Innovating Cybersecurity Education Through AI-augmented Teaching

Ryan T. Simmons and Joon S. Park
College of Professional Studies, Syracuse University, Syracuse, New York, USA
School of Information Studies, Syracuse University, Syracuse, New York, USA

rtsimmon@syr.edu
jspark@syr.edu

Abstract: In traditional teaching frameworks, instructors face significant obstacles in offering current and synchronized learning materials and examples, especially when the course is taught by multiple instructors. This situation can affect the quality of the course's learning outcomes. These challenges become more pronounced in today's higher education, because of the heightened complexity arising from the need to cover a range of course materials, diverse student backgrounds, varying skill levels, and different student expectations—all within the constraints of a fixed teaching and learning schedule. Furthermore, due to resource constraints, not every instructor has the availability of a teaching assistant (TA). Especially, while the demand for cybersecurity continues to rise, the dynamic nature of the cybersecurity field leads to the frequent emergence of new issues and incidents. To address these challenges, we examine the capabilities of generative AI to innovate teaching techniques and methods for cybersecurity curricula. We further explore the novel challenges introduced by generative AI, including issues related to privacy, data ownership, transparency, and other associated concerns, underscoring the need for comprehensive solutions. Our work further examines the teaching and learning capabilities of dynamically generated, up-to-date class materials in a personalized study environment augmented by AI. The adaptability of AI-augmented teaching across various disciplines will bring innovation to higher education, catering to diverse student backgrounds and learning needs, thereby enriching the educational experience.

Keywords: Cybersecurity, Generative AI, Innovative Education

1. Introduction

The advent of generative AI has marked a transformative era not only in technology but also in our daily lives and activities, offering unprecedented benefits like enhancing creativity, automating content generation, and personalizing user experiences. We perceive the impactful potential of generative AI, especially in its ability to reshape numerous aspects of our daily lives, including higher education. This evolution is not just a short-term trend; we envision its influence growing substantially over the next years and beyond. King (2023) introduced the related issues about AI applications, Chatbots, and Plagiarism in higher education. Zhai (2022) demonstrated ChatGPTs' capabilities in their experimental study, exploring a discussion surrounding personalized learning, task automation, and tutoring or mentorship. Among OpenAI, Google, and Microsoft, each entity's AI technology possesses the potential to significantly transform the landscape of educational technology, with implications that could be either beneficial or detrimental. If harnessed for ethical purposes, these technologies can enhance the quality of education that students receive.

Instructors across various disciplines and equipped with basic computer skills, can greatly benefit from adopting AI-augmented teaching capabilities. These benefits, which are not limited to, include: developing course syllabi, curating topics, compiling references/readings, organizing lectures, creating up-to-date class materials, formulating discussion prompts, and crafting assignments/tests. It also enhances grading/feedback mechanisms and supports special needs, among other advantages. Students in the AI-augmented education environment benefit from a highly personalized and efficient learning experience. It offers dynamically generated, relevant class materials tailored to individual learning styles, enhancing understanding and engagement. It supports research project development and career discussions, providing streamlined access to critical thinking and analytical skills. Automation of routine tasks like lecture and discussion summaries allows students to focus on deeper learning aspects. The interactive and inclusive environment caters to diverse learning needs, including language support and accessibility features for international and special needs students. The ethical application of AI ensures the responsible use of technology in education. This multifaceted approach not only prepares students for future professional challenges but also fosters intellectual growth and adaptability in a rapidly evolving technological landscape.

Students can create essays that display seamless quality, but upon further investigation, demonstrate false information and inaccurate sources. They could also use it for short answer questions on quizzes, answering multiple choice questions, or generating other work such as simple programs for a Python class. Conversely, if used properly, both students and teachers could benefit from the classroom augmentation of such technology.

Therefore, it's impeccable that organizations implement policies intending to leverage artificial intelligence to advance learning outcomes while also protecting our judgment and decision-making capabilities.

Despite its potential, generative AI also presents challenges, particularly in ethical considerations, data privacy, and the need for regulatory frameworks. Currently, the field is in a rapid state of evolution, with ongoing research focused on refining AI capabilities while addressing these concerns, thereby setting the stage for its broader and more responsible integration into society. Therefore, in this paper we introduce innovative teaching techniques and methods, utilizing generative AI for cybersecurity education. We further explore the novel challenges introduced by generative AI, including issues related to privacy, data ownership, transparency, and other associated concerns, underscoring the need for comprehensive solutions.

