International Journal of Digital Crime and Forensics
Volume 12 • Issue 4 • October-December 2020

Design of Cyberspace Security Talents Training System Based on Knowledge Graph

Xi Chen, Guizhou Normal University, China
Fangming Ruan, Guizhou Normal University, China
Lvyang Zhang, Yiwu Industrial and Commercial College, China
Yang Zhao, JiLin University, China

ABSTRACT

Internet, big data, global society, economy, life, politics, military, and culture are deeply integrated and have developed into an era of overlapping cyberspace and real society. Cyberspace security has become the most complex, comprehensive, and severe non-traditional security challenge facing all countries in the world. However, the talents in the field of cyberspace security cannot meet the practical needs of the development of cyberspace security. This paper puts forward the training scheme of network security talents, discusses the relationship between knowledge atlas and network space security, gives the construction and distribution of network space full knowledge atlas, and then constructs an education big data architecture for cyberspace security based on knowledge graph around the use of knowledge.

KEYWORDS

Cyberspace Security, Education Big Data, Knowledge Graph, Talents Training

1. INTRODUCTION

Today, the emergence, development and popularization of the Internet are changing the whole world. While bringing convenience to people, they also bring many hidden dangers. In recent years, data information has leaked, malicious attacks by hackers, the emergence of blackmail viruses, various network destruction incidents have occurred, and the network is full of traps and dangers. Network security has threatened people's security, social security, economic security and even It is national security. As a brand-new technical specialty, cybersecurity involves the lifeblood of the country and is related to the security and sovereignty of the country. Without national security, there is no national security.

The competition in cyberspace is, in the final analysis, talent competition. Under the impetus of global network technology, the development of the whole society is inseparable from the network. The development of all walks of life depends more and more on the security of cyberspace security

DOI: 10.4018/IJDCF.2020100104

talents, and the demand for network security talents has reached an unprecedented height (Weng, Ma, & Gu, 2016). Network security involves various fields, network security threats are frequent, and network security connotation is expanded. However, there are problems such as large number of network security talents, low professional and technical capabilities, and unreasonable structure. In terms of subject education, the cybersecurity subject curriculum is unreasonable, and it is not integrated with the actual social needs, and there is no correct guidance for the development of learners. The traditional talent training model can no longer meet the development needs of cultivating cyber security talents. The cyberspace security discipline has its own characteristics. It can't just cultivate network security talents through the simple theoretical knowledge of cybersecurity and the transfer of technical knowledge. And practice is not to train high-end talents for network security. The emergence of educational big data has provided a new powerful weapon for solving this problem. It uses educational big data to analyze and mine valuable information for cultivating cyber security talents, change the traditional talent training model, and establish a sound cybersecurity domain specific. Talent development plan.

In view of the shortage of network security personnel and the unreasonable training mode of network security personnel cannot meet the demand, this paper analyses the current situation and problems of network security personnel training, and puts forward a gradient training standard model of network security personnel, and designs a large data body of network space education based on knowledge graph. Department structure, strengthen the construction of cyberspace security specialty and discipline system, so that a steady stream of cybersecurity personnel into the field of cybersecurity.

2. GOLDEN STONE CYBERSPACE SECURITY TALENTS TRAINING

2.1. Preliminary Exploration of Cyberspace Security Talents Training System Based on Education Big Data

On May 29, 2012, the United Nations Global Pulse released the white paper "Big Data for Development: Opportunities and Challenges (Pules, 2012)." The report points out that the world has entered the era of "Big Data", which brings both opportunities and challenges. On April 17, 2016, China's first report on the development of big data in the field of education, the Blue Book on the Development of Big Data in China's Basic Education, was officially released. The report combed the progress of policies related to the global big data in education, interpreted the connotation and uniqueness of the big data in education, and analyzed the source and structure of the big data in education. This paper introduces 13 kinds of educational data acquisition technologies, which are commonly used in four categories, and puts forward 7 typical educational data analysis models (Lu, 2016). Although there are a large number of universities, educational training institutions and educational products in China, they are very small compared with the huge potential market scale. For network security personnel training is still in its infancy. Education big data is not only reflected in the "quantity", but also in the "value". How to make full use of the "quantity" and "value" of big data in education to cultivate network security talents is a common problem faced by all countries in the world.

