizing-generative-ai-and-cy

Digitalocean.com (n.d.) Understanding AI Fraud Detection and Prevention Strategies https://www.digitalocean.com/resources/article/ai-fraud-detection

Drake, V. (n.d.). *Threat modeling*. Threat Modeling | OWASP Foundation. https://owasp.org/www-community/Threat_Modeling

EC (2023, July 14) The role of Artificial Intelligence (AI) in Cyber Security https://www.eccu.edu/blog/technology/the-role-of-ai-in-cyber-security/

Farley, E (2024, Jan 04) AI Auditing: First steps towards the Effective Regulation of Artificial Intelligence https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4676184#:~:text=AI%20auditing%20standards%20should%20reflect,advancement%20of%20the%20technology%20itself.

Fruhlinger, J (2022, August 31) Stuxnet explained: The first known cyberweapon https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html

Goundar S., (2023, Oct 22) Leveraging Artificial Intelligence (AI) in Threat Modelling to Elevate Cybersecurity https://www.linkedin.com/pulse/leveraging-artificial-intelligence-ai-threat-elevate-sandeep-goundar/

Gupta, M., Akiri, C., Aryal, K., Parker, E., & Praharaj, L. (2023, July 3). From chatgpt to threatgpt: Impact of generative AI in cybersecurity and privacy. arXiv.org. https://arxiv.org/abs/2307.00691

Gupta, M., Praharaj, L., Akiri, C., Parker, E., & Aryal, K. (n.d.). (PDF) from chatgpt to threatgpt: Impact of generative AI in ... https://www.researchgate.net/publication/372074392_From_ChatGPT_to_ThreatGPT_Impact_of_Generative_AI_in_Cybersecurity_and_Privacy

Hughes C. (2024, Feb 13) Academic Plus Real-World Training Prepares a Cybersecurity- and AI-Ready Workforce https://accelerationeconomy.com/cybersecurity/academic-plus-real-world-training-prepare-a-cybersecurity-and-ai-ready-workforce/

Ivezic M. (2023, August 16) Outsmarting AI with Model Evasion https://defence.ai/ai-security/ai-model-evasion/

Khyatiraval. (2023, June 7). Generative AI for threat modeling. Community. https://community.threatmodeler.com/threatmodeling-appsec-130/generative-ai-for-threat-modeling-667#:~:text=AI%20can%20help%20automate%20the,their%20attack%20surface%20more%20accurately.

Krishnan, A. (2023, December 18). Generative AI is making Phishing attacks more dangerous: Techtarget. Security. https://www.techtarget.com/searchsecurity/tip/Generative-AI-is-making-phishing-attacks-more-dangerous#:~:text=General%20phishing%20attacks&text=Finally%2C%20AI%20chatbots%20can%20create,surface%20area%20of%20such%20attacks.

Kurdiez. (2023, February 4). How CHATGPT works technically for Beginners. YouTube. https://www.youtube.com/watch?v=uCIa6V4uF84

Lapata, M. (2023, October 12). What is Generative AI and how does it work? – the Turing lectures with Mirella Lapata. YouTube. https://www.youtube.com/watch?v=_6R7Ym6Vy_I

Lea, J. (2023, June 30). Securing the digital landscape: Generative AI in Cyber Security. LinkedIn. https://www.linkedin.com/pulse/securing-digital-landscape-generative-ai-cyber-security-jonas-lea

Limaj, B. (2023, February 15). Ethical considerations in AI-powered cybersecurity. Medium. https://medium.com/@besniklimaj/ethical-considerations-in-ai-powered-cybersecurity-45cd83db90e0

Menon, A. (2023, Jan 23) Data Poisoning and Its Impact on the AI Ecosystem https://mathco.com/blog/data-poisoning-and-its-impact-on-the-ai-ecosystem/

NJCCIC. (2017, August 10). Stuxnet. Cyber.nj.gov. https://www.cyber.nj.gov/threat-center/threat-profiles/ics-malware-variants/stuxnet

Okereafor, K. & Djehaiche, R. (2020). A Review of Application Challenges of Digital Forensics. https://www.researchgate.net/publication/341279240_A_Review_of_Application_Challenges_of_Digital_Forensics

Parmar, H. (2023, Sept 04) AI Powered Incident Response : Harnessing the power of self-healing end points. https://atos.net/en/lp/detect-early-respond-swiftly/ai-powered-incident-response-harnessing-the-potential-of-self-healing-endpoint

Pires, Luis Palma (2024, Jan 17) Empowering Cyber Guardians: A Paradigm Shift in Cybersecurity Education through AI Integration https://www.linkedin.com/pulse/empowering-cyber-guardians-paradigm-shift-education-ai-palma-pires-iuw5f/?trk=public_post_main-feed-card_feed-article-content

Prasad, M. (2024, January 24). *The ethical dilemmas of AI in Cybersecurity*. ISC.org. https://www.isc2.org/Insights/2024/01/The-Ethical-Dilemmas-of-AI-in-Cybersecurity

Rosencrance, L (2021, Oct 18) Tapping AI for Intrusion Detection Systems. https://www.iotworldtoday.com/security/tapping-ai-for-intrusion-detection-systems

Sowmiya , T., & Mary Anita E.A, (2023, August) A comprehensive review of AI based intrusion detection system Science Direct. https://www.sciencedirect.com/science/article/pii/S2665917423001630

Stanham, L. (2023, November 27). Generative AI (genai) and its impact in cybersecurity - crowdstrike. crowdstrike.com. https://www.crowdstrike.com/cybersecurity-101/secops/generative-ai/

Tivin, I. (2023, October 30). Expert advice on AI in cybersecurity: Toptal®. Toptal Engineering Blog. https://www.toptal.com/cybersecurity/questions-about-ai-cybersecurity#:~:text=Personalized%20security%20protocols%3A%20By%20creating,size%2Dfits%2Dall%20solutions.

Utilities One (2023, Nov 27) The Role of AI-Powered Intrusion Detection Systems in Communication Infrastructure

https://utilitiesone.com/the-role-of-ai-powered-intrusion-detection-systems-in-communication-infrastructure

Waller, J, (2023, Sept 07) How to safeguard your AI ecosystem: The imperative of AI/ML security assessments

https://www.synopsys.com/blogs/software-security/how-to-safeguard-your-ai-ecosystem.html#:~:text=Tangible%20benefits%20of%20AI%2FML%20security%20assessments,-Engaging%20in%20an&text=Regulatory%20compliance%20assurance%3A%20Such%20assessments,customers%2C%20partners%2C%20and%20stakeholders.