**Topic:** Why Artificial Intelligence Can't Replace Human Workforce in Cybersecurity

Sri Sai Sathvik Pidikiti

New Jersey Institute of Technology, College of Humanities and Social Sciences

English 102, Section 074

Professor Gabrielle Rossi

April 17th, 2026

## Introduction

Cybersecurity is evolving rapidly. AI-automated systems are now an extremely important component of internal defenses against cyber threats. AI-automated systems are computer programs that use artificial intelligence to analyze data, learn from patterns, and make decisions with minimal human involvement. These systems are designed to detect threats, respond to attacks, and improve over time based on new data. AI systems can detect unusual activity, monitor networks, and respond quicker than traditional cybersecurity tools (Ahmed, Okba, & Harous, 2024). AI analyzes large volumes of data from endpoints, cloud based applications, and servers to identify potential threats (Alowaidi et al., 2023). If AI monitors access logs over time, a sudden rush of access attempts may signal a brute force attack. AI systems would provide alerts and may perform automated actions, reducing human management and allowing analysts to focus on bigger attacks instead of reviewing every alert.

As demand for cyber security increases, cybersecurity jobs are rising. The U.S Bureau of Labor Statistics (2024) predicts a 35% growth in information security analysts by the end of 2032. The growth is due to the increase of artificial intelligence, cyber attacks and need for human oversight. Even though cyber security jobs are on the rise, job seekers must understand the capabilities and limitations that AI can have.

## How AI Works in Cybersecurity

There is a concentration of AI which helps to combat any threat and it's called machine learning models. The process of how machine learning models work is they identify malware, phishing, and suspicious activity by the historical data that has been given to them for training. They help identify potential attacks by identifying pattern changes before damage occurs

(Martínez Torres et al., 2019). For example, an AI system might flag an account attempting to access sensitive data at unusual times. These tools improve detection and reduce false alerts while identifying threats missed by traditional systems. AI is also used for fraud detection in e-commerce systems. It identifies unusual transtraction patterns such as purchases from new locations or repeated failed login attempts. Flagged cases are reviewed by humans to determine if they are fraudulent.

## Limitations of AI

AI requires human oversight because it relies on historical patterns. Attackers can introduce new patterns that confuse AI systems. False positives are common, and without human review , AI may sometimes identify normal activity as threats.

Adversarial attacks are another concern. Attackers don’t stick to one method for long. They constantly modify malware just enough that it won't match anything a system was originally trained to recognize, letting it slide past automated detection tools. That's part of why human oversight still matters so much. People have to step in, sort through alerts, confirm whether something is actually malicious, and decide how urgent the response should be instead of relying on a system to handle it alone.

Cyber security work isn't just a matter of processing information or following patterns; it involves interpretation. Analysts have to think about motive, anticipate what an attacker is trying to achieve, and understand what damage could realistically happen if something is ignored. AI can process data quickly, but it doesn’t really understand context in the way a person does, especially when situations are unclear or constantly shifting.

## The Human Role in Cybersecurity

Humans are extremely important when it comes to AI in cybersecurity. Analysts code, crunch data, and solve problems, but they also use instincts and experience to figure out what is actually going on behind the alerts (Zacharis et al., 2024; Karki et al., 2024). For example, when AI flags suspicious behavior across accounts, analysts determine whether it is a real attack or a system issue. False alerts are additionally filtered out so that they don't interfere with normal business activity or trigger unnecessary disruption. On the analyst side, the team continually refine detection logic and recalibrate machine learning models using fresh, real-world threat data as it comes in. Beyond that, they are responsible for shaping response frameworks, drafting security policies, and overseeing how AI systems are trained and adjusted over time (Alowaidi et al., 2023). When they are combined, automated detection and human interpretation create a more adaptive and efficient cybersecurity environment.

Across workplaces more broadly, AI has started to reshape day-to-day operations by absorbing repetitive, rules-based tasks that previously required constant human attention, freeing people to focus on more complex decision-making. Because of that, people can spend more time dealing with complex problems that actually require critical thinking. Still, AI isn't something you can just leave alone; workers need to understand its limits and pay attention to the choices it makes (Hoza, 2025). In most cases, getting into this field means earning at least a bachelor's degree in cybersecurity or a related area, in addition to important certifications such as CompTIA Security+, CISSP, or CEH (Bureau of Labor Statistics, 2024).

Day to day, cybersecurity analysts are busy with things like going through alerts, checking systems for vulnerabilities, and making updates to security policies. When AI tools are involved, their work can also include running simulated attacks, analyzing behavior patterns, and

identifying weak spots in the system. Even though automation takes some pressure off, it doesn't replace the need for people, human judgment and experience are still a huge part of making the right decisions.

