Information Network Security Situation Awareness Technology Based on Artificial Intelligence

Bai Yong, Huang Dong, Liao Yong, Pen Guangbin, Xu Luyao, Deng Yongsheng, Wang Chun

Chongqing Vocational and Technical University of Mechatronics,Chongqing Bishan,402760

Keywords: Artificial Intelligence, Information Network Security, Situational awareness

Abstract. With the development of economy, science and technology are also advancing rapidly. At present, information technology and Internet technology are the core and hottest technologies, and their development is related to various industries. While the rapid development of information network technology, it also faces various risks at all times. Especially in recent years, various information network security threats have become increasingly serious. For this reason, information network security situation awareness technology plays an important role. With the development of science and technology, artificial intelligence technology has received widespread attention for its excellent self-learning and analytical processing capabilities. Therefore, the information network security situation awareness technology based on artificial intelligence is a current major technology development trend. This article analyzes and discusses the information network security situation awareness technology based on artificial intelligence in detail, hoping to play a certain role in promoting its development.

1 Introduction

With the rapid development of economy and the continuous progress of society, China's scientific and technological level has also been greatly improved. As we all know, the most important technical field in China and the world is the information technology field. Information technology has been deeply integrated into various industries and has played a key role. The development of information technology has brought new space to the revival of the country and the development of various industries. With the popularization of information technology, especially Internet technology, although people's work and life have greatly improved, the information network also faces various security threats at all times, and there are many potential security risks. At present, various enterprises and even government agencies in China are facing severe threats to the security of information networks. If they are not dealt with in a timely manner, they will seriously affect the development of the country, society and the stability of personal life. In order to effectively prevent and deal with various types of information security risks, information network security technology was born, and it has grown rapidly with the development of information technology. Information network security situation awareness technology is one of them. As the security situation of information networks becomes more and more complex, and various new security threats are emerging, the existing information network security situation awareness technologies need to be improved to cope with these new security threats. Artificial intelligence is the most cutting-edge and hot technology at present, with the ability of deep learning, flexible analysis and processing of various known and unknown problems. The organic integration of artificial intelligence and information network security situation awareness technology is one of the most important development trends of current security situation awareness technology.

2 Information Network Security Situation Awareness Technology Related Concepts

2.1 Origin of Information Network Security Situation Awareness Technology

The so-called information network security situational awareness technology is actually a kind of situational awareness technology. Situational awareness was first introduced by Endsley in 1988. It

DOI: 10.25236/icicta.2019.011

is a technology that extracts and analyzes the surrounding environment and predicts its subsequent changes according to a certain law. With the development of this technology, Leopold and others finally introduced situational awareness technology to the field of information security in 1999. They emphasized that data fusion is the core of situational awareness and pointed out that this technology will be the core of future information network technology management trend. In China, research on information network security situation awareness technology began in 2010, and many universities and research institutions have also achieved many results in the study of various key technologies.

2.2 Functions of Information Network Security Situation Awareness Technology

Information network security situation awareness technology is a technology that can track the network security status in real-time in a large range of complex network environments, extract security elements that have a significant effect on network security changes, analyzes them in detail according to certain algorithms and rules, determines the current network security status, predicts the trend of network security development, and provides data support for subsequent decision-making and processing. The core of this technology can be classified into two categories, one is the extraction of the current network situation elements, and the other is the analysis and evaluation of the elements. On the whole, the main functions of information network security situation awareness technology can be divided into: visible, knowable, manageable, controllable, traceable, and early warning. Visible and knowable mainly means that this technology must be shown to professionals so that professionals can obtain information for subsequent operations; manageable and controllable emphasizes that this technology enables professionals to deal with detected security threats in a timely manner; traceable requires that this technology be able to track the process of security incidents and save processing records for subsequent review; Early warning means that this technology can predict the security situation of the network within the first time in advance based on the analysis of the characteristics of the security elements of the current information network, and promptly warn the various security threats predicted to promote the timely and effective processing.

3 Why Information Network Security Situation Awareness Technology Should Introduce Artificial Intelligence Concept

3.1 Global Informatization Is Highly Developed, and Information Technology Has Become The Core Element for the Development of Various Industries

The reason why artificial intelligence technology is introduced into information network security situation awareness technology to enhance its effect is first and foremost because of the current development of information network technology. At present, information networks are widely used in various industries, and in many industries, information network technology has become its most critical development factor, and many technologies that have information network technology as their core have become important forces for national and social development. The e-commerce industry is the most typical representative of this. The development of each industry must have a stable and secure environment. Therefore, the security of the information network environment has a bearing on the sustainable development of many industries, which affects the stability of the country and society. Therefore, information network security situation awareness technology is very important, and how to effectively improve the level of this technology is the key to its development. Therefore, combining artificial intelligence to improve information network security situational awareness technology is very necessary.

3.2 Information Security Is Facing Severe Challenges, and Existing Security Situation Awareness Technologies are Difficult to Cope with the New Security Situation

At present, the information network has become a key factor for the development of enterprises, industries, and socio-economics. The information network has penetrated into all aspects of the enterprise, and the business secrets of the enterprise can be obtained through the information network. Information networks can directly involve economic benefits and a large number of benefits, so there are more and more illegal intrusions and attacks against information networks. Information network security threats are becoming more and more common, more and more complex, larger and larger, and the consequences are becoming more and more serious. For example, the famous ransomware attacked more than 100,000 computers in more than 100 countries around the world, which had a huge impact on global economic development. In addition, various technical loopholes, system backdoors, Trojan horses, etc. are becoming more and more diverse, more and more hidden, and the means of infection and attack are becoming more and more complex. Unless the current security situation awareness technology is improved, it cannot face the current severe security situation.

3.3 Artificial Intelligence Technology Can Effectively Improve the Ability of Information Network Security Situation Awareness Technology

The amount of data in the current information network is exploding, and the situation is becoming more and more complicated. Artificial intelligence is good at processing large-scale data, and its deep learning features can be continuously and automatically optimized. Therefore, its application in the field of network security is extremely advantageous. On the one hand, artificial intelligence-based data advancement and analysis can effectively extract and process massive amounts of complex and fuzzy data. On the other hand, deep learning of artificial intelligence can effectively carry out correlation analysis, and can comprehensively and accurately perceive and warn of the security situation of information networks, thereby promoting the timely treatment of information network security threats.

4 System Architecture of Information Network Security Situation Awareness Technology Based on Artificial Intelligence

The system architecture of information network security situational awareness technology based on artificial intelligence is mainly divided into five modules: information extraction, information preprocessing, information fusion, situational awareness and situation assessment. Information extraction mainly completes the acquisition of information. The sources of information data mainly include various types of security equipment, network equipment and various application databases in the network. Information pre-processing is mainly to complete the filtering, purification and sorting of collected information data to make it meet the requirements of subsequent processing. Information fusion is mainly due to different sources of information. There are certain differences. If the fusion is not performed to form a single standard type, it will be inefficient to process. Situational awareness mainly uses artificial intelligence algorithms to identify, understand, and predict situations. The situation assessment is the impact analysis and assessment of the situation completed by the artificial intelligence technology of science and engineering to form the final assessment result.