In the process of training network security talents, it is very important to fully understand the needs of the market and the field, and to understand the needs and abilities of learners. The "quantity" of big data in education helps educators grasp the development of network security through the analysis of big data, grasp the learners' own characteristics and learning cognitive ability, so that each learner can be taught in accordance with his aptitude. The "value" of big data in education helps educators fully dig out the valuable information behind these big data and use it to train network security talents.

2.2. Golden Stone Plan

Cyberspace security has received the attention of countries around the world. More than 50 countries including the United States, South Korea, Japan, and the European Union have successively issued

national cybersecurity strategies. In terms of cyber security talent training, there are no exceptions. Many countries have plans to train cyberspace security talents. In the United States, there is a "National Cyberspace Security Education Program". It is expected that the general layout and actions of the country will be popularized in information security and regular academic qualifications. Education, professional training and certification have established a systematic and standardized talent training system to comprehensively improve the information security capabilities of the United States (Han, Wang, Huang, & Lu, 2012). There is a BOB program in Korea, which is a major program for cultivating cyber security talents in Korea. It trains 100 young hackers every year, and then selects the best among these young hackers to form a national hacker team.

On June 11, 2015, the Academic Degrees Committee of the State Council officially approved the addition of "cyberspace security" as a national first-level discipline (Zhang, Yu, & Zhai, 2016), which reflects the importance that the state attaches to the training of cyberspace security talents, and therefore designs a complete cyberspace security talent training. System and mode are particularly important (Yang, Zhou, & Liu, 2016). In this context, the author team has developed the Golden Stone Project, which provides a new engine for cultivating high-end network security talents in the future and leading the sustainable development of the network security industry. There are several main clues in thinking about the importance of cybersecurity and talent development in the new world order – big, understanding, knowledge, practice.

To say "big" first, if you want to be different, you must have a big perspective. The Confucius Institute promotes cultural concepts and philosophical systems throughout the world, which are worth learning from in terms of international cyber security talent development. Mr. Yang Yixian's "General Safety Theory" and "Safety History" have established a unified basic theoretical system of cyberspace security. Under the premise of almost no restrictions in science and engineering, it reveals some basics of hacker attack and defense and security evolution. law. These rules can be applied to all major branches of cyberspace security. Establishing an international network security talent training system requires a global perspective and a comprehensive understanding of the basic theoretical system of network security.

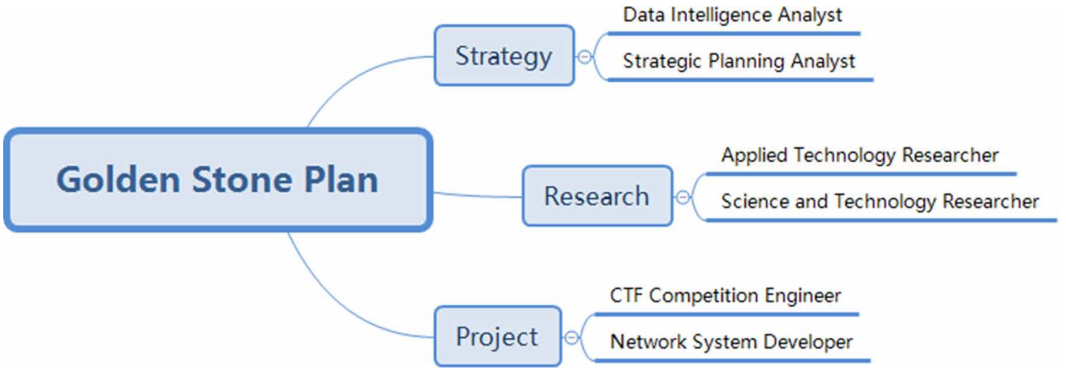
"Understanding", there are three important points in the process of cyber security talent training. The first one is "You want to understand him". The learner is our God. The needs and characteristics of learners are increasingly required to tailor them. The second one is "He wants to understand you". In the international network of talent training, effective communication is still the top priority. "You know him" and "He knows you too." After that, "you and he will understand it together." Security issues without borders have become a problem of pan-globalization, not only in the field of international cyber security talents, but also at the international level. The network security cooperation team will also be the future development trend, jointly promote the interconnection and sharing of network space, share the common governance, and jointly build a community of cyberspace destiny.

