Network Threat Intelligence Analysis Based on KNN Classification of Knowledge Atlas Characteristics

Wang Wenting, Zhang Hao, Liu Donglan, Liu Xin, Jing Junshuang

State Grid Shandong Electric Power Company Electric Power Research Institute, Jinan Shandong, 250003

Keywords: cyberspace security; knowledge map; research status; development trend

Abstract: As a new subject, Cyberspace Security not only involves information security and Cybersecurity in the traditional sense, but also extends the meaning of information space security in addition to land, sea, air and sky. By using the map of scientific knowledge, it can clearly and intuitively analyze the current research situation and development trend in related fields, and grasp it. Its research trends and future trends have certain practical significance for guiding the development of related research work. The research on Cyberspace Security is still in the initial development process of combining and subdividing information security, Cyberspace Security and cyberspace security.

1. Introduction

In order to transmit information on the network, both sides of communication need to establish a logical channel between receivers. This requires first determining the route from the sender to the receiver, and then selecting the communication protocol used in the route, such as TCP/IP. In order to transmit information safely in an open network environment, it is necessary to provide security mechanisms and services for information. The secure transmission of information includes two basic parts: one is to transform the transmitted information safely, such as encrypting information in order to achieve the confidentiality of information, adding some signatures for sender authentication, and the other is to send some secret information shared by both parties, such as encryption keys, in addition to trusted third parties. In addition, it is confidential to other users. In order to transmit information security, a trusted third party is usually needed. Its role is to distribute secret information to both parties and arbitrate when disputes arise between them. A secure network communication must take into account the following contents: (1) rules or algorithms for security-related information conversion; cryptographic information (such as keys) for information conversion algorithms; (2) distribution and sharing of secret information; and protocols for obtaining security services by using information conversion algorithms and secret information. Cyberspace means the information environment or information space for human existence. In 2012, the 18th National People's Congress of the Communist Party of China first adopted the concept of "cyberspace security". Cyberspace security can be regarded as the intrinsic expansion of cybersecurity and the inheritance and supplement of traditional cybersecurity. But unlike traditional network security, strictly speaking, Cyberspace Security not only refers to information security and cybersecurity, but also focuses more on the parallel space concepts of land, sea, air and sky. The information reflected by cyberspace security is more three-dimensional, more diverse and broader, reflecting more network and other spatial characteristics, and more infiltration. To other security areas [3]. After the publication of the report of the 18th National Congress, the security of cyberspace has attracted the attention of experts and scholars. Dong Zhibin [4] constructs China's Cyberspace Security Theory from the aspects of realistic value, ideological origin and system composition, and explores the realization path. Fang Xingdong [5] and others take prism gate as a hot issue of Cyberspace Security as a breakthrough point, deeply explore the new pattern of global cyberspace, and consider the strategic issues of Cyberspace Security in China under the new paradigm of cyberspace. However, compared with developed countries, China's understanding of Cyberspace Security is relatively lagging behind. At the same time, Cyberspace Security and Cyberspace Security have considerable overlap and inheritance, and Cyberspace Security is also the

DOI: 10.25236/aisct.2019.082

main research direction of cyberspace security.

2. Information Security Technology Based on Knowledge Map

Security features refer to what security threats the security unit can address. Information security features include confidentiality, integrity, availability and authentication security. Secrecy security mainly refers to protecting information from unauthorized entities in the process of storage and transmission. For example, credit card accounts and passwords transmitted online are not cracked. Integrity security means that information is not inserted, deleted, tampered with and redistributed as authorized entities in the process of storage and transmission, and the content of information is not changed. For example, users send e-mails to other people to ensure that the content at the receiving end remains unchanged. Availability security refers to the fact that a user cannot normally access resources that he would otherwise have the right to access due to an attack on the system. For example, to protect the security of mail servers from being attacked by DDOS can not work properly, is that users can send and receive e-mail normally. Authentication security is to prevent entities that do not have access to certain resources from accessing the network by some special means through some verification measures and technologies. Image retrieval is an important part of information retrieval. Since the 1970s, many scholars have studied image retrieval technology. They have proposed text-based image retrieval, content-based image retrieval and semantic-based image retrieval technology successively. Traditional text search is mainly based on keyword matching, focusing on optimizing search path algorithm and strengthening the establishment of learning and feedback models, such as Baidu and Google, which have achieved great success. However, there are many differences between image retrieval and text retrieval, and there are many problems, such as image content description, semantic understanding gap, complex feature extraction and so on. These problems restrict the further development of the research field of image retrieval, and are also the hot issues of image retrieval research

