The Social Impact of Predictive Cybersecurity Systems

Hamzah Zuhrah

CYSE 200T: Cybersecurity, Technology & Society

Old Dominion University

April 2026

(1) Cybersecurity has changed a lot in the last few years, mostly because of new technologies like AI and machine learning that can anticipate what will take place. These systems analyze chunks of data to locate threats before they even happen. At first, this seems like a big step forward, and in many ways, it is. But I also think it raises some important questions. When I think about this in terms of the *Short Arm of Predictive Knowledge*, it's clear that these systems can't predict all future cyberattacks. Because of this, overly depending on them may lead to problems like bias, privacy issues, and relying too much on automation.

Predictive cybersecurity systems have some clear advantages, especially when it comes to how quickly and effectively they work. Most of the time, old-fashioned cybersecurity tools only work after an attack has already happened, which can do a lot of damage. Predictive algorithms, on the other hand, look for patterns in network data to spot suspicious activities early on. For instance, machine learning algorithms can find strange traffic and flag it as a possible threat much faster than a human analyst (Journal of Cybersecurity, 2021). This helps companies act quickly and, in some cases, even stop attacks before they happen.

(2) Predictive cybersecurity is also helpful because it makes mistakes less likely to happen. Many problems with cybersecurity happen because of simple mistakes, like using weak passwords or setting up systems wrong. Automated systems are more dependable because they can keep an eye on networks all the time without getting overwhelmed. I saw this for myself when we had to analyze network traffic by hand in

one of my CYSE labs. It taught me how easy it is to miss even the smallest of details. To help with this problem, predictive systems are always looking for strange behavior. The International Journal of Cybersecurity Intelligence & Cybercrime also agrees with this idea, saying that automation makes systems more stable and secure in general (2022).

These systems do have some good points, but they also have some bad ones. According to the *Short Arm of Predictive Knowledge*, predictions are always based on data from the past. These systems can only see patterns they have already seen because of this. This is a problem when new kinds of cyberattacks come out. If a system hasn't been trained to recognize a certain attack, it might not be able to find it. It could also mistakenly flag normal behavior as suspicious, which would be a false positive.

(3) Another problem is that algorithms can be biased. The International Journal of Cyber Criminology says that biased datasets can make it harder to find real threats. This could mean that big risks are missed or that alerts that aren't needed go off (2023). This could make people feel safe when they shouldn't, because they trust the system even when it makes mistakes. Over time, relying on wrong predictions can make cybersecurity strategies less effective.

Another big worry is privacy. For predictive systems to work well, they need to be able to see a lot of data, like how users act and what happens on the network. This makes us think about how much monitoring is right. More surveillance may make people safer, but it can also be intrusive and violate people's privacy. It's still hard to find the right balance between privacy and security, and the issue hasn't been fully resolved yet.

(4) Some experts say that predictive cybersecurity systems will keep getting better as more data is collected and algorithms get better. This is a fair point, but it doesn't completely solve the problem of unpredictability. Cyber threats are always changing, and no system can be completely ready for attacks that have never happened before.

Some people think that tougher rules and laws can help lower these risks. Rules can be useful, but they often don't keep up with new technology. Because of this, there is often a gap between innovation and regulation, which can make things even harder.

In conclusion, predictive cybersecurity systems have clear advantages, especially when it comes to speed and efficiency. But when you look at these systems through the *Short Arm of Predictive Knowledge*, you can see that they have some big problems as well. They depend on old data, which makes it hard to find new threats, and they raise concerns about privacy and bias. Instead of taking the place of human decision-making, predictive systems should help people make decisions. Cybersecurity experts are still needed to assess threats and make smart choices. Companies should keep making these systems better, but they should also be aware of what they can't do.

In the end, there is no one perfect way to protect your computer from hackers. There will always be some level of uncertainty, even with the best predictive technologies. It is through accepting and acknowledging this limitation that we can as a society learn how to take a more balanced and responsible approach to cybersecurity. Organizations can make things safer and deal with the moral and practical problems that come with new technology by using both predictive technologies and human judgment.

References

- International Journal of Cyber Criminology. (2023). Algorithmic bias in cyber threat detection. https://www.cybercrimejournal.com/

- International Journal of Cybersecurity Intelligence & Cybercrime. (2022). The role of automation in modern cybersecurity systems. https://vc.bridgew.edu/ijcic/

- Journal of Cybersecurity. (2021). Machine learning and predictive analytics in threat detection. https://academic.oup.com/cybersecurity