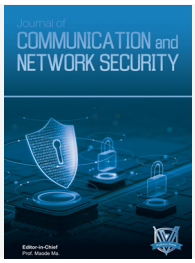
Journal of Communication and Network Security (JCNS)

DOI:http://doi.org/10.65098/jcns.01.2026.05.08



RESEARCH ARTICLE

THREATS AND COUNTERMEASURES OF ARTIFICIAL INTELLIGENCE TO CYBERSECURITY

Ming Wang, Zhiwen Sun, Haiyan Yang*

Hebei Normal University of Science & Technology, Hebei 066001, China
**** Corresponding Author E-mail: estherwu5712@gmail.com***

ARTICLE DETAILS

Article History:

Received 17 Sep 2025
Accepted 22 Dec 2025
Available online 9 Feb 2026

Online Article Code

ABSTRACT

Background and Purpose: The rapid advancement of artificial intelligence (AI) has brought both significant opportunities and unprecedented challenges to cybersecurity defense. AI-driven attack techniques are becoming increasingly sophisticated, while traditional cybersecurity measures often suffer from technological lag, limited response mechanisms, and insufficient intelligence. This study aims to examine the impact of AI on cybersecurity defense and to explore effective strategies for addressing AI-enabled security threats.
Methods: This paper analyzes the development characteristics and emerging trends of AI technologies in the contemporary digital environment. It systematically examines AI-based cyberattack models and their implications for existing security systems. Based on this analysis, comprehensive and practical countermeasures are proposed, integrating intelligent detection, adaptive defense mechanisms, and coordinated response strategies.
Results: The findings indicate that AI significantly reshapes both offensive and defensive dimensions of cybersecurity. While AI-enhanced attacks increase the complexity of threat landscapes, the adoption of intelligent security technologies can improve threat identification accuracy, response speed, and overall defense resilience. Integrated AI-based defense strategies demonstrate greater adaptability to evolving attack patterns.
Conclusion: Artificial intelligence plays a crucial role in enhancing modern cybersecurity defense. By leveraging advanced AI technologies and implementing comprehensive countermeasures, cybersecurity systems can achieve higher levels of intelligence, robustness, and effectiveness in addressing emerging cyber threats.

KEYWORDS

Cybersecurity, Threats and Countermeasures, Artificial Intelligence

In the context of the rapid development of information technology today, cybersecurity issues have become increasingly prominent, becoming a key topic that cannot be ignored in various fields. Especially with the widespread application of artificial intelligence technology, the challenges faced by cybersecurity have undergone qualitative changes. To address these new challenges, we need to re-examine and improve existing cybersecurity defense strategies. This paper will explore the cybersecurity threats brought by artificial intelligence technology to the field of cybersecurity from a new perspective, propose comprehensive countermeasures against these threats, and discuss how to use these technologies to strengthen cybersecurity defense. At the same time, this paper will also discuss the potential of new technologies in improving cybersecurity levels, hoping to provide some useful thinking and suggestions for future cybersecurity defense work.

1. OVERVIEW OF RELATED CONCEPTS

1.1 Artificial Intelligence

Artificial Intelligence (AI) (Zhou & Xu, 2021) is a scientific field dedicated to researching, developing, and applying computer systems capable of performing specific tasks. Its goal is to realize the processing, learning, and reasoning of information by simulating human intelligence. In recent years, artificial intelligence technology has received widespread attention and gradually penetrated into many fields, such as autonomous driving, medical diagnosis, and smart homes. Artificial intelligence has great potential in the field of cybersecurity. For example, by using machine learning algorithms, massive amounts of network data can be analyzed in real time to quickly identify potential threats and abnormal behaviors, thereby improving the efficiency of network defense. However, the development of artificial intelligence technology also brings challenges to cybersecurity. Malicious attackers may use artificial intelligence technology to develop more complex and unpredictable attack methods to evade traditional defense mechanisms. At the same time, artificial intelligence systems themselves may have security vulnerabilities, becoming potential targets for attackers. The application and impact of new technologies such as artificial intelligence in the field of cybersecurity are two-sided. On the one hand, it can

improve the efficiency and effectiveness of cybersecurity defense; on the other hand, it also brings new challenges and hidden dangers to cybersecurity. Therefore, while exerting the advantages of artificial intelligence technology, we should also pay attention to its potential risks in cybersecurity and take corresponding preventive measures.

1.2 Overview of Cybersecurity Defense

Cybersecurity defense (Zhang et al., 2020) refers to the process of taking a series of technical and management measures in a network environment to protect information systems and data from potential threats and damages. With the popularization of the Internet and the rapid development of information technology, the importance of cybersecurity defense has become increasingly prominent. However, cybersecurity defense faces many difficulties. Firstly, the diversity and constant evolution of network threats make it difficult for defense strategies to keep up. Attackers constantly adopt new technologies and methods to evade existing defense mechanisms. Secondly, the complexity of the network environment and the huge amount of data make it more difficult to identify real threats and abnormal behaviors. In addition, with limited resources, organizations often struggle to invest sufficient human and financial resources to build a sound defense system. Information leakage and malicious network attacks can cause serious privacy leakage or economic and property losses. In this context, effective cybersecurity defense is of great significance for safeguarding information security and ensuring the stable operation of cyberspace. An effective cybersecurity defense strategy can not only protect critical information assets, prevent unauthorized access and data leakage, but also improve an organization's ability to resist network attacks and reduce cybersecurity risks. A sound cybersecurity defense system helps maintain the stability of cyberspace. Therefore, continuously paying attention to the development trends of cybersecurity defense and constantly optimizing defense strategies have become important tasks in the field of cybersecurity.

2. ANALYSIS OF CURRENT SITUATION OF CYBERSECURITY AND ARTIFICIAL INTELLIGENCE THREATS

2.1 Analysis of Current Cybersecurity Situation

Significant achievements have been made in cybersecurity defense, but there are still some deficiencies. It mainly faces problems such as diversified network attack methods, wide sources of cybersecurity threats, imperfect laws, regulations and standard systems, and the urgent need to improve cybersecurity defense capabilities.

(1) Increasingly Diversified and Complex Network Attack Methods

In the current network environment, hackers attack network systems using various means, including Distributed Denial of Service (DDoS) attacks, malware, phishing, etc. These attack methods are constantly upgrading and are difficult to prevent. For example, with the popularization of IoT devices, hackers can use botnets to launch large-scale DDoS attacks, causing serious damage to target websites. In addition, the detection and response to Advanced Persistent Threat (APT) attacks also face great challenges. Such attacks are often targeted and concealed, able to lurk in the target system for a long time to steal information or carry out sabotage.

(2) Wide Sources of Cybersecurity Threats

In addition to attacks from hackers, cybersecurity threats may also come from multiple links such as internal personnel and supply chain partners. Internal personnel may cause cybersecurity incidents due to operational errors or malicious behaviors, while supply chain partners may become a transmission channel for cybersecurity risks due to security vulnerabilities or being hacked. As cyberspace has become an important part of modern politics, economy, culture, science and technology, and society, it has also become a stage for competition and confrontation between countries, involving national security and strategic interests. Some countries may use improper network attack methods to conduct political, economic, military and other investigations and sabotage on China's cyberspace, posing a certain threat to China's cyberspace sovereignty and further exacerbating the severity of the cybersecurity situation.

(3) Imperfect Laws, Regulations and Standard Systems

Although China has strengthened the construction of cybersecurity laws and regulations in recent years, there are still institutional deficiencies and insufficient policy implementation in cyberspace governance and data protection. The cybersecurity legal system needs to be further improved to adapt to the changing network environment. In addition, the cybersecurity standard system also needs to be established and improved urgently to provide technical and management guidance for enterprises and government departments.

(4) Urgent need to Improve Cybersecurity Defense Capabilities

Faced with the increasingly severe cybersecurity situation, the cybersecurity defense capabilities of relevant organizations need to be strengthened. In terms of talent training, the current training and reserve of cybersecurity talents are still insufficient, and the supply of talents with professional skills and practical experience is seriously lacking. To improve cybersecurity defense capabilities, it is necessary to increase the training of relevant security talents, establish and improve talent training mechanisms, and enhance the quality of talent training.

2.2 Threats of Artificial Intelligence to Cybersecurity

The application of artificial intelligence technology in the field of cybersecurity has brought new opportunities for defense work, but it also poses threats to cybersecurity. These threats are mainly reflected in the following aspects:

(1) Intelligent Attack Methods

Using artificial intelligence technology, attackers can implement automated and intelligent attack methods, such as automated vulnerability discovery and exploitation, intelligent password cracking, etc. These attack methods are difficult to detect and block in traditional defense systems, greatly increasing cybersecurity risks.

(2) Generative Adversarial Networks (GAN) (Wang et al., 2022)

Generative adversarial networks can be used to generate realistic fake content, such as forged text, images, audio, and video. These fake contents can be used for disinformation dissemination, online fraud, and other malicious activities, thereby posing a serious threat to cybersecurity.

(3) Artificial Intelligence Technology Enhances Concealment

Using artificial intelligence technology, malicious network attackers can more easily cover their tracks, making it more difficult for law enforcement agencies to track and obtain evidence. AI technology can also help malicious network attackers locate and target specific targets more accurately, thereby improving the efficiency and accuracy of attacks.