3. Research results and analysis

3.1 Statistical Summary

As a kind of resource, information is of great significance to human beings because of its universality, sharing, value-added, processability and multi-utility. The essence of information security is to protect information resources in information systems or information networks from various types of threats, interference and destruction, that is, to ensure the security of information. According to the definition of International Organization for Standardization, the meaning of information security mainly refers to the integrity, availability, confidentiality and reliability of information. Information security is an issue that any country, government, department and industry must attach great importance to. It is a national security strategy that can not be ignored. However, for different departments and industries, their requirements and priorities for information security are different.

China's reform and opening up has brought about a sharp increase in the amount of information in all aspects, and requires large capacity and efficient transmission of such information. In order to adapt to this situation, communication technology has undergone unprecedented explosive development. In addition to wired communications, radio communications such as short wave, ultra-short wave, microwave, satellite and so on are also more and more widely used. At the same time, in order to steal China's political, military, economic, scientific and technological secret information, foreign hostile forces use reconnaissance stations, reconnaissance ships, reconnaissance planes, satellites and other means to form a fixed and mobile, long-distance and short-distance, air and ground combined three-dimensional reconnaissance network to intercept China's communications transmission. Information in.

It is common for us to learn the inside story of a society from the literature. In the last 50 years of the 20th century, it is becoming easier and easier to learn the inside story of a society from the computers that belong to the society. Both organizations and individuals are entrusting more and more tasks to computers. Sensitive information is being transmitted between computer systems through fragile communication lines. Special information is stored in computers or transmitted between computers. Electronic banking enables financial accounts to be accessed through communication lines. Law Enforcement Department Doctors use computers to manage medical records. The most important problem is that they cannot transmit information without precautions against illegal (unauthorized) access.

There are many ways to transmit information, such as LAN, Internet and distributed database, cellular wireless, packet switched wireless, satellite videoconferencing, e-mail and other transmission technologies. In the process of storage, processing and exchange of information, there are possibilities of leaking or interception, eavesdropping, tampering and forgery. It is not difficult to see that a single security measure can hardly guarantee the security of communication and information. It is necessary to comprehensively apply various security measures, namely, through technical, managerial and administrative means, to realize the protection of the source, signal and information in order to achieve the purpose of secret information security.

System unit refers to the security problem of which system environment the security unit solves. For modern networks, the system unit involves the following five different environments. Physical Unit: Physical Unit refers to hardware equipment, network equipment, etc. The security unit with this feature solves the security problem of physical environment. Network Unit: Network Unit refers to network transmission, and the security unit containing this feature solves the security problem of network transmission caused by network protocol. System Unit: System Unit refers to the operating system. The security unit that contains this feature solves the security problems contained in the operating system of the end system or the intermediate system. Generally speaking, the security of data and resources in storage is a problem. Application Unit: Application Unit refers to an application, and the security unit that contains this feature solves the security problems contained in the application. Management Unit: Management Unit refers to the network security management environment, network management system for network resources security management.

3.2 Core Researcher Analysis

The knowledge map of literature authors can reflect the situation of researchers'publications and the cooperative relationship between different researchers. Do not change other settings, draw the map of researchers'knowledge.

1) Integrity

It means that information maintains the characteristics of non-modification, non-destruction and non-loss in the process of transmission, exchange, storage and processing, i.e. keeping the original information, so that information can be generated, stored and transmitted correctly, which is the most basic security feature.

2) Confidentiality

It means that information does not leak to unauthorized individuals, entities or processes according to the given requirements, or provides the characteristics of their utilization, that is, to prevent useful information from leaking to unauthorized individuals or entities, and to emphasize the characteristics that useful information is only used by authorized objects.

3) Availability

Network information can be accessed correctly by authorized entities and can be used normally or restored under abnormal conditions according to requirements. That is to say, the network information can be accessed correctly when the system is running, and can be quickly restored and put into use when the system is attacked or destroyed. Availability is a measure of the user-oriented security performance of network information systems.

4) Non-repudiation

In the process of information exchange, both sides of communication are convinced of the authenticity and identity of the participants themselves and the information provided by them. That is to say, all participants can not deny or deny their true identity, as well as the authenticity of the information provided and the operation and commitment completed.