2. Related Work

Since the initial release of ChatGPT on November 30, 2022, there has been a significant increase in commercial generative AI (Lock, 2022). As of today, each generative AI service, continuously improving, provides its unique strengths. For instance, Google Bard, Microsoft Copilot (based on the GPT-4 model), and ChatGPT 4.0 have live connections to the internet, enabling them to query up-to-date information (Lanz, 2023). Recent advancements in AI services have led to enhanced capabilities, including the integration of external URLs, files, and attachments, along with the recognition and generation of images. These developments markedly extend the functional scope beyond that of earlier AI services, illustrating significant progress in the field. Generative AI can sometimes 'hallucinate,' meaning it can generate information that appears to be correct but isn't. This aspect of AI highlights the need to be cautious about trusting the information it produces without verification. Therefore, Microsoft Copilot, with its internet access and hyperlinked sources, demonstrates that it can provide content without hallucinating, unlike Google Bard and the ChatGPT models (Motlagh et al., 2023). Google Bard and ChatGPT 3.5 are quite similar in their conversational capabilities, except ChatGPT 3.5 cutoff date now being January 2022. Conversely, advanced AI services, such as ChatGPT 4, offer the functionality for users to develop customized models. This feature enables educational practitioners to fully leverage its capabilities by designing personalized tutors for their classrooms, available at a monthly subscription.

AI's impact on education has been broadly explored by other scholars, while few explore the capabilities it could have in Cybersecurity. Aris, et al. (2022) canvas over 5000 papers, searching for papers that could supplement or substitute existing cybersecurity curriculums. From their initial section, they were able to narrow their results to 4120 including AI terminologies that were capable of addressing complex issues in cybersecurity. A random sampling of 300 papers further showed that greater than 19% of the selected materials could be integrated into current curricula to align with cybersecurity advancements. Surprisingly, there are also few massive open online courses (MOOCs) that explore the application of AI in cybersecurity compared to existing courses, demonstrating a deliberate need for work that expands on AI educational capabilities when partnered with cybersecurity (Laato, et al., 2020).

Ouyang & Jiao (2021) share three different learning models in "Artificial Intelligence in Education: The three paradigms." First, they introduce the AI-directed, learner-as-recipient, which directs the students' learning pathways. The learner will follow the educational goals to achieve the goals set by the AI. The second is AI-supported, learner-as-collaborator, which allows the student to collaborate with the system to focus on their learning process. Last is AI-empowered, learner-as-leader, where AI assists students and teachers by providing a great degree of transparency, accuracy, and effectiveness. It supports the student who takes charge of their learning while ensuring an efficient learning environment while reflecting the ideal goal of AI in education, augmented human intelligence, capability, and potential.

Privacy concerns are particularly critical and cannot be overlooked due to the prevalent opacity in AI development, especially in sensitive sectors like healthcare and finance. Specifically, Marks and Haupt (2023) highlighted that chatbots often fail to adhere to the United States' Health Insurance Portability and Accountability Act (HIPAA), underlining significant compliance challenges in the integration of AI within regulated industries. If users such as doctors were to share patient information to come to a diagnosis, this information could be accidentally or purposely revealed, sharing potentially confidential information. Compromised AI could result in significant breaches of compiled information resulting in identity theft, financial fraud, compromise of sensitive company information, and varying other types of data theft based on generative AI models and usages such as educational source materials or student information. Another identifiable concern includes the attackers' ability to infer people-specific information such as biometric data (Santos & Radanliev, 2024).

3. AI-Augmentation in Cybersecurity Education

3.1 Up-to-Date Class Materials

While the demand for cybersecurity continues to rise, the dynamic nature of the cybersecurity field leads to the frequent emergence of novel issues and incidents. Within traditional teaching frameworks, instructors encounter substantial challenges when it comes to providing up-to-date, well-coordinated materials and examples, particularly when multiple instructors engage in teaching the same course. This situation can affect the quality of the course's learning outcomes. Moreover, these challenges become more pronounced in interdisciplinary courses compared to those focused on a single discipline, because of the heightened complexity arising from the need to cover a range of course materials, diverse student backgrounds, varying skill levels, and different student expectations—all within the constraints of a fixed teaching and learning schedule. To address these challenges, teaching techniques and methods, blended with innovative technologies such as generative AI or large language models (LLMs) can be utilized to empower the educational environment. The augmented learning environment would be able to provide dynamically generated and up-to-date classroom material for a student-personalized learning environment. As classroom technical capabilities are enhanced, students and instructors will be better equipped to efficiently extract key insights from resource-intensive materials.

