IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# Artificial Intelligence and Cyber Threats

Ashok Kumar Reddy Nadikattu

*Sr. Data Scientist & Department of Information Technology*

*California USA*

**Abstract**

Artificial intelligence can ingest massive data and assimilate information into the system of the user. The AI algorithms apply training data that ensures people and enterprises learn how to respond to various situations. Thus, they learn by adding and copying additional data they are working with into the system with multiple software that can quickly detect the malicious attack, and AI helps determine what can be done in this situation. Through this, artificial intelligence has gained dominance in affiliated organizations across the world. The solutions AI provides for industries make it to be considered as an improvement in technology that helps the data to stay intact and away from criminals, and this is what enterprises prefer. All the changes created by artificial intelligence do not give organizations credit to relax and assume their system is in reasonable control, but they are expected to determine new ways in which artificial intelligence and machine learning can prevent malicious attacks forever. Following the above concepts, it is essential to apply literature that can provide data collection alternatives and have authentic information concerning artificial intelligence. Hence, the primary ideas addressed in the paper include how organizations use artificial intelligence to counter cyber threats, how AI improves cybersecurity, and how the information can be helpful to individuals and enterprises in the United States.

**Key Words:** Artificial intelligence (AI), Cyberthreats, Cybersecurity, Malicious attacks.

**Introduction**

In the last decade, the enterprise attack surface has grown and evolved rapidly, making the organizations frequently calculate the organization's risks. In response to the issues, artificial intelligence tools are commonly implemented to deal with cyber threats. Artificial intelligence (AI) has helped more organizations to improve the security posture effectively and reduce the breach risks. Machine learning and artificial intelligence are the essential tools in technology for information security as it helps companies and individuals to check and analyze the threats posed to the organization. The analysis starts from malware exploiting and identifying unwanted behaviors that might direct to downloading malicious software or experiencing

phishing attacks. The technologies have been improved to learn on and determine from the past how the criminals can display the new type of cyber threats. Current studies have focused on giving ideas on how artificial intelligence can be used to improve cybersecurity. The connection can be directed to organizations using the same steps to improve cyber threats and reduce chances for malicious attack.

Technology professionals have progressed in ensuring the efficiency of artificial intelligence is increased to help deal with the threats posed to organizations. An example of this is the training efficacy of Machine Learning, whereby stable ML applications are introduced every day to make sure the organizations' computer threats are dealt with. These include the attempts that help the organization produce and monitor data that the criminals may not attack. Artificial intelligence works in three ways Assisted intelligence, Augmented Intelligence, and Autonomous intelligence. Under assisted intelligence, the attempts of people to use AI are improved. Augmented intelligence allows companies to do what they could not do before when they experienced a cyber-attack. Autonomous intelligence is the solution developed for the future to help enterprises deal with threats. The connection to how artificial intelligence works is linked to data representations and improving cyber threats. Artificial intelligence allows cybersecurity systems to undertake human-like tasks and give protection to them. Thus, AI is approved in detecting and preventing high-risk network behaviors. Considering the above outline, it directs to the primary reason for having the entire discussion, which checks on how artificial intelligence is applied in countering cyber threats, how AI improves cybersecurity, and how the Research will help the United States.

**Literature Review**

**How Artificial Intelligence is used to counter cyber threats**

AI in cybersecurity is treated as an improvement in technology in instances that cyber threats are bothering the security of organizations and people. The first step for an organization is to understand what threat intelligence handles. Threat intelligence deals with evidence-based knowledge that includes actionable implications, indicators, mechanisms, and context advice on the trends in cyber threats. Threat intelligence allows the analysts to access all the information they need to be ahead of the criminals and threats and take the appropriate and accurate steps in dealing with the threats. Artificial intelligence helps in managing cyber threats. For example, the company can reduce the time they take to recover when they experience a security breach, which will make them avoid financial losses. AI ensures there is a faster response in times of cyberattacks. Artificial intelligence has the ability to process unstructured information in a cyber threat efficiently. With this regard, it learns and monitors the behavior at a fast speed to ensure plenty of response time that assists in avoiding all the forms of cyber threats. Furthermore, artificial intelligence can be used in finding the threat patterns by using leverage as a method to deal with threat intelligence feeds. Under this, the event logs and vulnerability information are determined and allow the organization to be proactive and prepare security insights systematically.

AI has been applied in impacting all primary modern industries that deal with data-driven models

that can be found in machine language. This has made more companies focus on network security as they know what risks can be got in high or minor cyber threats. In the cyber threat intelligence space, more is being discovered daily since companies use millions of dollars to get the AI services, indicating its impact on the company. Thus, more specialized artificial intelligence techniques are used in identifying threats faster than in previous years. AI has created room for improved cyber threats intelligence programs that companies use in reducing the threats directed to affect their operations. Artificial intelligence is helping organizations to counter cyber threats by avoiding managing backups and firewall systems (Hoadley & Lucas, 2018). AI is involved in introducing new solutions to cybersecurity issues and ensuring such traditional methods are not used in the future.