"Knowledge" is divided into four angles, strategy, tactics, battle, and war preparation. Strategically, to establish a sound international network security talent training system requires us to look at the world cybersecurity situation from top to bottom. In terms of tactics, we explore new ideas, new systems, and new mechanisms for talent training models from the shallower to the deeper. In the campaign, we will deploy talents from the outside to strengthen the joint training of universities and industries, and promote the in-depth cooperation and innovation in the talent training model among the various sectors of government, industry, and research. In combat readiness, there must be reserves for fighting, and high-end talents should be reserved from near to far.

Finally, it is "practice". In terms of the importance of practicing cybersecurity and talent cultivation in the new world order, there are two points. First, improve the top-level design of network security talent construction. Second, strengthen the construction of network security majors and discipline systems, accelerate the construction of network security talents and innovation bases, form a continuous training mechanism for school-enterprise cooperation as soon as possible, and promote the continuous development of high-level talents for network security.

Golden stone plans to set up three major positions according to the different needs of the current society for network security talents: strategic posts, research posts and technical posts. The strategic post requires network security personnel to conduct in-depth study of comprehensive knowledge in the field of network security, to grasp network security in general, to keep up-to-date information on network security, and to make corresponding strategic planning; The personnel conducted in-depth research on the events in the field of network security, analyzed the technical means and preventive measures contained therein, and issued research and analysis reports; the technical posts mainly required network security personnel to master the professional technical means in the field of network security. On the basis of these three major positions, each post was subdivided. In the strategic post, it is divided into data intelligence analysts and strategic planning analysts; in research posts, it is divided into application technology researchers and scientific and technical researchers; in engineering posts, it is divided into CTF competition engineers and network security system developers (Figure 1).

Figure 1. Golden stone plan structure diagram



According to the requirements of social security talents and the characteristics of network security itself, the training process can be divided into three stages. The first stage is to learn the introduction of network security, the status quo, the main threats, etc., and lead learners to fully understand network security. To cultivate learners' interest in cybersecurity and to lead learners. In the second stage, we will increase the learning of technical courses that must be mastered by cyber security technology, deeply explore the characteristics and interests of learners, and conduct special task evaluation and selection. The tasks include technology, scientific research, and strategic perspective. Through the assessment to understand the learner's knowledge of the situation, and self-recommended courses, in order to achieve the purpose of personality training. In the third stage, we will focus on actual combat and conduct in-depth battles with cyber security companies. Through the training and assessment of the first two stages, learners will find a position of their own interest or show their strengths in this aspect, and can focus on this direction in the third stage.