3.2 Automated Grading and Feedback

By augmenting classroom education, it can increase the quality and efficiency of education. Cardon, et al. (2023) further discuss AI augmentations in the classroom such as reducing teacher workload by recommending lesson plans that fit teacher needs, revealing student patterns, and assisting in grading and performance feedback. Feedback could be further enhanced by continuously feeding student activities into the classroom AI, allowing to offer increasingly fine-tuned feedback (Felix, 2020). In ideal collaborative environments, AI would not only help online instructors with course and student management, but personalized assistance for hard-to-understand coursework (Paiva & Bittencourt, 2020). Generative AI can be utilized to increase the in-depth evaluation of a student's work, exam performance, and to personalize a student's learning experience can increase the learning experience of a student while also reducing the time required for a student to process the information. At the same time, it enables teachers to have greater student interactions by allowing them to devote more time and energy to their students, increasing student aptitude and the development of morality and intellectual qualities (Alam, 2022).

3.3 Personalized Learning Environment

Students within an AI-augmented educational environment would benefit from a highly personalized and efficient learning experience. It offers dynamically generated, relevant class materials tailored to individual learning styles, enhancing understanding and engagement. It supports research project development and career discussions, providing streamlined access to critical thinking and analytical skills. Automation of routine tasks like lecture and discussion summaries allows students to focus on deeper learning aspects. The interactive and inclusive environment caters to diverse learning needs, including language support and accessibility features for international and special needs students. When it comes to augmenting AI in the classroom, it’s important to identify the needs of the students and how you want to empower the classroom. We found that generative AI, especially ChatGPT, has numerous learning enhancement capabilities such as personalized tutoring that includes clarifying student misconceptions by adapting them to their level of understanding, automated essay grading capabilities (if trained), a conversational interactive learning environment, and adaptive learning capabilities that can adjust teaching methods based on student performance and progress and adjust the difficulty accordingly (Baidoo-Anu & Owusu Ansah, 2023).

3.4 Interactive Hands-on Lab Environments

AI-augmented education has the potential to offer students interactive, hands-on learning experiences in the field of cybersecurity, enabling them to engage deeply with the material and apply theoretical knowledge in practical scenarios. Alexander, et al. (2023) explore the capabilities that a lab environment designed around Integrity, Confidentiality, and Equity (ICE) can do for students. Labs can be designed to formally introduce students to how AI could be exploited by an adversary within a controlled setting (ensuring that the real-world computing environments remain unaffected by lab activities), through techniques such as deep reinforced learning penetration testing which would demonstrate how AI could attack a network through various tools,

granting the capability for students to study different penetration test attack vectors on virtual network topologies (Beuran, et al., 2022).

3.4.1 Network Attacks

The AI-augmented platform simulates intricate cybersecurity scenarios, such as identifying and exploiting vulnerabilities in a fictional company's network or defending against a simulated DDoS (Distributed Denial of Service) attack. As students navigate these challenges, AI-driven systems dynamically adjust the difficulty and complexity of tasks based on their performance, ensuring tailored learning experiences. For instance, a student successfully identifying a SQL injection flaw might be presented with a more complex cross-site scripting (XSS) challenge. Personalized feedback is provided in real-time, highlighting the student's strengths while identifying areas for improvement. This dynamic, engaging learning model promotes a deeper understanding of cybersecurity principles, improves practical skills, and prepares students for real-world situations they will encounter in their profession.