5) Controllability

It refers to the characteristics that can effectively control the information dissemination and specific content in the network system, that is, any information in the network system should be controlled within a certain transmission range and storage space. In addition to the conventional form of communication sites and content monitoring, the most typical hosting policy, such as password, must be strictly controlled when the encryption algorithm is managed by a third party.

3.3 Core Co-citation Analysis

The application of academic papers can effectively evaluate the quality of academic papers and their academic influence. Generally speaking, the higher the citation frequency of academic papers, the higher their academic influence. Relevant academic papers are not cited frequently and published late. At the same time, the main research topics are still the development strategy of future information security, network security and Cyberspace Security and related theoretical speculation. Among the existing influential and strong academic papers, there are more comprehensive analysis of foreign advanced concepts to draw lessons from. Taking the most frequently cited big data era as an example, this paper analyses the characteristics of the information security strategy of the United States by interpreting the "big data research and development plan" of the United States Government, and interprets the development trend of the network security in the future. Overall, the concept of Cyberspace Security has not yet been clearly defined. Researchers often combine Cyberspace Security with information security. The related theory of Cyberspace Security is still in the early stage of development, which is consistent with the previous analysis.

3.4 Research Hotspots and Trends

The key words are the author's summary and concretion of the article, which embodies the central idea of the article. Without changing other software parameters, the key words are taken as the object of analysis, and the key words co-occurrence knowledge atlas and time sequence atlas are drawn respectively, taking the network space security as the boundary point for the first time in the report of the 18th National Congress of the CPC in 2012. Before 2012, Cyberspace Security did not appear as a key word. The research hotspots before 2012 mainly focused on network security and information security. E-commerce, e-government and digital library, as three practical areas, received the attention of researchers. After 2012, network security and information security as the main keywords still have a strong influence, but the keywords of network space, network governance, Internet governance have appeared many times. In the past research, besides network security and information security, there is a lack of centrality nodes in the atlas, which indicates that there is no clear direction and goal for related scientific research. Although the concept of cyberspace was formally put forward in 2012, there are still no influential scientific research results. With 2012 as the dividing line, the research focus of the two stages of high frequency keywords has changed greatly. In the previous stage (1998-2011), researchers paid more attention to the handling of specific details. In the latter stage (2012-2017), researchers mainly focus on the relationship between network security, information security, Cyberspace Security and macro-affairs, and the research field extends to the whole cyberspace. In addition, national security and cyberspace appear frequently at this stage, which is not only the original intention of the concept of cyberspace, but also the main research direction in the future. Cyberspace has the characteristics of cross-regional and cross-cultural. For the research of cyberspace security, we must look at the whole world and consider a variety of internal and external factors comprehensively.

4. Conclusion

As a newly proposed concept, cyberspace still lacks in-depth research. In related fields, there are neither core influential researchers and research groups nor leading scientific research institutions.

Generally speaking, the related disciplines of Cyberspace Security are still in the early stage of development and have broad research space. Research on Cyberspace Security requires researchers to have an international perspective, to analyze problems from a global perspective and to draw on advanced experience. On the other hand, we should take national security as a starting point and face up to the backwardness and shortcomings of China's cyberspace governance in order to effectively standardize the order of cyberspace. The analysis of CSSCI index data can not fully understand the development of cyberspace, especially the lack of Engineering Science and technology literature. The data need to be further improved in order to provide useful reference for related research.

References

[1] Vrooman H, Cocosco C, Stokking R, et al. KNN-based multi-spectral MRI brain tissue classification: Manual training versus automated atlas-based training[J]. Progress in Biomedical Optics & Imaging, 2006, 6144:61443L-61443L-9.

[2] Yijiu Zhao, Yu Hen Hu, Jingjing Liu. Random Triggering-Based Sub-Nyquist Sampling System for Sparse Multiband Signal. IEEE Transactions on Instrumentation and Measurement. vol. 66, no.7: 1789-1797, 2017

[3] Yijiu Zhao, Shuangman Xiao. Sparse Multiband Signal Acquisition Receiver with Co-prime Sampling, IEEE Access. vol.6, pp. 25261-25269, 2018.

[4] Bragg D C. Reference Conditions for Old-Growth Pine Forests in the Upper West Gulf Coastal Plain[J]. Journal of the Torrey Botanical Society, 2002, 129(4):261-288.

[5] Zhang Y, Wang S, Phillips P, et al. Detection of Alzheimer's disease and mild cognitive impairment based on structural volumetric MR images using 3D-DWT and WTA-KSVM trained by PSOTVAC[J]. Biomedical Signal Processing & Control, 2015, 21:58-73.