

AI Supporting Cybersecurity Curriculum

Henry Collier

Thomas Edison State University, USA

hcollier@tesu.edu

Abstract: Artificial Intelligence is the next frontier. As Machine Learning and Generative AI continue to advance, threat actors are using AI to increase the effectiveness of their attacks. Whether through AI-enhanced social engineering attacks or sophisticated malware that current methods cannot detect, AI is changing the threat landscape. It is imperative that students in the field of cybersecurity be taught to use AI to strengthen defensive measures. This paper outlines the need for and recommended best practices for implementing AI training in cybersecurity education to ensure that the defenders of our data are prepared for the next virtual battlefield.

Keywords: Artificial intelligence, Cybersecurity, Curriculum

1. Introduction

Artificial Intelligence (AI) has been a topic of discussion since Alan Turing first discussed it in his publication *Computing Machinery and Intelligence*. The world of Science Fiction has taken this and run rampantly with it, with many examples like Hal in the movie 2001 A Space Odyssey, where Hal loses his mind and kills everyone, or more poignantly in the Terminator series where SkyNet is bound to destroy humanity in its entirety. The world of science fiction is filled with examples of AI, and in most cases, it is the worst of what AI would bring, if ever truly invented. Current forms of AI like ChatGPT or Google Gemini are considered generative AI, and thus far do not have the capacity that SkyNet or Hal represented in pop fiction. Current forms of AI cannot think for themselves, they cannot replicate genuine consciousness, or the emotions that come with consciousness (Cebal-Loureda, Rincón-Flores, & Sanchez-Ante, 2024). Furthermore, current forms of AI struggle with common sense aspects, complex ethical judgements, and true innovation (Cebal-Loureda, Rincón-Flores, & Sanchez-Ante, 2024). What the current forms of AI do exceptionally well is process data and conduct pattern analysis over large data sets at an incredible speed. (Cebal-Loureda, Rincón-Flores, & Sanchez-Ante, 2024).

From a purely academic perspective, AI brings both positive and negative attributes to the table. For example, since the release of AI to the general public, there has been an increase in the number of potential plagiarism events (Kotsis, 2024). Professors are starting to suspect that students are using AI to write their papers. The problem is that AI does such a great job of paraphrasing the data that it searches, typical plagiarism detectors cannot detect that the papers have indeed been plagiarised (Collier, 2025). The current answer to this problem is the development of two websites which claim they can detect whether something has been written by AI or not. However, in a study conducted in 2024, testing the efficacy of these two tools, it is clear that the tools only have about a 50% efficacy value (Collier, 2025). The study utilized 150 papers written by individuals where English was their first language, English was their second language, and where AI wrote them entirely. The study demonstrated that the AI detection tools would falsely determine that papers written by a human were partially or completely written by AI, and where papers that were known to have been written by AI, were partially or mostly written by a human (Collier, 2025). The results of this study demonstrate that we do not have the tools to properly identify if something was written by AI or a person. Therefore, it is imperative that students are taught how to properly use AI in the classroom. However, for the cybersecurity community, this extends beyond simply teaching how to use AI in the classroom in a manner that supports education, but also how to use AI as an effective cybersecurity tool.

The cybersecurity community has seen a significant increase in the number of attacks that have been influenced partially, or entirely by one form of AI or another (Collier, 2025) (Truong, et al., 2020). As is noted in the paper *AI in Social Engineering: The Next Generation of Offensive Cyber Operations*, which was presented at the 24th European Conference on Cyber Warfare and Security, held at the Deutsches Forschungszentrum für Künstliche Intelligenz/ German Research Center for Artificial Intelligence in 2025, there is clear evidence that nation state actors are using AI to develop and implement social engineering attacks that have an increased probability of success (Collier, 2025). Due to this change in approach to offensive cyber operations, it is imperative that higher education institutions begin to teach their students how to use AI as a force multiplier.

2. Defining AI in Cybersecurity Curriculum

Implementing AI in cybersecurity curriculum should be handled in a different manner than implementing AI in any other form of curriculum. Instead of trying to teach the cybersecurity student how to use AI to better write a paper, it is imperative that students are being taught the tactics and techniques of using AI as a cybersecurity tool (Aris, et al., 2022) (Grover, et al., 2022). AI can be used in cybersecurity from both an offensive and a defensive perspective and it is imperative that institutions of higher education teach these methods to students (Morel, 2011). Research has shown that AI is being implemented in many ways in the cybersecurity community, ranging from adapting social engineering schemes, developing sophisticated malware, identifying security lapses in systems, assessing potential social engineering threats, deconstructing malware, to include ransomware and much more (Khan, et al., 2024).