3. PRELIMINARY CONSTRUCTION OF KNOWLEDGE GRAPH OF CYBERSPACE SECURITY DISCIPLINE

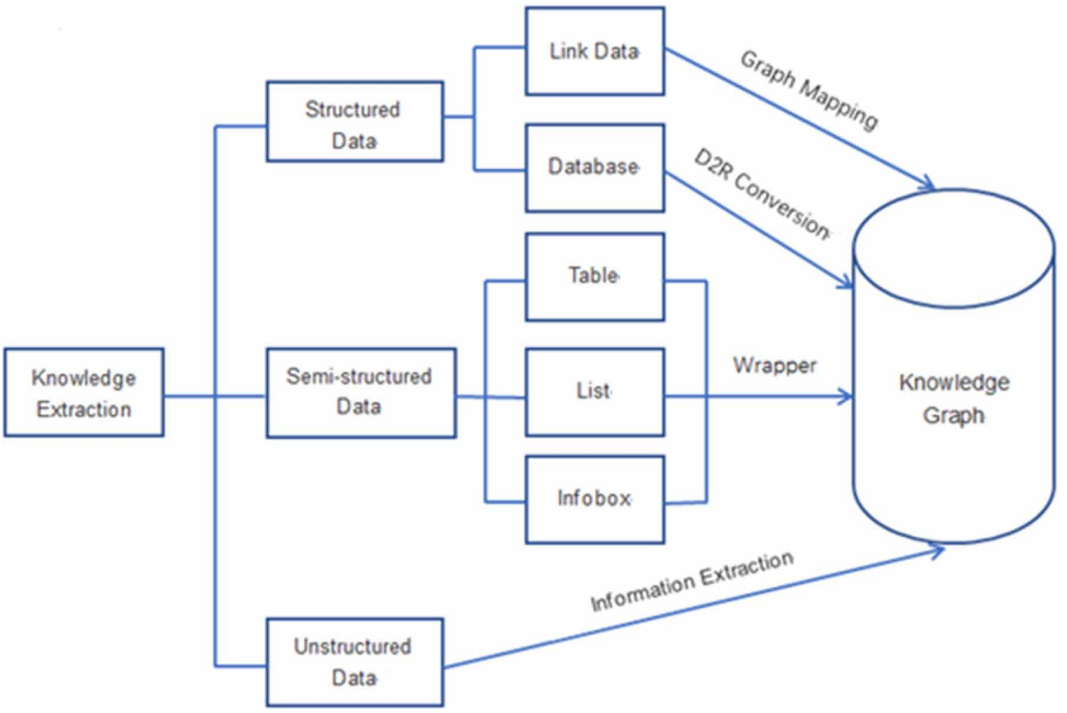
According to the six positions set by the Golden Stone Project, the abilities required for each position are different. The courses and knowledge required to be learned in the process of training should also be different. However, from the current cyberspace security discipline system, the curriculum is too singular, targeted and practical, and the links between courses are often neglected. The knowledge learned by learners is fragmentation. Cannot be combined into a completed system. Although the

discipline of cyberspace security has certain links with disciplines such as computer, mathematics, and communication, it also has its own characteristics that are different from other disciplines. However, the existing curriculum and training programs are mostly directly selected from these similar disciplines. They do not fully consider the differences in the discipline of cyberspace security, and specifically set up courses and develop training programs for this subject.

Constructing the subject knowledge graph can effectively solve the problem of unreasonable cyberspace security curriculum setting and help learners to fully understand the cyberspace security discipline. The knowledge graph is essentially a semantic network. It is a graph-based data structure composed of nodes and edges. That is, the knowledge graph is a structured semantic knowledge base that describes the concepts and their relationships in the physical world in symbolic form (Zhou & Ma, 2018). The points in the knowledge graph represent entities in the real world, and each edge represents the relationship between the entity and the entity. Each entity is represented by several attributes, and the entities are related by the attributes of the entities (Wu, Chen, & Zhao, 2017). The knowledge graph construction mainly includes three steps of knowledge extraction, knowledge representation and knowledge storage.

Knowledge extraction is the extraction of knowledge from data of different sources and different structures, and the formation of structured data is stored in the knowledge graph. The resources used for knowledge extraction are mainly divided into structured data, semi-structured data and unstructured data. The structured data includes the linked data and the relational database that have existed in the form of knowledge graph. For the linked data, the map mapping method can be used to extract the knowledge. For the relational database, the D2R conversion method is mainly used to extract the knowledge. Semi-structured data contains tables, lists, forms, and Infobox, which can be extracted using a wrapper. For unstructured data, this branch is extracted using information in natural language processing for knowledge extraction (Figure 2).