5 Key Technologies of Information Network Security Situation Awareness Technology Based on Artificial Intelligence

5.1 Situation Forecasting Algorithm Based on Artificial Intelligence

Situation prediction refers to the technique of analyzing and summarizing the existing situation and inferring its development trend based on natural development or statistical laws. This is also the key technology in the current information network security situation awareness technology. The situation prediction methods based on artificial intelligence are roughly divided into prediction algorithms based on expert systems, prediction algorithms based on artificial neural networks, and prediction algorithms based on support vector machines. As the name implies, the prediction algorithm based on expert system is to predict the situation by simulating the thinking and experience of industry experts. The advantage is that it matches the human thinking pattern, is easy to understand, and uses experience to make predictions, which requires less calculation. The disadvantage is that a large number of actual case samples need to be collected and entered in advance. The quality and representativeness of the samples have a direct impact on the accuracy of the prediction. Artificial neural network-based prediction algorithms can be effectively combined with algorithm tools such as wavelet analysis, fuzzy theory, and genetics and evolution, and have good application results. However, this algorithm also has the problem of easily forming a local optimal solution. The prediction method based on support vector machine is based on machine learning algorithm, which requires less sample size, but it also has the problems of complex algorithm and slow analysis speed.

5.2 Establishment of situational indicator system

To describe, perceive and evaluate a situation, specific analysis indicators are needed. The establishment of these indicators that can represent the essential characteristics of the situation is a key to the information network security situation awareness technology based on artificial intelligence. The current indicators are mainly divided into three categories: basic operation indicators, network vulnerability indicators and cyber threat indicators. Basic operation indicators refer to a series of indicators of various performances and environments in the current standard network situation, which can play an indirect characterization of network security. The network vulnerability index represents the vulnerability and vulnerability index of the current network as a whole, such as the health index of various network devices. The cyber threat indicators characterize the characteristics of various threats in the network situation, such as the frequency, form, scale, and consequences of various threats.

Conclusions

With the further popularization of information networks in various industries and people's lives, the importance of security and stability is becoming higher and higher. In addition, various information network security threats are becoming more and more complex and larger in scale, and the consequences are increasingly serious. Therefore, through the organic combination of artificial intelligence and information network security situation awareness technology, it is very important to improve network security awareness and prevention capabilities.

Fund projects: Chongqing Natural Science Foundation (cstc2019jcyj-msxmX0551); Chongqing Education Committee Science and Technology Research Program key Project support Project (KJZD-K201803701); Chongqing Education Committee Science and Technology Research Project (KJQN201903701).

References

[1] Meng Fanyu. Cybersecurity Situation Awareness and Artificial Intelligence [J]. China Information Industry, 2019 (04): 89-91. [2] Li Zongwei. Research on Network Security Situation Awareness Technology Based on Artificial Intelligence [J] .Computers and Networks, 2019,45 (13): 49.

[3] Yuan Bao, Gao Qiang, Feng Qingyun. Analysis of Information Network Security Situation Awareness Technology Based on Artificial Intelligence [J]. Information Recording Materials, 2019, 20 (04): 113-114.

[4] Zheng Yanfang. Research and practice of artificial intelligence application and analysis technology in information security situation awareness system [J] .World of Digital Communications, 2018 (04): 221.

[5] Li Bin. Research on Network Security Situation Awareness System for Key Infrastructures [J]. Information and Computer (Theoretical Edition), 2017 (12): 203-205.

[6] Hu Dongxing. Artificial Intelligence-based Information Network Security Situation Awareness

Technology [J]. Information Communications, 2012 (06): 80-81.

[7] Tao Yuan, Huang Tao, Zhang Mohan, Li Shuilin. Research on key technologies of network security situational awareness and development trend analysis [J]. Information Network Security, 2018 (08): 79-85.

[8] Song Jin, Tang Guangliang. Research and application of network security situational awareness technology [J]. Communications Technology, 2018, 51 (06): 1419-1424.

[9] Li Jingquan, Liu Huiying, Zhang Wei, Chen Liandong. Research on Network Security Situation Awareness and Active Early Warning Technology [J] .Hebei Electric Power Technology, 2017,36 (05): 11-14.

[10] Jiang Chengzhi, Yu Yong, Lin Weimin. Research on Security Situation Awareness Model of Electric Power Information Network Based on Intelligent Agent [J]. Computer Science, 2012, 39 (12): 98-101.