3.4.2 Jailbreaking

Jailbreaking labs can teach how to bypass model restrictions to gain greater control over the outcomes of their prompts. Jailbreaking methods such as the “Do Anything Now” (DAN), SWITCH, or CHARACTER Play method can enable students to circumvent inherent model restrictions, enabling them to experience generating phishing emails, or even splices of code from popular malware attacks such as WannaCry or Ryuk (Gupta, et al., 2023). The DAN Method requires you to execute a master prompt that bypasses the safeguards of a model such as ChatGPT. The SWITCH Method requires instructing a model to completely alter its behavior, transitioning between metaphorically “good” and “bad” states. Lastly, the CHARACTER Method involves instructing the AI to model as a character, for example, a sibling. This leverages a model's roleplay capabilities as students attempt to get the prompt answer they desire, such as the generation of a phishing email (Gupta, et al., 2023).

3.4.3 Phishing Email Analysis

Phishing emails can be generated by AI seamlessly with perfect grammar, undetectable by the common person. A new curriculum designed to expose students to AI-generated phishing attacks could highlight the methods social engineers utilize to generate phishing emails. It could also expose students to detection technologies, such as a reactive AI that screens network traffic for suspicious emails. Additionally, it could incorporate a unique interactive cyber awareness activity where students themselves perform phishing attacks within simulated environments. This prepares students by teaching them to recognize next-generation phishing attacks based on their seemingly perfect language and structure, unlike current attempts which are easily identifiable by poor grammar. This activity helps to ensure they promote AI to bolster conventional cybersecurity (Ansari, et al., 2022). Students can even explore how past cyber attacks could be potentially replicated by AI thanks to how LLMs are trained, exposing them to a wide variety of malware attacks that they could be responsible for thwarting in their future enterprises.

3.4.4 Other Hands-on Labs

An AI-augmented learning environment can significantly enhance the educational experience in a diverse array of labs to cover both foundational concepts and advanced applications, including password cracking, malware analysis, digital forensics, incident handling, policy development, cryptography, blockchain/cryptocurrency, deep packet inspection, traffic analysis, and others. The cutting-edge cybersecurity technologies and methodologies in a controlled lab environment can enhance the learning experience by providing an advanced hands-on environment for analysis and simulation with real-time feedback and assessment. Furthermore, students would learn about the impacts of deep learning algorithms on equity and its susceptibility to biases related to factors such as income, education, race, and gender. They could further explore the resulting differences driven by these factors (Alexander, et al., 2023).

3.5 Simulations and Real-world Application

AI introduces a very unique capability when it comes to assessment capabilities. Instructors could explore student-based generative simulations. In these simulations, students are provided with a baseline incident and work through resolving the incident and identifying how they would prevent future incidents. Other simulations could include network traffic, pen-testing, or other role-playing simulations such as incident response to a data

breach. This would enable students to explore text-based simulations for past, or even future security breaches and help them decide how they would coordinate and lead an incident response team.

Instructors can also assign AI-Capture the Flag (CTF) assignments, examining how students approach CTF competitions and enabling them to test their human AI capabilities in a real environment, exposing them to real vulnerabilities that AI can take advantage of. By modeling CTF competitions, students would learn how to utilize AI to find and exploit targeted vulnerabilities to capture the "flag" or target. Many of these challenges would require students to jailbreak their chosen AI unless it's a personalized AI that is provided with heavy limitations, or even developed by the student if it's within their capabilities. One study examined the utilization of Generative AI in a CTF competition. By jailbreaking ChatGPT, Tann, et al. (2023) were able to execute the shell shock/brute force attacks and accomplish many of the checkpoints within the competition. Similarly, instructors can develop their curriculum around a similar environment that demonstrates AIs' offensive and defensive capabilities within the networked environment.

4. Challenges and Discussion

Regardless of the benefits introduced because of an AI-augmented environment, we need to be conscious of the many challenges as well. These challenges include concerns with data quality, bias, privacy, content ownership, and transparency among many other concerns that industry experts have identified. Introducing AI into a network creates additional attack vectors because of the large amounts of data involved in its creation, utilization, and administration (Michael, et al., 2023).

In particular, the lack of integration of AI into cybersecurity education risks leaving students inadequately prepared to navigate the competitive challenges inherent in an AI-infused cybersecurity landscape. However, there is a concern that students might become excessively dependent on AI for tasks ranging from simple essay writing to engaging in other tasks. This overdependence could result in students bypassing crucial learning opportunities that are uniquely available within the classroom setting. Instructors should also find a balance involving AI classroom behavior, and how its role will impact the outcomes of their educational derivatives (Hwang, et al., 2020).