Figure 2. Knowledge extraction classification and inclusion of technical diagram

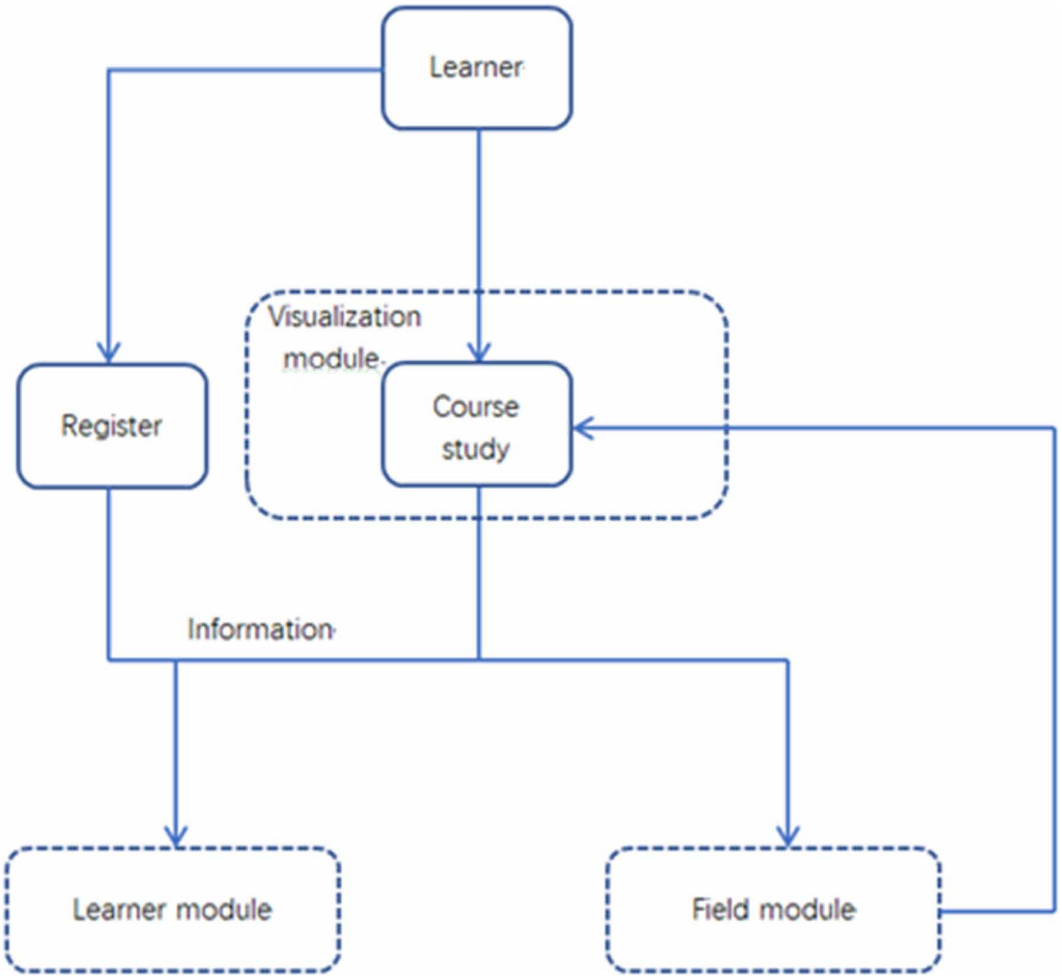


Knowledge representation is to realize the modeling of things in the real world and the relationship between things, to give data in line with the logical information expressed by human beings, and to enable barrier-free communication between people and computers (Ou, 2018). Early knowledge representation methods include first-order predicate logic, production systems, frameworks, semantic networks and so on (Li & Feng, 2017), but these methods all have various defects. At present, most of them use RDF, RDFS, OWL, XML and other representation methods to construct knowledge modeling and expression. Knowledge storage mainly stores knowledge graph in the form of graphs in the database. Typical databases include Google's Frecbase, Microsoft's Stori, OrientDB and PostgreSQL.

4. ARCHITECTURE DESIGN

The education big data architecture design of cyberspace security education based on knowledge graph includes three modules: learner module, domain module and visualization (Figure 3).

Figure 3. Cyberspace security education big data architecture design diagram



4.1. Learner Module

The learner model is a data structure used to represent the learner's current knowledge state (Polson & Richardson, 2013). It reflects the learner's personal characteristics, knowledge learning state, cognitive ability and so on. The learner model should include learner-related personal characteristics, interactive elements between learners and the system, learning situation of knowledge, and all behaviors related to teaching activities. The more information the learners have in the model, the better they can understand the positions, abilities and cognitive level of the learners who want to work in the field of network security and train the learners according to the current requirements of network security. Typical student models include lead plate model, cover model, cognitive model and so on. Different models have different emphasis. In order to reflect the learner's information comprehensively and update the student model dynamically, this paper synthesizes and simplifies the classical student model, and finally constructs a student model based on CELTS-11 specification. The model includes three parts: personal information, knowledge structure and learning behavior.

4.2. Domain Module

Domain module is used to describe the curriculum, knowledge points and their relationship by constructing knowledge map. The data resources of network security knowledge atlas mainly come from the training programs and courses established by different universities in the subject of network space security, and the professional training courses set up by network security enterprises. The original resource data are extracted by different technical means, and the pre-processed data are logically defined and described to build ontology database and form ontology model. The ontology model is mapped to the knowledge map, and the knowledge relationship of the subject is visualized to the learners in the form of knowledge map.

The specific construction process of this knowledge map is as follows:

1. Identifying areas for knowledge mapping.

   The knowledge domain of this system is network space security.

2. Defining hierarchies.

   This step is mainly used to determine the hierarchical structure of knowledge structure atlas, including the number of layers and the specific meaning of each layer.

3. Extracting the main concepts in the knowledge domain according to the hierarchical structure.

   According to the hierarchical structure defined in the second step, this step extracts knowledge concepts from the knowledge domain and determines the hierarchy of the concepts.

4. Defining relational models.

   This step determines the type of relationship between knowledge concepts and the level of nodes connected by each relationship.

5. Designing knowledge structure atlas storage structure.

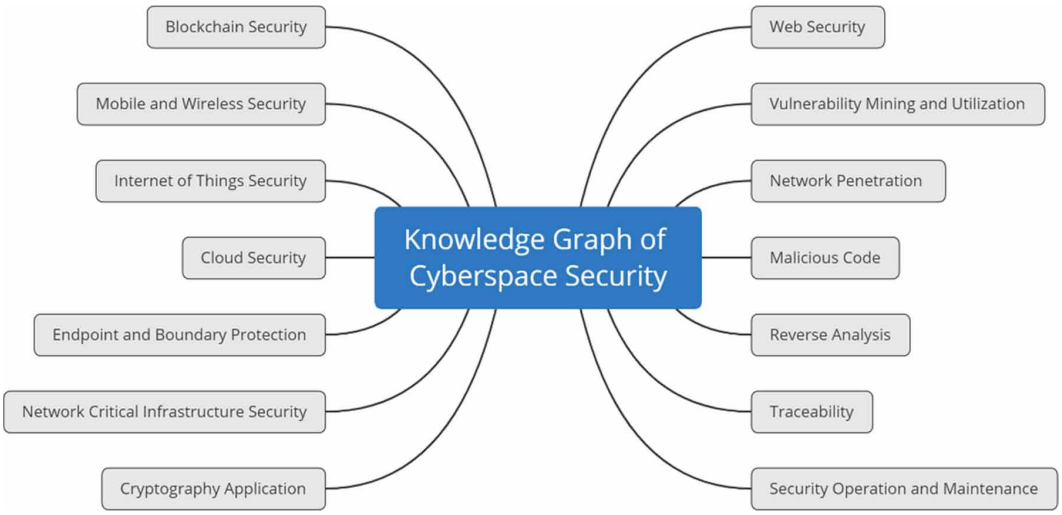
   This step defines the storage structure for the designed knowledge structure atlas. The storage structure mainly includes node tables and relational tables.

6. Constructing a Map of Knowledge Structure.

According to the defined hierarchical type and relational model, and the selected knowledge concepts, the knowledge structure atlas is constructed.

This paper divides the knowledge and skills system of Cyberspace Security talents into 14 subsystems, which are Web security, vulnerability mining and utilization, network penetration, malicious code, reverse analysis, traceability forensics, security operation and maintenance, cryptographic application, network key infrastructure security, endpoint and boundary protection, cloud security, Internet of Things security, mobile and wireless security. Secure block chain. Each first-level node is divided into several second-level nodes, and the second-level nodes are classified into several third-level nodes, not more than four-level nodes (Figure 4).

Figure 4. Knowledge graph of cyberspace security



4.3. Visualization Module

Visualization module is the interface between learners and the system, and the display interface of the system. Based on the knowledge logic relationship of learners' cognitive level, post competence requirements and knowledge map, the corresponding courses are recommended and presented to learners through visual module.