3. Implementing AI in Cybersecurity Curriculum

Implementing AI into cybersecurity curriculum is different than implementing AI into other areas of curriculum within higher education. In non-cybersecurity curriculum, AI needs to be implemented in a manner that is complimentary to the curriculum. It comes with the thought that students will need to use AI in order to be more successful in their academic journey. This can include using AI to help structure a paper to ensure a smooth, well-structured product. Furthermore, it can be used to identify potential resources for a paper, as well as provide guidance on adjusting the language of a paper to improve its reception amongst the targeted audience. In cybersecurity education, these tools are still valuable, but what is more valuable to the cybersecurity student is learning the nuances surrounding the use of AI as a tool within the cybersecurity community. When you breakdown the various approaches to cybersecurity, it is easy to see how AI can strengthen both defensive postures and support offensive missions.

AI's ability to parse large data sets at exceptionally fast speeds can be instrumental in detecting potential threats and monitoring the overall health of a system (Grover, et al., 2022) (Mohamed, 2025). Adding AI as part of a structured detection and monitoring system decreases the probability of a threat actor gaining persistent access to a system. The AI system can analyse how data is traversing a network and identify anomalous behaviour in a matter of seconds or minutes, rather than days or weeks (Mohamed, 2025). Instead of a threat actor gaining access to a system and having long term access, AI can be implemented in a manner that catches the access and either shuts it down, or simply notifies the security team, reducing how long a threat actor has access (Khatibi, et al., 2025). As a component of this approach, AI can be used to identify known malware through signature detection, while also detecting unknown malware by assessing anonymous data that matches the tendencies of known malware (Khatibi, et al., 2025).

In addition to detecting technical methods of attack, AI is instrumental in identifying and quarantining social engineering attacks, reducing the likelihood that an employee will become a victim of social engineering attacks (Fakhouri, et al., 2024). As phishing and social engineering attacks become more sophisticated, resulting in a higher hit ratio, AI is going to be a crucial resource in detecting and shutting down these attacks (Fakhouri, et al., 2024) (Kolluri, 2024).

Furthermore, on the defensive posture, we are seeing AI being used as part of the incident response process, by implementing an automated approach to incident response where AI identifies a potential attack, then either automatically quarantining the suspected malware, or shutting down key services and notifying the security team for further evaluation and mitigation (Natalapati, 2024).

AI can also be used in the offensive or even the active defensive approach to cybersecurity (Loaiza, et al., 2019). From an offensive perspective, AI can be a great tool in the development of next generation cyber-attacks. For example, AI can be used to develop malware that bypasses current detection methods, and is polymorphic, which increases the odds of persistence (Mancini, 2024). Another approach is AI can be used to identify and take advantage of known and unknown vulnerabilities within a system. The technical approaches are not the only opportunities for offensive cyber operations. The easiest way to gain access to a system isn't through a technical attack, but rather through a human attack. Social engineering has a significantly higher probability of success over traditional hacking (Carruthers, 2026). Now that AI has been introduced to the offensive cyber world, Social Engineering has taken dramatic steps towards being almost undetectable by current methods and this is entirely because of AI (Mancini, 2024). As educators, it is imperative that we incorporate the tactics and techniques of incorporating AI into both offensive and defensive cyber capabilities, to include social engineering.

In order to be successful in implementing AI into the operational aspects of cybersecurity education, we need to develop new exercises and activities that allow students the opportunity to practice using AI as a tool. There are some very important concerns with this approach, which are outlined in the next section.

4. Ethical Concerns

Teaching cybersecurity has come with ethical concerns since the early days of cybersecurity being taught. For example, the lessons taught in a cybersecurity program come with the risk that the student will use the skills learned for nefarious activities. AI brings its own level of concern. Since AI can significantly increase the likelihood of success, the risk of a student choosing to use their knowledge and their skills for immoral or illegal purposes increases. As educators, we have a moral obligation to try and ensure students don't get tempted to do evil with the skills we teach. In addition to the concern that a student may decide to use AI and cybersecurity in a threatening manner, it is also important to note that accidents could happen that have resounding effects.