## Traditional Cybersecurity vs AI

Older cybersecurity systems often depend on set rules and preregistered patterns, which can be extremely limiting and inefficient today. Because of this, these systems sometimes aren't able to catch newer or more sophisticated and powerful threats (SailPoint Technologies, 2023). For example, a firewall has a chance of completely missing a phishing attack if it doesn't match anything it was originally programmed to detect. AI improves detection by learning from past data and updating definitions of normal behavior. While errors can occur, human analysts evaluate and refine AI systems to make sure it will be accurate (Ahmed et al., 2024). Combining AI with human input increases effectiveness and reduces risk.

## Personal Interest and Career Path

My personal interest in cybersecurity comes from how systems are being protected and how they are protected from attacks. Personally, I find it interesting how AI can be used for both defense and attacks (IBM, n.d.). I additionally agree that skills such as coding, problem-solving, and data analysis are extremely important to cybersecurity, which is similar to any other field today (SailPoint Technologies, 2023). AI helps detect threats such as phishing by identifying unusual patterns in the systems, while humans figure out whether alerts flag real risks. As cybercrime increases, the demand for cybersecurity professionals continues to grow. I am

particularly interested in how an individual can specialize in areas such as AI-based defenses or risk assessment because they combine technical knowledge with decision making.

## Conclusion

In conclusion, Artificial intelligence has changed cybersecurity so much. It makes the detection faster, improves response times and decreases the amount of work that requires human support. Even though AI plays an important role in securing networks and protecting sensitive data there will always be a need for humans to explain and solve alerts generated by AI, respond to complex attacks and to update systems. The combination of AI and human review provides stronger security than depending on one. Career opportunities in cybersecurity continue to grow, offering roles that involve working with AI to protect systems. AI alone is not sufficient to protect an organization; human review and feedback will enhance the effectiveness of AI.

## References

Ahmed, M., Okba, K., & Harous, S. (2024). Generative Artificial Intelligence for Cyber Security: Literature Review and Challenges. *Scientific Journal University of Saba Region*, *7*(2), 425–470. https://doi.org/10.54582/TSJ.2.2.109

Alowaidi, M., Sharma, S. K., AlEnizi, A., & Bhardwaj, S. (2023). Integrating artificial intelligence in cybersecurity for cyber-physical systems. *Electronic Research Archive*, *31*(4), 1–21. https://doi.org/10.3934/era.2023097

Gupta, M., Akiri, C., Aryal, K., Parker, E., & Praharaj, L. (2023). From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy. *IEEE Access*, *11*, 1–1. https://doi.org/10.1109/ACCESS.2023.3300381

Handa, A., Sharma, A., & Shukla, S. K. (2019). Machine learning in cybersecurity: A review. *Wiley Interdisciplinary Reviews. Data Mining and Knowledge Discovery*, *9*(4), e1306-n/a. https://doi.org/10.1002/widm.1306

Hoża, K. (2025). AI in cybersecurity. *Zeszyty Naukowe Wyższej Szkoły Finansów i Prawa w Bielsku-Białej, 29*(3). https://doi.org/10.19192/wsfip.sj3.2025.4

Karki, S., Hasan, A. B. M. M., & Sanin, C. (2024). Use of ML and AI in Cybersecurity-A Survey. *Procedia Computer Science*, *246*, 1260–1270. https://doi.org/10.1016/j.procs.2024.09.552

Kasakliev, N., Somova, E., & Gocheva, M. (2024). Artificial Intelligence for Good and Bad in Cyber and Information Security. *Mathematics & Informatics*, *67*(1), 82–94. https://doi.org/10.53656/math2024-1-6-art

Martínez Torres, J., Iglesias Comesaña, C., & García-Nieto, P. J. (2019). Review: machine learning techniques applied to cybersecurity. *International Journal of Machine Learning and Cybernetics*, *10*(10), 2823–2836. https://doi.org/10.1007/s13042-018-00906-1

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

Taddeo, M., McCutcheon, T., & Floridi, L. (2019). Trusting artificial intelligence in cybersecurity is a double-edged sword. *Nature Machine Intelligence*, *1*(12), 557–560. https://doi.org/10.1038/s42256-019-0109-1

Zacharis, A., Katos, V., & Patsakis, C. (2024). Integrating AI-driven threat intelligence and forecasting in the cyber security exercise content generation lifecycle. *International Journal of Information Security*, *23*(4), 2691–2710. https://doi.org/10.1007/s10207-024-00860-w