Ethical Implications of Artificial Intelligence

Zachary D. Weaver

Department of Computer Science, Charleston Southern University

CSCI 210: Introduction to Computer Science Through Robotics

Professor Michael O’Neill

October 26, 2024

Ethical Implications of Artificial Intelligence

Cybersecurity is an ever-changing field relative to computer science and involves protecting information systems, networks, and data from all types of security breaches and malicious attacks. As technology continues to expand, cybersecurity is a crucial component to safeguarding personal data and IT infrastructure. Cyber professionals are entrusted with tools like artificial intelligence (AI) that can impact the privacy and security of others. This leads many to question what the limits should be for AI in a field that so heavily revolves around information system security. To answer these questions, ethics must be used as a guideline for responsible behaviors to ensure integrity and accountability are implemented in every situation. Analyzing ethical issues using the ACM Code of Ethics and a Christian worldview allows for a deeper understanding of how to navigate the ethical implications of AI in the cybersecurity community.

Impact of AI in Cybersecurity

With AI becoming more popular in many computing industries, we must first examine how it will impact the field of cybersecurity. Cyber threats are always evolving in both frequency and complexity. In cybersecurity specifically, AI can offer enhanced detection and prevention measures that can be used in response to common attack methods. Over the past few years, many organizations have researched the security implications of AI and machine learning in corporate environments. To many, AI has provided a way to keep up with constant barrages of cyber attacks. An article written by World Wide Technology goes into detail explaining how the benefits of AI have been embraced among cyber operations. It reads, “The sheer amount and complexity of data and threats, in the midst of an ongoing talent shortage, have become impossible to tackle” (*Embracing the Benefits of Generative AI in Cybersecurity Operations,* 2023). With so many available jobs in cybersecurity, AI can mitigate a lack of filled cyber positions or threat detection mechanisms. The article goes on to explain how AI has been a beneficial innovation that security professionals desperately need in order to keep up with constant adversarial attacks.

Using artificial intelligence can be both a useful tool and a malicious vulnerability which is why its future implementation must continue to be done carefully and ethically. The Cybersecurity and Infrastructure Security Agency (CISA), has identified five key lines of effort (LOEs) that will be used going forward to ensure AI is implemented responsibly and ethically. The first LOE explains, "CISA's adoption of AI will ensure responsible, ethical, and safe use-consistent with the Constitution and all applicable laws and policies, including those addressing federal procurement, privacy, civil rights, and civil liberties" (*Artificial Intelligence, n.d*). AI has the power to process vast amounts of sensitive data. If used maliciously, having this amount of power could lead to invasions of privacy and system exploitation, which is why CISA is dedicated to a national AI implementation strategy that protects critical and personal infrastructures. One of the biggest ethical concerns with AI usage in cybersecurity is the invasion of privacy through automated monitoring systems. Privacy has always been a predominant issue in the field of computing as seen by the creation of data privacy laws like the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR). AI systems that are designed to monitor networks for potential security threats may inadvertently collect personal data leading to privacy violations which constitutes the need for a systematic way to evaluate ethical decision making.

Ethical Analysis

As we continue to learn more about AI and machine learning, the future of cybersecurity will include continued AI integration with cyber defense tools and practices. Knowing what to do when faced with an ethical decision is crucial in a field that so values confidentiality, integrity, and availability.

Professional Ethical Principles

Over the years, multiple ethical codes and methodologies have been created to evaluate ethical decision-making. The Association for Computing Machinery (ACM) Code of Ethics and Professional Conduct focuses on key principles that encourage computing professionals to protect society from abuses in AI technology. General principles like “Avoid Harm” and “Respect Privacy” emphasize the need to protect people from unethical uses of AI like privacy breaches (Association for Computing Machinery, 2018). Additionally, the ACM general ethical codes encourage cybersecurity professionals to design systems that prevent AI misuse of personal information.