For example, the Morris Worm was originally designed to simply gauge the size of the Internet, but due to some coding errors, the worm replicated in an uncontrolled manner, resulting in massive unintended disruptions on the Internet (FBI, 2018). So, it is imperative that as we begin to teach how to use AI as a cyber tool, we do so with some stringent safeguards, to include requiring any AI based cyber exercise be only used in a sandbox.

Outside of the ethical concerns that exist, there are some pedagogical issues that need to be addressed.

5. Pedagogical Concerns

From a pedagogy standpoint, there are several concerns with implementing AI into cybersecurity curriculum. To begin with, anytime something new is implemented within higher education that automates a process, there is a concern that critical thinking will be degraded (Nikolopoulou, 2024). In cybersecurity this extends to the concept of adversarial thinking, which is critical in the cybersecurity industry. Additionally, utilizing AI tools in cybersecurity creates an environment where things become so automated that the cybersecurity professional may distance the students from the real-world impact of their actions (Nutalapati, 2024). Just because you can do something, doesn't mean you should. As educators, we are obligated to teach the students the moral and ethical use of their knowledge, skills and tools. Students need to fully understand the ethical implications of what they are doing and the risk of causing harmful actions.

From a structural perspective of pedagogy, and classroom implementation, it is important to note that this isn't the wild, wild west of cybersecurity education, where there are no consequences for one's actions (Kamak, et al., 2024). Therefore, educators need to make sure they are building safeguards into their curriculum to significantly reduce the possibility that an experiment or assignment makes it into the wild, which could cause significant damage. Therefore, assignments and lab activities need to be fully developed and tested prior to implementation, and they need to be contained within safe environments like a sand boxed environment that has no access to the outside world.

The goal of implementing AI in a cybersecurity curriculum is to give the students the necessary skills to utilize this powerful tool to support their organization's security posture. With threat actors using AI more and more, it is not a question of if we teach students to use AI as a tool, but more about how we teach them to use it.

6. Potential Outcomes

Teaching AI in cybersecurity curriculum will result in a variety of positive outcomes. The first and most important is teaching students how to use AI as a tool in cybersecurity provides them with the hands-on experience that reinforces how the cybersecurity community is actually operating today (Tian, 2025). This makes students job-ready, needing less time to come up to speed on the job. AI provides a significant improvement in the detection of threats on a network through better pattern recognition, which results in students learning how pattern recognition is used in conjunction with traditional methods like rules and signatures (Aris, et al., 2022). Teaching AI in cybersecurity curriculum further gives students the skills to better identify how threat actors are using AI in an offensive manner, which gives them better skills to anticipate adversarial tactics, design better countermeasures, and to think like both a red team and a blue team member (Matthews, et al., 2025).

7. Best Practices

Based on this author's experience implementing AI across a variety of curriculums, to include cybersecurity, here is a list of best practices that should be followed when implementing the teaching of AI as a cybersecurity tool.

- Teach AI as an assistant, not as a replacement.
- Emphasize the human-in-the-loop approach.
- Build curriculum from a cybersecurity fundamentals approach, then layer on AI tools.
- Ensure data sets implemented are realistic, and domain specific.
- Teach how AI is being used in adversarial and misuse perspectives.
- Integrate ethics, law and governance throughout, do not introduce it as a footnote.
- Increase complexity over time. You want to test the student's ability to adapt and overcome future unknown challenges.
- Align AI tools with business and industry outcomes and goals.
- Ensure students are using reflection and metacognition to further understand how AI has changed their thinking to ensure they do not lose track of the end goal—better cybersecurity.
- Utilize sandbox domains to ensure leakage doesn't occur and students can learn in a safe and productive environment.
- Prepare instructors to teach AI in cybersecurity, as much as teaching students how to use AI as a tool

8. Conclusion

It is not a question of if we should be teaching AI as a strategic tool in cybersecurity or not, but rather it is a question of how we do it. AI has seen a significant boom in its use in cybersecurity, especially since the release of generative AI chatbots to the general public. This increases the threats we experience as AI is making offensive cyber activities easier for a less technically qualified population of threat actors. As educators, we have an obligation to our students to ensure our curriculum is not only robust, but more importantly, current. Developing curriculum that teaches students how to use AI as a tool in cybersecurity in a safe and productive manner is exceedingly important for the cybersecurity industry. We are at a crossroads, teach AI or not, and if an organization decides to "not" teach it, then they will put themselves in the rear-view mirror very quickly. For this reason, now is the time for institutions of higher education to review and analyse their cybersecurity education and implement new approaches to teaching AI as a cybersecurity tool to the next generation of cyber defenders. Universities need to develop a set of best practices and follow them to ensure consistent student outcomes. Moreover, they need to encourage students to be creative.

