Impact of AI on Cybersecurity

Teaundra Thompson

Charleston Southern University

CSCI 301 : Survey of Scripting Languages

Mr. O’Neil

3/8/2025

Impact of AI on Cybersecurity

Technology has come a long way over the past eighty years. There have been revolutionary developments such as *AI* and *ML*. The development of AI has provided many benefits to society, but also many drawbacks and possible dangerous consequences in the future. My major is *Cybersecurity* and AI poses both benefits and dangers to technological security infrastructures. One-way programmers and IT professionals try to mitigate these dangers by following a code of ethics. There are two codes of ethics that are followed, the ACM and IEEE code of ethics. The ACM code of ethics states that computing professionals' work should be beneficial to society, and their work should not produce harm (2018). Integrity and trustworthiness are also required characteristics of a computing professional according to the ACM (2018). Professionals should also foster equity and fairness and avoid discrimination against marginalized groups (*ACM Code of Ethics and Professional Conduct* 2018). Computing professionals are also required to credit the creators of work they may use or cite (*ACM Code of Ethics and Professional Conduct* 2018). There is a special emphasis on the protection of data in the ACM code of ethics; professionals should be sure to create systems that are secure and constantly monitor and maintain these systems (2018). As the name suggests, a computing professional must maintain a professional demeanor and character; that includes their work and social interactions with others (*ACM Code of Ethics and Professional Conduct* 2018). If a computing professional has a position of leadership, they should "ensure that the public good is the central concern during all professional computing work" and follow all the typical duties required of a leader (*ACM Code of Ethics and Professional Conduct* 2018). Finally, a computing professional should follow and heed the ACM code of ethics and hold other members accountable for code violations (2018). The IEEE code of ethics follows nearly the same code of ethics as the ACM, but is emphasizes the "safety, health, and welfare of the public" (2020). Due to the focus of engineering of the IEEE code of ethics there is no special emphasis on protecting and securing digital data unlike the ACM code of ethics (2020). These codes of conduct provide guidelines for computing professionals and engineers.

AI as a Double-Edged Sword

As the world of computers and technology are rapidly evolving, so are the uses and functions of AI. The number one benefit of AI is its capability to complete various tasks free from human error (IBM, 2025). It can automate tasks and complete tedious repetitive tasks in a split second effortlessly. When it comes to AI in cybersecurity, it has major benefits and detrimental drawbacks. AI can help companies analyze patterns and entity behaviors to determine if there is an impending cyber-attack (Human, 2025). On the other hand, hackers can use AI to improve their infiltration methods, increasing the occurrence and successfulness of cyber-attacks (*The near-term impact of AI on the cyber threat 2024*). Without AI, security analysts would need to review massive amounts of data to detect threats and anomalies, but AI can review large quantities of data at a rapid speed (*The near-term impact of AI on the cyber threat 2024*). A component of AI that is used often in the field of cybersecurity is Machine Learning (ML). ML learns from data and analyzes patterns and can make decisions with little to no human intervention (Khan, 568). ML also can improve threat detection and responses to threats (Khan, 568). Along with the benefits AI brings to Cybersecurity, it also brings some ethical concerns. Due to the fact AI can complete certain jobs much faster than a human, such as analyzing a large amount of information, it has the potential to take jobs from people and completely automate them (OZDEN, 92). AI uses data created by humans, and therefore some biases can be present in the data making AI biased also. This can lead to discriminatory results when it comes to AI implementing security measures or things of that nature (OZDEN, 92). AI often uses large amounts of personal data to function properly, so this raises concerns about the privacy of individuals and how their data is used (OZDEN, 92). AI is ever evolving and so are the ethical problems along with it.

