Ethan Lawson

04/16/2025

# The Role of Artificial Intelligence in Cybercrime

Topics Relation to the Principles of Social Science:

Artificial intelligence (AI) is only going to become more advanced, and it is already difficult to tell what has been created by it. AI powered/created bots, deepfake technology, and phishing schemes can identify and exploit human psychological weaknesses. There have already been multiple cases of deepfake technology and bots being used for gaining trust to steal important information. AI bots have become so adaptable for social media purposes that they can create videos instantly and formulate responses to posts that are likely to garner the most attention/money. These bots are so prevalent they can sway public opinion by influencing collective behavior. Objectivity is crucial to datasets used to train AI models because they can amplify bias.

Study's Research Questions or Hypotheses:

With the growing usage of AI driven cyberattacks, it has become necessary to incorporate this new technology and techniques into cyber defense systems (Dilek et al., 2015). Doing so would significantly improve detection, prevention, and response by improving the adaptability and flexibility of defenses. The learning capabilities of AI can help address gaps in remediating the sheer volume and complexity of threats.

Types of Research Methods:

The research methods used in this article are a literature review of experimental research and case studies which apply AI to combat cybercrime by various methods.

Types of Data and Analysis:

The data used in this article was references to many others who have incorporated neural networks and AI into intrusion detection/prevention systems. To be trained for usage against cybercrime AI needs access to many types of data. Some examples of such data include malware signatures, baseline for normal operations, common phishing attempts, performance metrics, and historical and global cybercrime activities. Human intervention has become inadequate in addressing new cyberattacks. Researching and developing autonomous AI driven defenses that surpass human intelligence is the future of combating cybercrime.

Relation to PowerPoint Presentations Concepts:

Human factors relate to developing AI because our bias, human error, limited understanding of this technology, and fear slow its growth. Cyberpsychology relates to this article because our behavior and psychological states are impacted by its use. Threats is a related concept because

AI has created countless ways for attackers to use it maliciously. Another is perception of safety which AI driven intrusion prevention/detection systems will change our view of.

Relation to Challenges, Concerns, and Contributions of Marginalized Groups:

Vast amounts of data are needed to train AI models. Continuing to develop such systems would increase the amount of data farming and the information of marginalized groups could be misused or over-exploited. If the datasets used to train AI models include biased data algorithms it can perpetuate or amplify this. We may be approaching a time when the human race is the marginalized group.

Overall Contributions of Study to Society:

Some notable contributions to society that such research might create are improved threat detection and response, public safety, privacy, cost reduction for organizations, innovation in the field of cybersecurity, and creation of international standards and guidelines for its usage.

Conclusion:

In conclusion, the relationship between AI and cybercrime is complex. Traditional defense mechanisms that we count on are growing inadequate due to the constant evolution of cyberthreats. The widespread malicious use of this technology already exists so it is time to make it more common defensively. Further development will create revolutionary breakthroughs for cyber defense systems. However, "A wide range of both ethical and legal questions come up in light of the potential autonomy of this technology." (Dilek et al., 2015). Sadly, new ways that AI is used maliciously will continue to flourish as well.

## Reference

Dilek, S., Cakır, H., & Aydın, M. (2015i). Applications of artificial intelligence techniques to Combating Cyber Crimes: A Review. *International Journal of Artificial Intelligence & Applications*, *6*(1), 21–39. https://doi.org/10.5121/ijaia.2015.6102