Ethical Declaration: Ethical clearance was not required for this research.

AI Declaration: The AI tool ChatGPT was used to identify sources to be used for citation based on specific statements within the document. In no way was AI used in the actual writing of this document.

References

- Aris, A. et al., 2022. Integrating Artificial Intelligence into Cybersecurity. Minneapolis, ASEE.
- Aris, A. et al., 2022. Integrating Artificial Intelligence into Cybersecurity Curriculum: New Perspectives. Minneapolis, ASEE.
- Carruthers, S., 2026. We can't stop social engineering for good, but we can fight back. [Online] Available at: <https://www.ibm.com/think/insights/why-social-engineering-still-works> [Accessed 08 02 2026].
- Cebral-Loureda, M., Rincón-Flores, E. G. & Sanchez-Ante, G., 2024. What AI can do: strengths and limitations of Artificial Intelligence. Boca Raton: CRC Press.
- Collier, H., 2025. AI in Social Engineering: The Next Generation of Offensive Cyber Operations. Kaiserslautern, ACI .
- Collier, H., 2025. Efficacy of Detecting AI Plagiarism in Higher Education. Lisbon, 2nd International Conference on Education Research.
- Fakhouri, H. N. et al., 2024. AI-Driven Solutions for Social Engineering Attacks: Detection, Prevention, and Response. 2nd International Conference on Cyber Resilience (ICCR) .
- FBI, 2018. FBI News. [Online] Available at: <https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218> [Accessed 09 02 2026].
- Grover, S., Broll, B. & Babb, D., 2022. Cybersecurity Education in the Age of AI: Integrating AI Learning into. Toronto, SIGCSE.
- Kamak, R., Debo, D. & Saaida, M., 2024. Challenges of AI in higher education. LVR Center. Libra Academy, p. 102.108.
- Khan, M. I., Arif, A. & Khan, A. R. A., 2024. The Most Recent Advances and Uses of AI in Cybersecurity. BULLET: Jurnal Multidisiplin Ilmu, 3(4).

- Khatibi, A. et al., 2025. Advanced AI-Driven Cybersecurity: Analyzing Emerging Threats and Defensive Strategies. *Natl. Acad. Sci. Lett.*.
- Kolluri, V., 2024. Revolutionary Research On The AISentry: An Approach To Overcome Social Engineering Attacks Using Machine Intelligence. *International Journal of Advanced Research and Interdisciplinary Scientific Endeavours*, 1(1).
- Kotsis, K. T., 2024. Artificial Intelligence Creates Plagiarism or Academic Research?. *Artificial Intelligence Creates Plagiarism or Academic Research*, 1(6).
- Loaiza, F. L., Birdwell, J. D., Kennedy, G. L. & Visser, D., 2019. *Utility of Artificial Intelligence and Machine Learning in Cybersecurity*, Arlington: Institute for Defense Analyses.
- Mancini, A., 2024. *AI-Generated Malware and How It's Changing Cybersecurity*. s.l.:Impact.
- Matthews, N., Schwartz, C. & Wright, M., 2025. Teaching Generative AI for Cybersecurity: A Project-Based Learning Approach. *Journal of The Colloquium for Information Systems Security Education*, 12(1).
- Mohamed, N., 2025. Artificial intelligence and machine learning in cybersecurity:a deep dive into state-of-the-art techniques and future paradigms. *Knowledge and Information Systems* , Volume 67, p. 6969–7055.
- Morel, B., 2011. *Artificial Intelligence a Key to the Futureof CyberSecurity*. New York: ACM.
- Nikolopoulou, K., 2024. Generative Artificial Intelligence in Higher Education: Exploring Ways of Harnessing Pedagogical Practices with the Assistance of ChatGPT. *International Journal of Changes in Education*, 1(2), pp. 103-111.
- Nutalapati, P., 2024. Automated Incident Response Using AI in Cloud Security. *Journal of Artificial Intelligence, Machine Learning and Data Science*, 2(1).
- Tian, J., 2025. Integrating Artificial Intelligence into the Cybersecurity Curriculum in Higher Education: A Systematic Literature Review. *Education Sciences*, 15(11).
- Truong, T. C., Diep, Q. B. & Selinka, I., 2020. Artificial Intelligence in the Cyber Domain: Offense and Defense. *Symetry*, 12(3).