Ethical Concerns

As humans, we have some biases, and sometimes some prejudices. This can lead to AI obtaining some of those same biases and prejudice due to it relying on humans to learn. According to the ACM code of ethics, we as professionals should not have such biases (2018). Galatians 3:28 says "There is neither Jew nor Gentile, neither slave nor free, nor is there male and female, for you are all one in Christ Jesus."(NIV). Both the ACM code of ethics and the Bible agree that professionals should not have discriminatory biases, and by working to eliminate these internal biases AI would not model those preconceptions in it is work. When it comes to AIs access to vast amounts of personal data on individuals, the ACM says that we must avoid harm and have integrity (2018). If AI has access to sensitive personal data, individuals must be made aware of it and their consent for such access should be inquired for beforehand. Proverbs 10:9 says, "Whoever walks in integrity walks securely, but whoever takes crooked paths will be found out." Making sure AI has permission from individuals to access information is crucial, because if consent is not given the legal drawbacks will be detrimental to companies. The ACM and the Bible agree that individuals should be aware of the possibility that AI can access their personal information, and they should be able to choose if they will allow that. As technology progresses, jobs are becoming more automated, and AI has the potential to take jobs from people working in Cybersecurity. The ACM code of ethics says that care should be taken when modifying or changing systems, and if a change has a negative effect there should be a rollback (2018). In Proverbs 14:31 it is said "Whoever oppresses the poor shows contempt for their Maker, but whoever is kind to the needy honors God". According to this verse, it is wrong for AI to completely automate jobs because that would oppress professionals in cybersecurity and prevent them from providing for their families. CEO's and President's will face consequences down the line if they completely automate their corporations. AI should be used to assist professionals in their work instead of taking their jobs. Humans will still be needed to monitor these AI systems because of their unpredictability at times.

Professional Ethics and Christian Ethics

In all honesty, majority of the principles in the ACM code of ethics are derived from Christian ethics and values. Principles such as integrity, honesty and responsibility which is present in the ACM code of ethics are core principles of Christianity. On the other hand, the Bible does not address anything about computers and AI, but the ACM does. The ACM provides clearer ethical principles in areas where the Bible does not, but these principles are still Christian-like. For example, The ACM Code of Ethics says that a computing professional should contribute to the welfare of society and to human well-being (2018). The Bible speaks about doing well unto other several times, for example in Hebrews 13:16 “And do not forget to do good and to share with others, for with such sacrifices God is pleased.” Both the ACM code of ethics and the Bible combines, sufficiently address the ethics surrounding AI. They both support each other, and they are also strong enough to be used independently.

Conclusion

The biggest concern about AI is the idea that one day it may overthrow humankind and wreak havoc on our world, but with Christian and professional ethics such a thing will not occur. These ethics keep technology in check and provide a safe work environment for professionals. AI can provide many benefits to the work environment and make Cybersecurity professionals more productive, but it is imperative for those in leadership to train their employees on the ethical uses of AI to prevent bias and data leaks. Privacy and security are two main components of Cybersecurity, and sometimes AI does not obey those rules, so ethics are important to keep AI in check.

References

ACM Code of Ethics and Professional Conduct. Association for Computing Machinery. (2018). https://www.acm.org/code-of-ethics

Human. (2025, February 13). *AI in cybersecurity: Pros and cons*. HUMAN Security. https://www.humansecurity.com/learn/blog/ai-in-cybersecurity-pros-and-cons/#:~:text=Enhanced%20Threat%20Detection%20and%20Prevention.%20Threat%20detection,from%20normal%20patterns%20and%20identifying%20potential%20threats.

IBM. (2025, February 14). *What is Artificial Intelligence (AI)?.* IBM. https://www.ibm.com/think/topics/artificial-intelligence

IEEE Code of Ethics. IEEE. (2020). https://www.ieee.org/about/corporate/governance/p7-8.html

Khan, M. I., Arif, A., & Khan, AR. A. (2024). The Most Recent Advances and Uses of AI in Cybersecurity. *BULLET : Jurnal Multidisiplin Ilmu*, *3*(4), 566–578. https://journal.mediapublikasi.id/index.php/bullet/article/view/4540.

NIV Bible | YouVersion. (n.d.). YouVersion | the Bible App | Bible.com. https://www.bible.com/bible

OZDEN, C. (2023). AI ethical consideration and cybersecurity. *International Studies in Social, Human and Administrative Sciences-I*, *85*.

The near-term impact of AI on the cyber threat. NCSC. (2024). https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat