Application of Artificial Intelligence Technology in Security Defense of Cyberspace

Limin Huang*
Shandong Institute of Commerce & Technology, Shandong, China, 250103

*Corresponding author e-mail: zhangshumei520@outlook.com

Abstract. In the process of its development and application, the computer network has created the virtual network space, and as the relationship with the computer network is becoming more and more close, the improvement of the security defense of cyberspace ability is becoming more and more urgent. The use of artificial intelligence technology in cyberspace security defense can not only accept and process a large number of Internet information quickly and efficiently, but also improve the security defense of cyberspace and prevent the infringement of illegal elements, which is a matter of great concern to every user. Based on the analysis of the characteristics of cyberspace security defense and artificial intelligence technology, this paper discusses the application of artificial intelligence technology in cyberspace security defense with examples.

Keywords: artificial intelligence, cyberspace, security defense

Nowadays, after decades of rapid development, the computer network has established a very close relationship with people, not only plays an increasingly important role in people's life and production, but also plays an important role in all walks of life. The development, popularization and wide application of the Internet have brought us a variety of conveniences, wonderful experience and spiritual entertainment, but also a variety of unsafe factors that may appear in the use. As a concept, cyberspace is open, invisible, and can't be found, but it does exist and has a unique operating characteristic that is different from that of the physical space. There are occasionally losses by attacks or deceptions. Therefore, the security of cyberspace has been paid more and more attention, and the continuous improvement of cyberspace security defense ability goes hand in hand with the development of network, in order to prevent network attacks, resist illegal intrusion, provide users with a secure and reliable cyberspace security environment, and guarantee user's rights and interests. In recent years, the rapid development of artificial intelligence technology has gained more and more important application in the network space security defense. Compared with the traditional way, artificial intelligence has obvious advantages, and the advantages are also continuously expanded and are widely favored.
1. Cyberspace security and artificial intelligence technology

1.1 Cyberspace risk
Various basic information technologies form virtual network space under the interaction of Internet, computer system, communication transmission network, embedded controller and so on. At present, there are mainly three sources of cyberspace security risk in China. First of all, the Internet cause in our country started late and the foundation is weak. The security defense of cyberspace is still in a relatively weak stage at present, and there are some security incidents in which cyberspace is subjected to illegal intrusion and malicious attack. As the Internet develops rapidly, it is difficult to predict the new situation of the cyberspace in the research of new protection system that is supposed to deal with the virus invasion. Because of the following problems can’t be prejudged in advance, the response work cannot take the initiative to attack, can only passively confront. Secondly, the core part and important technology of computer facility equipment and system in our country are introduced from abroad, so that the whole system itself has many unknown factors and unreliable elements, and the security risk of cyberspace is increased. The third, it is a short time since computer network popularity in china. Users from all corners of society, most of them have limited cognition of the network, serious lack of awareness of cyberspace security. Thus, they only pay attention to its favorable functions when using the network, but do not pay attention to the confidentiality of privacy such as personal network accounts, passwords and so on, resulting in information leakage, identity replication, illegal transfer of property, to bring lost to their own rights and interests.

1.2 Cyberspace defense
Cyberspace defense is established in order to deal with the cyberspace risk, protect information of the network users, by means of a series of defensive means such as interference prevention and illegal intrusion. The intrusion detection technology is used for monitoring and detecting other computers which are not authorized by the legal authority. How it works is shown in figure 1.

![Figure 1. Intrusion Prevention Engine Schematics](image)

1.3 The development and advantage of artificial intelligence
At present, through the development of more than 70 years as shown in Figure 2, artificial intelligence technology has been one of the most leading technologies in the field of computer science, and has been deeply and widely studied in recent years. The rapid development of science and technology also provides technical support and basic guarantee for the universal application of artificial intelligence technology in people's production and life. From the birth to the present, the controversy of the definition of artificial intelligence has never been interrupted, which does not hinder the continuous advancement of artificial intelligence technology. Through the research and character analysis of a series
of problems, the academic circles have divided the artificial intelligence into the "strong artificial intelligence" and the "weak artificial intelligence"[4]. The network system space changes at a real-time, with large number of information with the same nature, and the totally different form or very different form. Artificial intelligence is based on the management system of self-learning and fuzzy logic, and assists the management system to efficiently handle the changing information in the transmission process. The application of artificial intelligence technology also makes it possible for many different administrators to work together.

![Figure 2. The Development of artificial Intelligence](image)

### 2 Examples of typical application of artificial intelligence in security defense of cyberspace

#### 2.1 Intelligent firewall
Firewall is one of the most commonly used defense techniques to prevent illegal intrusion and malicious attacks in cyberspace security defense. In the past, the firewall we used in the past has also undergone careful defense design, carried out a lot of simulated attacks, and envisioned a variety of attack behavior, which is difficult to achieve satisfactory defense effect because of its mechanical adaptability. The combination of artificial intelligence technology and firewall to form intelligent firewall has the ability to comprehensively analyze and judge the incoming data information, eliminate the hidden danger of cyberspace security in time, block the whole risk of cyberspace, and has higher efficiency and more accurate recognition ability than the traditional network firewall. The application of artificial intelligence technology makes up for the shortcomings of traditional firewall in some aspects, eliminates some loopholes in the past, greatly improves the security defense performance of cyberspace, improves the security of users to the process of accessing cyberspace, and makes the security defense of firewall more effective.

#### 2.2 Neural network system
Artificial intelligence technology has been applied in neural network system, and it is also a promising and effective application in cyberspace security defense. As the name implies, neural network system is as complex as human brain nerve. It can identify and select a large number of information that flows into cyberspace. It needs to have particularly strong storage, operation and control capabilities. It can also effectively monitor and analyze complex and changeable information. It plays a more and more important role in cyberspace security defense. The neural network system has the characteristics of great fault-tolerance and self-iterative learning ability, and the independent neuron can detect the security risk of the network space separately and improve the safety and defense effectiveness of the cyberspace. Neural network system uses multi-perception technology to detect viruses, which is applied to the network system in continuous circulation on the basis of collecting the previous data, which greatly
improves the accuracy of intercepting risk information. Although the present artificial intelligence technology is still in the primary stage of the development of the neural network system, it has not been fully applied, but in view of the important position of the network space security defense in the development of the Internet, the application of the artificial intelligence technology will be further in-depth with the development of the network. The value of inestimable will be more and more reflected.

3. Conclusions
In recent years, with the deepening of the research of artificial intelligence, the rapid development of artificial intelligence technology has been widely used in all walks of life. In this era of information network, Internet system has become an indispensable tool in various industries. People's interests are more and more closely related to cyberspace, and the challenges faced by cyberspace security are becoming more and more serious. Speed up the pace of research, improve and expand the application of artificial intelligence technology in cyberspace security defense, improve the accuracy and comprehensiveness of computer database detection in an all-round way, and protect the further development of information network.

References
[1] Huang Lijun, Peng Feng. Application of artificial intelligence technology in library computer network security [J]. Journal of Modern Information, 2008 (12).
[2] Zhao Ping. Research on computer Database intrusion Detection Technology [J]. Science & Technology Information, 2016 (28): 23-24.
[3] Wu Yuanli, Si Guangya, Luo Pi. Application of artificial intelligence technology in cyberspace security defense [J]. Application Research of Computers, 2015 (08).
[4] Ma Xiurong Wang Huayu. The application of artificial intelligence in network security management is briefly described. Journal of Hulunbeier University, 2005 (02).