(4) Legal and Ethical Challenges

The application of AI technology in the field of cybersecurity has brought many unresolved legal and ethical issues. For example, AI systems in the field of cybersecurity may generate discrimination and prejudice based on the data they learn, leading to unfair decisions and processing. In addition, when problems arise during the participation of AI technology in cybersecurity defense, how to define the attribution of responsibility and how to formulate relevant laws and regulations for effective supervision are also urgent issues to be solved. These issues need to continuously explore and improve relevant laws and regulations in practice.

3. CYBERSECURITY THREAT COUNTERMEASURES BASED ON ARTIFICIAL INTELLIGENCE

In the face of the increasingly complex network threats brought by

the rapid progress of artificial intelligence technology, it is crucial to formulate more intelligent cybersecurity defense strategies with the help of artificial intelligence technology. It can not only save human and various costs but also achieve efficient response to cybersecurity threats.

(1) Intelligent Defense Strategies and Human-Machine Collaboration

In cybersecurity defense, the collaboration between artificial intelligence technology and humans is crucial. Artificial intelligence can help security personnel process large amounts of cybersecurity data more efficiently, discover potential threats, and automatically adjust defense strategies. At the same time, security teams can use the natural language processing capabilities of artificial intelligence to achieve real-time monitoring, reporting, and analysis of cybersecurity incidents. Through the collaboration between artificial intelligence technology and cybersecurity professionals, the effect of cybersecurity defense can be significantly improved.

(2) Security Early Warning and Risk Assessment (Ma et al., 2021)

With the help of artificial intelligence technology, the prediction and assessment of cybersecurity risks can be realized. Through big data analysis and machine learning algorithms, potential security threats in network behavior data can be mined to detect and warn of attacks in advance. Artificial intelligence can use historical data for pattern recognition to predict potential attack behaviors. Through early warning, cybersecurity teams can predict risks in advance and make decision-making arrangements for cybersecurity defense before a crisis occurs. In addition, artificial intelligence technology can also conduct quantitative assessment of cybersecurity risks, providing decision-makers with a more intuitive basis for judging security status. Individuals, enterprises, and government organizations can reasonably allocate security resources and formulate more targeted defense strategies according to the actual risk situation.

(3) Establish a Sound Security Mechanism

Cybersecurity defense relies not only on technical means but also on the establishment of a sound security mechanism. This includes formulating detailed cybersecurity policies, network behavior norms, and implementing effective security training. Firstly, relevant departments need to strengthen legislative work, formulate and improve cybersecurity-related laws and regulations to provide a strong legal guarantee for cybersecurity defense work. In addition, relevant organizations should also formulate suitable cybersecurity policies and norms according to relevant regulations, clarifying cybersecurity responsibilities and obligations. This enables relevant organizations to more effectively monitor network behaviors and prevent internal personnel or external attackers from causing losses by exploiting policy loopholes. At the same time, relevant organizations should also establish strict security review mechanisms to ensure that partners and supply chain members comply with corresponding security regulations. Finally, security training is a key link to improve employees' security awareness and skills. Relevant organizations can use artificial intelligence technology to customize personalized training programs, providing training content at different levels according to the responsibilities and knowledge levels of organizational members.

(4) Continuous Monitoring and Optimization of Defense Strategies

Artificial intelligence technology can help governments, enterprises, individuals, or other relevant organizations realize continuous monitoring and optimization of cybersecurity defense strategies. By collecting and analyzing a large amount of data, artificial intelligence systems can automatically adjust defense strategies in real time, making cybersecurity defense strategies more targeted. For example, by monitoring network traffic and device behaviors, artificial intelligence can identify new attack patterns and vulnerabilities and provide corresponding defense suggestions. In addition, artificial intelligence can use reinforcement learning technology to continuously learn and optimize defense strategies, achieving real-time and effective response to cybersecurity threats.

4. APPLICATIONS OF ARTIFICIAL INTELLIGENCE IN CYBERSECURITY DEFENSE

Artificial intelligence-based cybersecurity defense systems integrate multiple technologies to achieve comprehensive and multi-layered protection. The following application examples cover key areas such as intrusion detection, firewalls, anomaly behavior detection and response, and malware detection, demonstrating how an effective defense system can be constructed to address increasingly severe cybersecurity challenges.

(1) Deep Learning-Based Intrusion Detection System (DeepIDS) (Lin et al., 2021)

DeepIDS uses deep learning techniques to perform real-time analysis of network traffic, automatically learning normal behavior patterns and detecting anomalous traffic. By comparing known attack signatures with real-time network traffic data, DeepIDS can effectively identify potential cyberattacks and enhance network security defense capabilities. DeepIDS has strong adaptability, enabling it to quickly adjust to changes in network environments and reduce false positives and false negatives. In addition, the DeepIDS system can effectively address zero-day attacks and emerging attack techniques, improving the overall security protection level of enterprise networks.