Artificial intelligence helps cybersecurity organizations to detect the threats posed to their data by using complex algorithms. Through this, the enormous quantities of risk data can be dealt with in a faster way. Thus, artificial intelligence supplements the security systems which lack more and accurate security resources. With this regard, it is responsible for assimilating information and ingest massive data into the organization's design that needs to ensure the threats are reduced and cannot impact the performance (Srivastava, Bisht & Narayan, 2017). The reasoning systems that AI operates with help people develop and learn new cyber threat patterns. Under this, it indicates a specific growth in cognitive abilities of how the threats are handled, making artificial intelligence augment cybersecurity to be considered the natural choice (Vähäkainu & Lehto, 2019). Furthermore, AI is used by firms to counter cyber threats by unlocking new potentials. It allows new technology processes to be discovered to ensure the risks are reduced.

Artificial intelligence is essential in studying some unusual activities experienced in the system of the organization (Li, 2018). In a case where all things are connected to the network in the company, the firm needs a lookout for the unusual activities that can affect its performance, and AI is responsible for the task. Artificial intelligence is necessary for empowering the cybersecurity systems to maintain the authorized figures in the company's system when it's finding unauthorized activities (Parrend et al., 2018). For this instance, it is connected to running tests that allow the organization to adapt to changing strategies that help in preventing cyber threats. The tests keep companies and individuals informed of the matters concerning cybersecurity and how they can be handled (Calderon, 2019). Most organizations prefer to use AI-driven platforms other than singular AI-based management products as the AI-driven platforms can enhance security in a company's systems.

Artificial intelligence is necessary for detecting the loopholes in the systems of an organization. It can consume heaps and tons of loads of information that shows how the company can progress in preventing cyber threats. The voracious thirst for new data and processing through huge information allows artificial intelligence to attach to the system's database and determine the loopholes (Trifonov et al., 2018). Furthermore, AI is applied in analytics of data, which makes it to have the ability to ward off the threats posed to a company's system. It ensures that detecting threats is faster and has practices that can help companies determine what

they can do to deal with cybersecurity. An example of this is how SAP NS2 allows the technology to be applied in a real-life situation by allowing fusion technologies and data analytics to learn and accumulate cybersecurity measures. To the national security officials, artificial intelligence and machine learning, when combined, help in processing troves of data and delivering a robust system applied in protecting sensitive data from unauthorized individuals.

**How Artificial Intelligence Improves Cybersecurity**

The impact of AI on cybersecurity can be explained through concepts like threat hunting. Traditionally, indicators and signatures were used in identifying the threats. The techniques may have been effective in those days, but it's hard to use such approaches due to the development of technology. AI has led to the introduction of signature-based techniques that can help an organization detect 95% of threats. In this regard, firms use artificial intelligence to foster threat hunting by incorporating behavioral analysis to detect attacks. An example is how the AI models can introduce profiles to applications in a company network to process massive data. Besides, artificial intelligence can be applied in vulnerability management (Conti et al., 2018). Companies cannot handle the vulnerabilities they come across daily, and AI allows them to link it with machine learning to analyze the behavior of individuals (Taddeo, McCutcheon & Floridi, 2019). The process helps the firms to avoid vulnerabilities before they are patched and reported.

Artificial Intelligence has been improving the situation in data centers by monitoring and optimizing all the processes in the system of the organization. The continuous monitoring and calculative powers of artificial intelligence give an insight into the company's values to improve the security and effectiveness of infrastructure and hardware (Wirkuttis & Klein, 2017). In this instance, artificial intelligence reduces the cost of maintaining hardware as it gives notification on when and why to fix the system to avoid breaking down (Lee et al., 2019). Furthermore, AI can be applied in network security to create policies and network topography of the company. Under policies, the security policies determine the network connections that are legit for the organization to use and not affected by malicious behaviors. A topography network allows the firms to identify the workloads designed for a specific application.

**How the Research will help the United States**

The study on artificial intelligence and cybersecurity has an advantage to the citizens and organizations in the United States who have systems that need to be protected from malicious acts. The connection between AI and cybersecurity can allow the systems to be trained to determine malware attacks and ransomware (Johnson, 2019). Since most people and enterprises in the U.S complain about cyber threats, artificial intelligence scans the availability of risks before they are integrated into the system. The United States has previously been using the traditional approaches, but carrying out such Research will help prove how AI has predictive functions that surpass the conventional techniques, and the roles help in improving the efficiency of systems in the company (Madhok et al., 2016). The United States is classified among the leading countries with better technology and is expected to show how cyber threats can be reduced. With this

regard, the U.S can use artificial intelligence to prove to other countries how it can analyze and monitor the endpoints of cyber-risks in the system of the organization. In the end, citizens and enterprises in the United States can use AI to understand and improve the knowledge they have on cybersecurity threats.

