PakTech Today | Pakistan's Premier Technology Magazine
Vol. 01, Issue 05 • May 2026

TECHNOLOGY FEATURE Industrial News / Technology Report / Research Communication

AI vs AI: The invisible Cyber war shaping our Digital Future

There exists an invisible cyber war in which artificial intelligence acts as the attacking and defending agent for the future of cybersecurity.

By **M. Talal Ashraf** | Affiliation / University of Agriculture, Faisalabad | Published: 12th April 2026
talalashraf1585@gmail.com | Student / Computer Science

Introduction

With the evolution of artificial intelligence (AI), our lives have changed and so has the way we deal with any kind of cyber threat. The development of AI technology has led to a whole new era of cyber warfare, where the use of AI is seen on both sides of the attack and defense fronts. This invisible warfare is changing the entire perspective of digital security and comes with its own set of advantages and disadvantages. In this paper, we will examine the rising trend of AI attacks, their defenses, and issues related to them.

The Rise of AI-Powered Cyber Threats Impact

The advent of AI has brought about a drastic change in the dynamics of cyber attacks. In the past, human intelligence was used to detect and combat any kind of cyber attacks. However, in today's world, hackers have employed AI technologies that can scan, penetrate, and adapt to evade detection. For example, in cases where Russia has attacked Ukraine through the internet, the NotPetya malware program powered by AI has been employed.

Defense in the Age of Intelligent Machines

The application of AI is also enhancing the capabilities of cyber security defense mechanisms. The AI system assists the Blue Teams in monitoring vast volumes of data on the network for any suspicious activity, which may indicate an impending attack. Prior to the occurrence of the attack, the AI system assists the Blue Teams in understanding their environment and detecting any vulnerability. The use of tools like intrusion detection systems has become increasingly important in detecting and preventing any attacks.

The Role of Data and Automation

The use of artificial intelligence in relation to cybersecurity requires access to substantial amounts of information because the system requires analyzing large amounts of data in order to determine whether there are any trends that may lead to cyber-attacks. This technology will use such a huge amount of information to determine whether there are any trends in the network that might lead to cyber-attacks. One thing about the effectiveness of this technology is that it depends on the quality of information used. Google created a software called CodeMender that utilizes artificial intelligence in analyzing codes and determining their weakness and offering solution to address this weakness. Apart from analyzing codes, artificial intelligence can be used in cybersecurity for other purposes.

© PakTech Today

Future Risks: Beyond Human Control?

As AI technology continues to develop, there are worries that its ability will outstrip the ability of human control, whether offensive or defensive. Sophisticated AI-based cyber threats that tamper with data and not just steal them create a serious security threat for industries that depend on critical data. As the AI technology can function autonomously, unintended consequences can result, and defense measures will lead to severe interruptions. This lack of control represents a huge shift in cybersecurity as systems grow increasingly complicated due to IoT advancements.

The Need for Ethical and Secure AI Development

As for this issue, it is necessary to pay attention to the importance of moral issues related to AI development when considering the ways the future of artificial intelligence may impact our lives. First of all, it is necessary to acknowledge the fact that any unethical practices, biases in the operation of algorithms, insufficient testing of AI software, etc., may lead to various hazards that include privacy breach and exploitation of vulnerabilities in critical infrastructures. It should be stated that all the aforementioned problems have occurred when developing software products using AI technology. Therefore, it becomes clear that it is crucial to cooperate with each other and develop certain standards that will ensure safety in relation to artificial intelligence. In addition, at present, another problem appears to be important regarding AI, which pertains to cybersecurity. Thus, one can say that it is time to emphasize the importance of AI ethics.

Conclusion

The power of AI is not only a threat but also an active player in the emerging cyber war. This unknown battle of AI opponents and defenders will keep reshaping the cyberspace. In the ongoing cyber war, both the opponent and the defender will make use of AI. However, without controlling the technology of AI, the threats are still inevitable. The ethical development of AI, cooperation worldwide, and vigilance are some of the essential elements to ensure that AI will contribute positively to the cyber world.

About the Author

M. Talal Ashraf studying Computer Science and particularly interested in edge computing, cybersecurity, and future developments in decentralized data storage systems. They can be reached at talalashraf1585@gmail.com.

Keywords: Artificial Intelligence; Cybersecurity; IoT; Digital War; Computer Science; Pakistan Tech

References

[1] RAND Report (2018) How Artificial Intelligence could reshape future warfare.

[2] Eric Schmidt, Henry Kissinger, Daniel Huttenlocher (2021) The age of Ai: And our Human Future.

[3] Yuri Diogenes, Erdal Ozkaya (2018) Cybersecurity: Attack and Defense Strategies.

[4] Nicole Perlroth (2021) This is how They tell me the world ends.

[5] Public Agenda (2020) Rewiring Democracy.