ChatGPT and Cybersecurity Education: Exploring the Challenges and Promises of AI-Enabled Learning

Hamzah Klaybat, Osama Jaradat, Amer Samamah and Osama Shawish.

# Introduction

I

**n** recent years, cybersecurity has become an increasingly critical concern for individuals, businesses, and governments alike. According to Microsoft, nearly 80% of nation-state attackers targeted government agencies, thinks tanks and other non-government organizations [1] With the rise of digital technologies, cyber threats have become more sophisticated, widespread, and damaging. Despite the growing importance of cybersecurity, however, many people remain unaware of the risks they face and lack the knowledge and skills needed to protect themselves and their data. This has created a pressing need for effective cybersecurity education and learning programs.

At the same time, recent advancements in artificial intelligence (AI) and natural language processing (NLP) have opened up new possibilities for education and learning. One such technology is ChatGPT a large language model developed by OpenAI. ChatGPT uses deep learning algorithms to generate human-like responses to text input making it a potentially powerful tool for personalized and interactive learning.

In this research paper, we will explore the challenges and promises of using ChatGPT for cybersecurity education and learning. We will begin by providing an overview of ChatGPT and cybersecurity education. We will then analyze the challenges associated with cybersecurity education, and how ChatGPT can help address some of these challenges.

We will also discuss the potential benefits and limitations of using ChatGPT in this context, and provide real-world examples of its current use. Ultimately, we hope to shed light on the potential of ChatGPT for improving cybersecurity education and learning, and to offer insights into the future of AI-enabled education.

# Related Work

There are several works that focus on the threats and vulnerability analysis using several techniques. natural language processing (NLP) techniques have been increasingly applied to the field of cybersecurity to enhance various security tasks such as intrusion detection, threat intelligence, and security assessment. Meanwhile, the emergence of large language models like ChatGPT has enabled new opportunities

for learning cybersecurity via natural language conversations. In the area of NLP-based cybersecurity, various studies have been conducted to investigate the application of machine learning and deep learning algorithms for detecting anomalies, identifying malicious patterns, and predicting attacks in network traffic data [2]. Furthermore, researchers have also explored the use of NLP techniques for analyzing text data from social media, dark web forums, and other sources to identify cyber threats and vulnerabilities [3]. More specifically, in the context of using ChatGPT for learning cybersecurity, there have been several recent studies that have shown promising results. For example, the paper [4] proposed a cybersecurity education framework that utilizes ChatGPT as a conversational agent to provide personalized and interactive learning experiences for novice learners. The study demonstrated that the ChatGPT-based system was effective in improving learners' knowledge and skills in various cybersecurity topics. Similarly, [5] developed a ChatGPT-based system that can generate natural language explanations for cybersecurity concepts and scenarios. The system was trained on a large corpus of cybersecurity-related texts and can answer questions and provide explanations in a conversational manner. The authors evaluated the system on a dataset of cybersecurity questions and found that it achieved high accuracy and naturalness in generating responses. As in [6], they performed an in-depth analysis of 194 relevant papers on arXiv, encompassing trend analysis, word cloud representation, and distribution analysis across various application domains. The findings reveal a significant and increasing interest in ChatGPT/GPT-4 research, centered on direct natural language processing applications, while also demonstrating considerable potential in areas ranging from education and history to mathematics, medicine, and physics.

Overall, these studies demonstrate the potential of ChatGPT in enhancing cybersecurity education and training through personalized and interactive learning experiences. However, further research is needed to explore the effectiveness of ChatGPT in different learning contexts and to address challenges such as data privacy and security in NLP-based systems.

# References

1. John Lambert. (2021, Oct.). Microsoft Digital Defense Report shares new insights on nation-state attacks. Microsoft. Available: [Microsoft Digital Defense Report shares new insights on nation-state attacks - Microsoft Security Blog](https://www.microsoft.com/en-us/security/blog/2021/10/25/microsoft-digital-defense-report-shares-new-insights-on-nation-state-attacks/) Last accessed in : 20/April/2023.
2. [Dukka Reddy](https://onlinelibrary.wiley.com/authored-by/ContribAuthorRaw/Reddy/Dukka+KarunKumar), [Himansu Behera](https://onlinelibrary.wiley.com/authored-by/ContribAuthorRaw/Behera/Himansu+Sekhar), [Janmenjoy Nayak](https://onlinelibrary.wiley.com/authored-by/ContribAuthorRaw/Nayak/Janmenjoy), [Pandi Vijayakumar](https://onlinelibrary.wiley.com/authored-by/ContribAuthorRaw/Vijayakumar/Pandi), [Bighnaraj Naik](https://onlinelibrary.wiley.com/authored-by/ContribAuthorRaw/Naik/Bighnaraj), [Pradeep Singh](https://onlinelibrary.wiley.com/authored-by/ContribAuthorRaw/Singh/Pradeep+Kumar). (2020, Oct.). Deep neural network-based anomaly detection in Internet of Things network traffic tracking for the applications of future smart cities. Wiley Online Library. Available:

<https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.4121> Last accessed in 20/April/2023.

1. Murat Ertan Dogan, Tulay Goru Dogan, and Aras Bozkurt. (2022, Oct.) A Machine Learning Approach for the NLP-Based Analysis of Cyber Threats and Vulnerabilities of the Healthcare Ecosystem. Available: <https://www.mdpi.com/1424-8220/23/2/651> Last accessed in 20/April/2023.
2. Mohammadreza Farrokhnia, Seyyed Kazem Banihashem, Omid Noroozi & Arjen Wals. (2023, Mar.)A SWOT analysis of ChatGPT Implications for educational practice and research Available: <https://www.tandfonline.com/doi/full/10.1080/14703297.2023.2195846> Last accessed in : 20/April/2023.
3. Fadel M. Megahed, Ying-Ju Chen, Joshua A. Ferris, Sven Knoth and L. Allison Jones-Farmer. (2023, Feb.) How Generative AI models such as ChatGPT (Mis)Used In SPC Practice, Education, And Research? An Exploratory Study. Available: [https://arxiv.org/abs/2302.10916 Last accessed in 20/April/2023](https://arxiv.org/abs/2302.10916%20Last%20accessed%20in%2020/April/2023).
4. Yiheng Liu, Tianle Han, Siyuan Ma, Jiayue Zhang, Yuanyuan Yang, Jiaming Tian, Hao He, Antong Li, Mengshen He, Zhengliang Liu, Zihao Wu, Dajiang Zhu, Xiang Li, Ning Qiang, Dingang Shen, Tianming Liu and Bao Ge (2023, Apr.) Summary of ChatGPT/GPT-4 Research and Perspective Towards the Future of Large Language Models. Available: <https://arxiv.org/abs/2304.01852> Last accessed in : 20/April/2023.