The study is necessary to the United States. It will show enterprises and people how artificial intelligence is included in the current cybersecurity in situations where there is a need to detect threats. Cases of security breaches have led to an increase in demand for solutions that can help in reducing the violations (Wang & Lu, 2019). Following this, for the general public in the U.S, the connection between cyber threats and artificial intelligence is on the mainstream as such issues need to be solved. Therefore, the study helps to show companies based in the United States how to secure consumer data and manage artificial intelligence intending to avoid security breaches. Furthermore, many individuals would wish to use artificial intelligence but don't know what it can do to their businesses (Anwar & Hassan, 2017). In this case, the above Research is appropriate in giving an overview to such people as it gives some insights about artificial intelligence and how it can be vital in dealing with cybercrimes. Besides, enterprises and people can learn the advantages they have while investing in AI solutions as it helps reduce the cyber threats poses by malicious activities.

**Conclusion**

In conclusion, artificial intelligence creates a significant impact on the organization that decides to use it by countering cyber threats, improving cybersecurity in organizations, and helping countries like the United States deal with malicious attacks. The AI technologies have an infancy that proves most designers and organizations can still determine ways to detect cyber threats and develop software that is efficient in preventing an attack (Taddeo & Floridi, 2018). Artificial intelligence assists cybersecurity firms in assessing the threats posed to their data or system by using complex algorithms. Most organizations have chosen ways to use artificial intelligence, and what's remaining is creating designs and placing resources that machine learning can use when developing algorithms and routines. With this regard, the organizations can monitor and optimize all the processes found in the system (Veiga, 2018). AI experts are expected to provide solutions that can ensure all the traditional techniques for preventing cyber threats are not available, and they cannot surpass the effectiveness of the modern approaches. Such directives can depend on future Research that can promote artificial intelligence by creating more applications that can detect and prevent malicious attacks from spoiling what organizations and people have achieved, for example, on financial advancements. Data-driven models found in machine learning can impact the performance of an organization that depends on network security since AI introduces cyber threat intelligence that detects the level f the risk (high level or minor level). Thus, this is a shred of evidence that shows the integration of artificial intelligence with other aspects like data analytics, cloud computing, and machine can work. Therefore, the company should depend on artificial intelligence alone and include the different elements to create efficiency. In the end, all the problems connected to cybersecurity will have appropriate solutions.

References


1. Anwar, A., & Hassan, S. I. (2017). Applying Artificial Intelligence Techniques to Prevent Cyber Assaults. *International Journal of Computational Intelligence Research*, *13*(5), 883-889.
2. Calderon, R. (2019). The benefits of artificial intelligence in cybersecurity.
3. Conti, M., Dargahi, T., & Dehghantanha, A. (2018). Cyber threat intelligence: challenges and opportunities. In *Cyber Threat Intelligence* (pp. 1-6). Springer, Cham.
4. Hoadley, D. S., & Lucas, N. J. (2018). Artificial intelligence and national security.
5. Johnson, J. (2019). Artificial intelligence & future warfare: implications for international security. *Defense & Security Analysis*, *35*(2), 147-169.
6. Lee, J., Kim, J., Kim, I., & Han, K. (2019). Cyber threat detection based on artificial neural networks using event profiles. *IEEE Access*, *7*, 165607-165626.
7. Li, J. H. (2018). Cyber security meets artificial intelligence: a survey. *Frontiers of Information Technology & Electronic Engineering*, *19*(12), 1462-1474.
8. Madhok, E., Gupta, A., & Grover, N. (2016). Artificial Intelligence Impact on Cyber Security. *IITM Journal of Management and IT*, *7*(1), 100-107
9. Parrend, P., Navarro, J., Guigou, F., Deruyver, A., & Collet, P. (2018). Foundations and applications of artificial Intelligence for zero-day and multi-step attack detection. *EURASIP Journal on Information Security*, *2018*(1), 1-21.
10. Srivastava, S., Bisht, A., & Narayan, N. (2017, January). Safety and security in smart cities using artificial intelligence—A review. In *2017 7th International Conference on Cloud Computing, Data Science & Engineering-Confluence* (pp. 130-133). IEEE.
11. Taddeo, M., & Floridi, L. (2018). Regulate artificial intelligence to avert cyber arms race.
12. Taddeo, M., McCutcheon, T., & Floridi, L. (2019). Trusting artificial intelligence in cybersecurity is a double-edged sword. *Nature Machine Intelligence*, *1*(12), 557-560.
13. Trifonov, R., Nakov, O., & Mladenov, V. (2018, December). Artificial Intelligence in Cyber Threats Intelligence. In *2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC)* (pp. 1-4). IEEE
14. Vähäkainu, P., & Lehto, M. (2019, February). Artificial intelligence in the cyber security environment. In *ICCWS 2019 14th International Conference on Cyber Warfare and Security: ICCWS 2019* (p. 431). Academic Conferences and publishing limited.
15. Veiga, A. P. (2018). Applications of artificial intelligence to network security. *arXiv preprint arXiv:1803.09992*.
16. Wang, Q., & Lu, P. (2019). Research on application of artificial intelligence in

computer network technology. *International Journal of Pattern Recognition and Artificial Intelligence*, *33*(05), 1959015.

17. Wirkuttis, N., & Klein, H. (2017). Artificial intelligence in cybersecurity. *Cyber Intelligence, and Security Journal*, *1*(1), 21-23.