Artificial Intelligence and Applications in Cyber Criminology

Jason W. McCarthy

Old Dominion University School of Cybersecurity

CYSE 201S: Cybersecurity and the Social Sciences

Professor Yalpi

October 2, 2024

Table of Contents

Artificial Intelligence and Applications in Cyber Criminology

Introduction

AI in Cybercriminology can be game-changing in both positive and negative ways. While it has the potential to make the process of empirical research smoother when performing tasks related to data collection, ethical considerations are in play. Depending on how the AI model is trained, objectivity could also be negatively impacted. The study on the applications of Artificial Intelligence Techniques to Combatting Cybercrimes: A Review looks at how Artificial Intelligence can deter multiple types of cybercrime, including computer intrusion and Computer Worm detection on Metropolitan Networks.

The Need for Human Oversight

When looking at the application of Artificial Intelligence being used as an IDPS, or Intrusion Detection and Prevention System, the article lays out what this should look like. The recommendations include limited human oversight (Dilek et al., 2015). This brings into question the validity of the data being received and used. If no oversight is in place, then the data collected for research and preventative purposes isn't being reviewed to ensure no bias exists in the dataset. One of the implications of detecting cybercrimes is the need to attribute them to groups or individuals. Often, these crimes occur from overseas sites, and naturally, these crimes are committed by terror cells or state-organized groups where the groups are a minority in the United States. However, when the crime occurs domestically, it is easy to trace the connection back through the internet provider and make assumptions about the personal data collected. When one person in a neighborhood or a group commits such a crime, a focus is often put on an entire neighborhood or to watch for further crimes.

Objectivity

Objectivity is important for the integrity of any information used to combat cybercrime and for ensuring that it is used responsibly by the Artificial Intelligence entity. The system can use this data to adapt to user behavior over time (Dilek et al., 2015). Therefore, such a system should be trained to use the data collected on all users and not just a subgroup or subset. Implementing objectivity throughout the development process and having outside parties review the work is important.

Conclusion

A well-known example of using AI to combat crime is surveillance technology, such as security cameras, that use facial recognition to collect images. These systems can easily be manipulated to collect data on a discriminate basis against any race, not just minorities. Laws highly regulate such systems; likewise, a system like the one discussed in this article should be subject to similar regulations to ensure it is used ethically. While AI can combat cybercrime and crime alike, it is the responsibility of those involved to ensure that those methods are being used in a manner conducive to society.

References

Dilek, S., Cakir, H., & Aydin, M. (2015, February 12). *Applications of artificial intelligence ...* arXiv. https://arxiv.org/pdf/1502.03552