(2) Intelligent Application Firewall (IAF) (Zhu et al., 2022)

IAF integrates artificial intelligence technologies to automatically identify and block malicious traffic. It is capable of self-learning and self-adjustment, as well as real-time updates of security policies to cope with constantly evolving attack methods. In addition to analyzing traffic characteristics, IAF performs in-depth analysis of application-layer protocols, providing more fine-grained security protection. IAF can also work collaboratively with other security devices, such as intrusion detection systems, to achieve more comprehensive and efficient cybersecurity defense.

(3) Behavior Analysis-Based Anomaly Detection and Response System (BAEDR) (Zhang & Sun, 2021)

BAEDR uses machine learning techniques to conduct real-time analysis of network traffic and user behavior. By identifying abnormal behaviors, the BAEDR system can automatically take corresponding actions, such as isolating suspicious devices or restricting their access permissions. Moreover, BAEDR can generate security reports in real time, providing strong support for security teams. Through correlation analysis of internal and external data, BAEDR can accurately detect potential threats and improve security response speed. In addition, the system features self-learning and continuous optimization capabilities, enabling it to continuously enhance detection accuracy.

(4) Malware Detection and Analysis System (MDS) (Zheng et al., 2022)

The MDS system employs artificial intelligence technologies to identify, analyze, and defend against malware. Through deep learning and natural language processing techniques, MDS can extract key information from large volumes of threat intelligence and rapidly identify and classify malware. At the same time, MDS performs both dynamic and static analysis of malware to reveal its behavioral characteristics and propagation mechanisms, thereby providing effective defensive strategies for security teams. Furthermore, MDS has self-learning and continuous optimization capabilities, allowing it to adapt to the constant evolution of malware and emerging attack techniques, and to improve the accuracy and timeliness of malware detection and defense.

5. CONCLUSION

Against the background of the rapid development of artificial intelligence technology, technological progress has also brought new challenges, and the cybersecurity situation has become increasingly severe. Artificial intelligence technology plays an important role in cybersecurity defense. This paper introduces the threats and challenges brought by artificial intelligence technology to cybersecurity defense, proposes

corresponding countermeasures, and constructs a highly practical and operable defense system by combining various technologies from the application level. In cybersecurity defense, it is necessary to make full use of artificial intelligence technology and combine it with traditional defense means to jointly respond to network threats. Through the collaboration between artificial intelligence and humans, the effect of cybersecurity defense is improved. In addition, cybersecurity practitioners need to pay close attention to technological development trends, continuously optimize cybersecurity defense strategies, and constantly improve cybersecurity defense capabilities to ensure the security of cyberspace.

REFERENCES

Lin, Shuo, Shang, Fubo, & Gao, Zhijun. (2021). Intrusion detection model based on deep learning. *Control Engineering of China*, *28*(9), 1873-1878.

Ma, Wengang, Zhang, Yadong, & Guo, Jin. (2021). An abnormal traffic detection method based on LSTM and improved residual network optimization. *Journal on Communications*, *42*(5), 23-40.

Wang, Wei, Li, Yujie, & Guo, Fulin. (2022). A survey of generative adversarial networks and their text-image synthesis. *Computer Engineering and Applications*, *58*(19), 14-36.

Zhang, Bing, Ren, Jiadong, & Wang, Ning. (2020). A survey of cybersecurity risk assessment and analysis methods. *Journal of Yanshan University*, *44*(3), 290-305.

Zhang, Sainan, & Sun, Biao. (2021). A survey of network anomaly detection methods based on machine learning. *Journal of Jilin University (Information Science Edition)*, *39*(6), 732-742.

Zheng, Rui, Wang, Qiuyun, & Lin, Zhuopang. (2022). A mining malware detection method based on threat intelligence hierarchical feature integration. *Acta Electronica Sinica*, *50*(11), 2707-2715.

Zhou, Chunping, & Xu, Changdi. (2021). Research on the application of artificial intelligence technology in big data cybersecurity defense. *Network Security Technology and Application*, (11), 61-63.

Zhu, Simeng, Du, Ruiying, & Chen, Jing. (2022). Web application firewall reinforcement scheme based on recurrent neural network. *Computer Engineering*, *48*(11), 120-126.

Cite The Article: Ming Wang, Zhiwen Sun, Haiyan Yang (2026). Threats and Countermeasures of Artificial Intelligence to Cybersecurity. *Journal of Communication and Network Security*, 1(1): 05-08.