Christian Worldview

One of the greatest driving factors when it comes to ethics is personal beliefs. As Christians, making ethical decisions should be grounded in principles that honor responsibility, morality, and personal sanctification. The Bible teaches us that, as followers of Christ, we ought to uphold truth, honesty, and integrity in everything that we do. Proverbs 11:3 says, “The integrity of the upright guides them, but the unfaithful are destroyed by their duplicity” (*New International Version,* Proverbs 11:3). This verse reminds us that cyber professionals should act with integrity and commit to ethical standards. Just as the upright are guided by integrity, ethical AI use requires a commitment to respecting the privacy of others. Moreover, avoiding duplicity means we must also refrain from deceptive or malicious practices. Another key verse that describes how we should act as Christians is Colossians 3:23. It reads, “Whatever you do, work at it with all your heart, as working for the Lord, not for human masters” (*New International Version,* Colossians 3:23). This verse emphasizes the importance of committing to excellence and selflessness. When developing and implementing AI, we must always strive for high standards that prioritize others' needs above our own. When faced with ethical issues concerning the use of AI, making decisions from a Christian worldview ensures AI is used appropriately and puts the focus on serving others rather than personal ambition.

Methodology & Application

While the ACM’s ethical principles and a Christian worldview provide a good foundation for ethical decision-making, having an in-depth process built on those principles and beliefs provides a more consistent and applicable approach when faced with moral dilemmas. One methodology developed by the army outlines a six-step approach that cyber professionals can apply when ethical issues arise. The steps are as follows:

1. Understand the situation or environment.
2. Define the situation or problem.
3. Develop an approach to the issue.
4. Consider and evaluate any biases or assumptions.
5. Decide and implement a course of action.
6. Continuously assess the situation, problem, and approach.

Applying this approach to ethical AI use in cybersecurity gives us a structured way to make decisions. One issue that can be analyzed as an example is the use of AI threat detection and user profiling. As previously mentioned, AI systems are being used more to monitor network traffic and examine potential security threats by viewing a user’s online behaviors. While this type of defense mechanism can be beneficial to a systems security posture, it still raises ethical concerns about user privacy invasion. Using an ethical methodology, a cyber professional must first recognize, understand, and define the issue of user privacy invasion. After approaching and analyzing the issue, a decision must be made to address the ethical issue. It is in this decision-making step, that foundational principles and worldviews must be applied. Once the decision is made, a solution can be implemented like setting limits on AI data collection to further protect users' privacy. Finally, the cyber professional must continually assess their decision and adapt their solutions as security needs evolve.

Comparing Viewpoints

Comparing the ethical perspectives of both the ACM Code of Ethics and a Christian worldview leads to several similarities and differences in how both address the issue of AI ethics. To begin, both perspectives emphasize respect for privacy and integrity. While the ACM advocates for ethical principles like avoiding harm and respecting privacy, a Christian worldview similarly values principles of honesty and integrity. Both viewpoints encourage actions that honor the well-being of others while also recognizing our ethical duty as Christians to serve Christ. While there are some similarities to the two viewpoints, differences also arise in the motivation behind these fundamental ethical values. The ACM’s ethical guidelines are centered around professional responsibility and can be used to promote ethical AI use through secular principles. The Christian perspective, on the other hand, is instead grounded in faith and emphasizes service to Christ and stewardship over one's personal morals. Even though both viewpoints advocate for ethical action, the Christian worldview additionally prompts cyber professionals to view their work as a service to a higher calling.

Conclusion

The future integration of AI in cybersecurity will undoubtedly present many significant opportunities and ethical challenges. AI tools have many benefits including enhancing threat detection and streamlining data security however, some of these benefits come with additional concerns around user privacy and data integrity concerns. Ethical frameworks like the ACM Code of Ethical Principles offer guidance in respecting the privacy and safety of others while a Christian worldview adds a moral lens rooted in honesty and serving others. When paired with a structured methodology, ethical viewpoints provide a comprehensive approach to addressing issues with AI ethics in cybersecurity. Understanding how to ethically approach a decision-making process is one of the many ways cyber professionals can strive for excellence.

References

Artificial Intelligence | CISA. (n.d.). Www.cisa.gov. https://www.cisa.gov/ai

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

Department of the Army. (2020, November 27). *Moral leadership* (Pamphlet 165-19). U.S. Department of the Army.

Embracing the Benefits of Generative AI in Cybersecurity Operations. (2023, July 24). Www.wwt.com. https://www.wwt.com/article/embracing-the-benefits-of-generative-ai-in-cybersecurity-operations

ISC2. (2024, January 24). *The Ethical Dilemmas of AI in Cybersecurity*. Www.isc2.org. https://www.isc2.org/Insights/2024/01/The-Ethical-Dilemmas-of-AI-in-Cybersecurity

New International Version. (2011). BibleGateway.com. http://www.biblegateway.com/versions/New-International-Version-NIV-Bible/#booklist