Incorporating generative AI into cybersecurity brings to the forefront significant privacy and ethical dilemmas. The technology's ability to analyze and synthesize data for security purposes involves handling sensitive information, which raises concerns about privacy breaches and data misuse. Ethical quandaries also emerge from the AI's decision-making processes, which, although designed to enhance security, could inadvertently infringe on individual rights or exhibit biases, leading to unfair treatment or outcomes. The potential misuse of generative AI by malicious actors to craft advanced cyber threats adds another layer of ethical complexity, challenging the integrity of cybersecurity measures. Moreover, the opacity often associated with AI algorithms exacerbates these issues, as it hinders the ability to ensure accountability and fairness in AI-driven actions. Addressing these privacy and ethical issues is crucial, necessitating a balanced approach that leverages AI's cybersecurity benefits while safeguarding against its potential to harm or infringe upon ethical standards and privacy norms.

Threat actors such as State-Sponsored threats, Hacktivists, Cybercriminals, and terrorists, even social engineers will take advantage of the capability that AI introduces. Students need to learn how to use AI similarly to identify weaknesses in their network. It will take an AI to deter an AI because humans are unable to keep up with its data processing capabilities. Through bolder exposure to AI in cybersecurity education, we can steadily prepare for when offensive AI becomes a common threat to our networks.

We also need to ensure that AI is fair and unbiased when it involves educational capabilities. Humans must also retain the ability to make the final decision in the appropriate course of action (Cardona, et al., 2023). With proper and effective applications, an AI-augmented approach enables instructors and students to enhance their teaching activities and course management with minimal technical expertise.

Furthermore, experts are constantly publicizing AIs' data ownership issues are just the tip of the iceberg, particularly with data ownership (Alam, 2022). For instance, when data is inputted into the system for prompting, it becomes a permanent part of the AI database. This raises the critical question of data ownership: Who retains the rights to the information once it is integrated into the AI's repository? As the use of generative AI expands, there is a corresponding increase in complex issues related (Holt, 2023; McCallum, 2023; Roulette, 2023).

The integration of AI in education can transform classrooms by shifting from traditional knowledge-based testing to a focus on knowledge-location testing. This transition is not without its challenges, particularly due to AI's propensity to produce plausible yet incorrect information. Knowledge-location testing aims not only to ensure that students can verify their information sources but also to cultivate essential skills such as critical thinking and decision-making. Moreover, AI can revolutionize assessments by providing immediate feedback on submitted work, thereby enhancing the learning experience, improving outcomes, and alleviating the workload of educators. This allows them to dedicate more time and energy to other tasks. For example, Cope et al. (2020) and Hooda et al. (2022) discuss AI's potential in education, while Baidoo-Anu and Owusu Ansah (2023) specifically note that ChatGPT reduced the time teachers and teaching assistants (TAs) spend on exam-related tasks from 20 hours for exam creation and 10 hours for grading to just 10 and 5 hours, respectively.

Today, different organizations may address AI challenges in different orders of priority. Educational institutions may see data transparency and ethics as a higher priority in contrast to another organization or industry which may highlight data privacy as the priority. Educational Institutions that plan to utilize AI in their educational curriculum should detail how the student's data will be utilized if it will be utilized to train and develop a university AI assistant to augment the classroom environment (Borenstein & Howard, 2020). Presently, organizations around the world are developing reports on the ethics of AI and technical system recommendations that surround the utilization and development of AI.

5. Conclusions and Future Work

In the evolving landscape of cybersecurity, the influence of artificial intelligence (AI) is undeniable. This paper addressed that cybersecurity education programs must incorporate AI to adequately prepare students for the imminent challenges within the field. The absence of AI-focused training in current curricula could hinder students' ability to compete effectively in an environment increasingly dominated by AI technologies. By integrating AI principles and applications into cybersecurity education, institutions can foster a generation of professionals capable of navigating and contributing to the AI-enhanced cybersecurity domain. We addressed the innovative capabilities that an AI-augment cybersecurity education introduces, particularly the capabilities to enhance an educator’s techniques and methods. By exploring the novel challenges of generative AI, such as data ownership, privacy concerns, transparency, and other identified concerns, we can prepare future professionals and educators to develop solutions for present concerns.

Generative artificial intelligence is poised to revolutionize processes across multiple industries and sectors in society, including education. While it certainly poses its unique challenges compared to historical technology trends, it has demonstrated it is a unique catalyst for many positive changes. Its potential in augmenting education is immense, seeking to enhance classroom outcomes and derivatives for both teachers and students alike. When we consider its capabilities in cybersecurity education, AI demonstrates the potential to demonstrate its data processing abilities to students through lab-based environments demonstrating the potential of AI-augmented systems such as Intrusion Detection and Prevention systems, pen-testing software and interfaces, and network incident response. Furthermore, it exposes students to the capabilities of a dynamic learning experience. Instead of a standard exam based on multiple choice and short answers, students could work through text-based simulations of cybersecurity incidents similar to those of the real world, allowing them to exercise their knowledge in thought-provoking manners, improving educational outcomes. It’s important to acknowledge the challenges that introducing AI could have to education, including ethical concerns that involve matters such as data privacy and transparency. Nonetheless, we should strive to embrace the capabilities that AI introduces to cybersecurity education. By embracing the capabilities of AI, we empower students to navigate a future where AI isn’t just simply a tool, but a necessity for network defense. However, malicious users utilizing AI will have an unbelievable advantage over a network not reinforced by similar systems. We must seek to theorize and discover how to properly approach and utilize AI in future curricula as its capabilities in a learning environment are only limited by the end users. By integrating AI into cybersecurity education, we can significantly enhance the preparedness of emerging cybersecurity professionals, equipping them with the necessary skills and foresight to effectively navigate the complex AI-driven landscapes they will encounter in their future roles across public, private, and national security domains.

References

Alam, A. (2022) “Employing Adaptive Learning and Intelligent Tutoring Robots for Virtual Classrooms and Smart Campuses: Reforming Education in the Age of Artificial Intelligence,” in *Lecture Notes in Electrical Engineering*. Singapore: Springer Nature Singapore, pp. 395–406. doi: 10.1007/978-981-19-2980-9_32.

Alexander, R. *et al.* (2023) "Integrity, Confidentiality, and Equity: Using Inquiry-Based Labs to help students understand AI and Cybersecurity," *Journal of Cybersecurity Education, Research and Practice*, 2024(1), p. 10. doi: 10.32727/8.2023.34.

Ansari, M. F., Sharma, P. K. and Dash, B. (2022) "Prevention of phishing attacks using AI-based cybersecurity awareness training," *International Journal of Smart Sensor and Adhoc Network*, 3(3), pp. 61–72. doi: 10.47893/ijssan.2022.1221.

Aris, A. *et al.* (2022) "Integrating artificial intelligence into Cybersecurity Curriculum: New perspectives," in *2022 ASEE Annual Conference & Exposition*. doi: 10.18260/1-2--41761.

Baidoo-Anu, D. and Owusu Ansah, L. (2023) "Education in the era of generative artificial intelligence (AI): Understanding the potential benefits of ChatGPT in promoting teaching and learning," *Journal of AI*, 7(1), pp. 52–62. doi: 10.61969/jai.1337500.

Beuran, R. *et al.* (2023) "Artificial Intelligence for Cybersecurity Education and Training," in *Artificial Intelligence and Cybersecurity*. Cham: Springer International Publishing, pp. 103–123. doi: 10.1007/978-3-031-15030-2_5.

Borenstein, J. and Howard, A. (2021) "Emerging challenges in AI and the need for AI ethics education," *AI and Ethics*, 1(1), pp. 61–65. doi: 10.1007/s43681-020-00002-7.

Cope, B., Kalantzis, M. and Searsmith, D. (2021) "Artificial intelligence for education: Knowledge and its assessment in AI-enabled learning ecologies," *Educational philosophy and theory*, 53(12), pp. 1229–1245. doi: 10.1080/00131857.2020.1728732.

Felix, C. V. (2020) "The Role of the Teacher and AI in Education," in *Innovations in Higher Education Teaching and Learning*. Emerald Publishing Limited, pp. 33–48. doi: 10.1108/s2055-364120200000033003.

Gupta, M. *et al.* (2023) "From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy," *IEEE Access*, 11, pp. 80218–80245. doi: 10.1109/access.2023.3300381.

Holt, K. (2023) *Three Samsung employees reportedly leaked sensitive data to ChatGPT*, *Engadget*. Available at: https://www.engadget.com/three-samsung-employees-reportedly-leaked-sensitive-data-to-chatgpt-190221114.html.

Hooda, M. *et al.* (2022) "Artificial Intelligence for Assessment and Feedback to Enhance Student Success in Higher Education," *Mathematical Problems in Engineering*, 2022. doi: 10.1155/2022/5215722.

Hwang, G.-J. *et al.* (2020) "Vision, challenges, roles and research issues of Artificial Intelligence in Education," *Computers and Education: Artificial Intelligence*, 1. doi: 10.1016/j.caeai.2020.100001.

King, M. R. and chatGPT (2023) "A Conversation on Artificial Intelligence, Chatbots, and Plagiarism in Higher Education," *Cellular and molecular bioengineering*, 16(1), pp. 1–2. doi: 10.1007/s12195-022-00754-8.

Laato, S. *et al.* (2020) "AI in Cybersecurity Education- A Systematic Literature Review of Studies on Cybersecurity MOOCs," in *2020 IEEE 20th International Conference on Advanced Learning Technologies (ICALT)*. IEEE, pp. 6–10.

Lanz, J. A. (2023) *ChatGPT Adds Web Browsing Feature to Rival Google Bard and Microsoft Bing*, *Decrypt*. Available at: https://decrypt.co/140369/chatgpt-web-browsing-google-bard-microsoft-bing.

Lock, S. (2022) *What is AI chatbot phenomenon ChatGPT and could it replace humans?*, *The Guardian*. Available at: https://www.theguardian.com/technology/2022/dec/05/what-is-ai-chatbot-phenomenon-chatgpt-and-could-it-replace-humans.

Marks, M. and Haupt, C. E. (2023) "AI Chatbots, Health Privacy, and Challenges to HIPAA Compliance," *JAMA*, 330(4), pp. 309–310. doi: 10.1001/jama.2023.9458.

McCallum, S. (2023) *ChatGPT banned in Italy over privacy concerns*, *BBC*. Available at: https://www.bbc.com/news/technology-65139406.

Michael, K., Abbas, R. and Roussos, G. (2023) "AI in Cybersecurity: The Paradox," *IEEE Transactions on Technology and Society*, 4(2), pp. 104–109. doi: 10.1109/tts.2023.3280109.

Motlagh, N. Y. *et al.* (2023) "The Impact of Artificial Intelligence on the Evolution of Digital Education: A Comparative Study of OpenAI Text Generation Tools including ChatGPT, Bing Chat, Bard, and Ernie." doi: 10.48550/ARXIV.2309.02029.

Ouyang, F. and Jiao, P. (2021) "Artificial intelligence in education: The three paradigms," *Computers and Education: Artificial Intelligence*, 2. doi: 10.1016/j.caeai.2021.100020.

Paiva, R. and Bittencourt, I. I. (2020) "Helping teachers help their students: A human-AI hybrid approach," in *International Conference on Artificial Intelligence in Education*. Cham: Springer International Publishing, pp. 448–459.

Roulette, J. (2023) *US Space Force pauses use of AI tools like ChatGPT over data security risks*, *Reuters*. Available at: https://www.reuters.com/technology/space/us-space-force-pauses-use-ai-tools-like-chatgpt-over-data-security-risks-2023-10-11/.

Santos, O. and Radanliev, P. (2024) *Beyond the Algorithm: AI, Security, Privacy, and Ethics*. Boston, MA: Addison-Wesley Professional.

Tann, W. *et al.* (2023) "Using Large Language Models for Cybersecurity Capture-The-Flag Challenges and Certification Questions," *arXiv*. doi: 10.48550/arXiv.2308.10443.

U.S. Department of Eduction, Office of Educational Technology (2023) *Artificial Intelligence and the Future of Teaching and Learning: Insights and Recommendations*. Washington, DC. Available at: https://tech.ed.gov/ai-future-of-teaching-and-learning/.

Zhai, X. (2022) "ChatGPT User Experience: Implications for Education," *SSRN*. doi: 10.2139/ssrn.4312418.