

Eugene Antwi

Matthew Umphlet

CYSE 200T

May 3, 2026

AI-assisted intrusion detection and the future of cyber defense

(1)As technology in the world advances, we are seeing that our digital infrastructure is also advancing. I believe that artificial intelligence is our new future and how we do things in our day-to-day lives. Our traditional security tools and infrastructure can no longer handle the increase in technology and technological advancements that are happening in our modern-day society. Those old tools can't keep up with the scale, speed, or threat predictability of today's technologies. Because of this, I believe that AI-assisted intrusion detection will shape our future and change the way we use it to defend ourselves. As we all know, AI is still a work-in-progress tool that won't be perfect overnight, meaning that using it for protection will also come with its own risks. In this paper, I want to address how AI can work to improve network security, security tools, and what we need to do to make AI more integrated into our future.

(2)AI can be used to massively increase and improve network security far better than traditional tools or humans can. Networks today produce lots of traffic, user data, and logs, that to a human team can be missed or under-analyzed just because we are human. A solution for this would be the use of AI in networks, which can be used to analyse for the smallest of pattern changes. AI can learn what normal networks should look like. Once the AI detects changes, it can then report these changes to the authorized users as threat notifications. An excerpt from Check Point Engage states that “Faced with these challenges, businesses are turning to AI cybersecurity solutions to level the playing field. With AI network monitoring, you can process

massive data streams in real time to improve detection accuracy and catch sophisticated, evasive attack vectors”(Check Point). With this, AI can reduce the number of network breaches and full-scale attacks that could occur due to unauthorized network access. This can tie into the CIA triad with Integrity in mind to keep users' networks safe and secure. I think that's very important because hackers day in and out are looking for stealthy and sneakier ways to gain network access and cause damage and destruction. Another excerpt from Syracuse University states that “if an AI-powered system detects ransomware starting to spread from one device, it can isolate that device from the network immediately while notifying the security team”(Syracuse University).

(3)AI cannot only help us with network defense, but it can also help with improving the security tools we already have implemented today. Keepnet excerpt states that “physical security is a critical pillar of any organization's overall security framework. It protects both people and assets from physical threats, serving as the first line of defense against breaches that can lead to data theft, operational disruption, and reputational harm”(Keepnet). This shows that physical security and other security tools are important, but they can be improved upon as technology advances. Today, AI software has been built into different surveillance tools, cloud security, and warning systems. This is all possible due to machine learning. Cisco explains that “machine learning lets computers learn without being explicitly programmed. Put another way, machine learning teaches computers to do what people do: learn by experience”(Cisco). Machine learning enables these technologies to learn to detect or stop threats on a case-by-case basis without human input. I know this may raise concerns that these systems can be hacked, making their purpose of threat detection less effective. This is why organizations and civilians should still use AI, but be cautious of it at the same time. I believe that this form of AI integration will really allow there to be fewer intrusions on companies and breaches of security.

(4)As our world continues to evolve, AI is also evolving. We can see this from when AI videos first came out to where you could easily tell that it was created by AI software, to now, not being able to tell as much if something is real or fake. This proves that AI isn't going anywhere, and we should embrace it and use it to the best of our abilities. This means we first have to learn how to responsibly use it in our lives. In the occupational aspect, Microsoft has come out with a list of 10 ways AI can be useful in the workplace. I will go over a few: “Enriched hiring process, and “improved decision making”(Microsoft). Both of these go hand in hand; the hiring process can go faster using AI because you can allow it to sift through tons of applications to match your company's requirements. Improved decision-making is in the name; AI will allow the best option to be made using input requirements. For consumer use, we can use tools like Alex, Google, and Siri for our day-to-day use on our phones and at home. All of these things sound nice, but that can't distract us from the fact that AI isn't perfect, so humans should still be able to make the final decision on things that AI might suggest to us. As I've reiterated, AI isn't perfect, so we need to be cautious as we integrate it into our lives.

I believe that AI- assisted intrusion detection can really shape our future of cyber defense. As we continue to advance as a society, we can see that AI is assisting in network security, advancing the security tools we already have today, and continues to integrate itself into our lives. Even though this sounds good, we still have to take into account that AI isn't perfect, and as it enters our society, we have to stay vigilant about our privacy, data, and the misuse of AI. While these concerns are valid, I am confident that we can use AI in security for its intended purpose. In conclusion, AI can help with network security, advance security tools, and assist with AI integration in our society.

Works cited

“AI in Cybersecurity: How AI Is Changing Threat Defense.” *ISchool | Syracuse University*, 20

July 2025, ischool.syracuse.edu/ai-in-cybersecurity/.

“Discover 10 Benefits of AI in Your Workplace.” *Microsoft.com*, 2023,

www.microsoft.com/en-us/microsoft-365/business-insights-ideas/resources/benefits-of-ai-in-your-workplace?msockid=105b89c743b16a773bba9ff8423a6b09. Accessed 23 Apr. 2026.

hillelz. “AI in Network Security - Why Cyber Defense Now Depends on It.” *Check Point*

Software, 27 Oct. 2025,

www.checkpoint.com/cyber-hub/cyber-security/what-is-ai-security/ai-in-network-security/.

“Machine Learning and Security.” *Cisco*, Mar. 2025,

www.cisco.com/site/us/en/learn/topics/security/what-is-machine-learning-in-security.html

.

Ozan Ucar. “What Is Physical Security? Definition, Examples & Best Practices (2026).” *Keepnet*

Labs, 8 Dec. 2024,

keepnetlabs.com/blog/what-is-physical-security-importance-examples-and-measures.