5. CONCLUSION

Cyberspace has become the "second living space" of all countries in the world. The international competition and confrontation around cyberspace is increasingly fierce. The cyber warfare has obvious asymmetry. The network security prevention and control capability is weak, and it is difficult to effectively deal with organized organizations between countries. Cyber attacks, even a hacker can challenge a country and threaten the security of an entire country. Countries around the world have fully realized the importance of cultivating cyberspace security talents and have raised the cyberspace security talents to the strategic level of national security. There is a huge gap in cyberspace security talents, and the shortage of high-end talents is particularly serious. This has always been a shortcoming in the development of cyberspace security. Countries are improving the cyberspace security talent

training mechanism, starting from the basic education of cyberspace talents, and accelerating the construction of a cyberspace discipline system. The rise of educational big data is changing the traditional talent training education model and accelerating the transformation and upgrading of the education model. Make full use of the two major advantages of the "quantity" of education big data and the "value", deepen the analysis and excavate the information that guides the training of cyberspace security talents, and help the establishment of cyberspace security personnel training programs. This paper proposes the network security talent training plan - the Golden Stone plan, and describes the relationship between cyberspace security and knowledge graph, and builds a cyberspace security education big data structure system based on knowledge graph. The training of cyberspace security talents has a long way to go. It needs to be oriented to the needs of the country and society, to the renewal and development of technology, to put capacity training at the core position, and to promote the continuous growth of network security talents.

REFERENCES

Jian, W., Ma, C., & Liang, G. (2016). Discussions on the talent cultivation of cyber security. *Chinese Journal of Network and Information Security*, *02*, 2–3.

Li, H. R., & Feng, H. P. (2017). *Review of Knowledge Graph Domain in Information Behavior*. Library Theory& Practice.

Lu, Q. (2016). Blue Book on China's Basic Education Big Data Development (2015). *Information Technology Education in Primary and Secondary Schools*, *5*, 4.

Ou, Y. (2018). A Survey of Knowledge Graph Technology Research. *Electronics World*, *13*, 55.

Polson, R. (2013). *Foundations of intelligent tutoring systems*. Psychology Press. doi:10.4324/9780203761557

Pulse UNG. (2012). *Big data for development: Challenges & opportunities*. Naciones Unidas.

Wei, H., Xing, W., Xue, H., & Lu, C. (2012). Analysis of the NICE Network Space Security Talent Team Framework in the United States. *Security Science and Technology*, *09*, 53.

Wu, Chen, & Zhao. (2017). Learning Path Recommendation Based on MOOC Platform Data and Knowledge Graph—Taking Software Engineering as an Example. *Industrial and Informatization Education*, (11), 33-38.

Yang, L., Zhou, X., & Liu, S. (2016). Research on the training mechanism and mode of cyberspace security talents under the background of big data. *Journal of Information*, *35*(12), 80–87.

Zhang, H., Yu, H., & Zhai, J. (2016). Planning suggestions for cyberspace security personnel training. *Journal of Network and Information Security*, *3*, 1–9.

Zhou, L., & Ma, Z. (2018). Intelligent Reference Architecture Design of Network Information System Based on Knowledge Graph. *Journal of Chinese Academy of Electronics*, *4*(13), 379.

Chen Xi is a postgraduate student of Cyberspace Security in College of Big Data and Computer Science, Guizhou Normal University. Her main research fields are cybersecurity, data mining, and so on.

Fangming Ruan received his BS degree in electronic engineering in Jul 1982 from Guizhou University of China, received MA degree in education in Jul 2006 from Guizhou Normal University of China, and received Ph D in Engineering with major in electromagnetic fields and electromagnetic waves, Jul 2009 from Beijing University of Post and Telecommunication. He was with Liupanshui Normal College from Aug 1982 through Feb 2000 as an instructor and an associate professor (since1997). In Mar 2000 he moved to Guizhou Normal University of China. From Sept 2004 through Sept 2005 he worked as a visiting scholar in Fujiwara Electromagnetic Environment Lab of Nagoya Institute of Technology, Japan. Since Dec 2006 he has been a full professor in Guizhou Normal University. Dr Ruan is a senior member of China Institute of Electronics (CIE), a senior member of China Institute of Communication (CIC). Since Nov 2015 Dr Ruan has been awarded IEEE senior membership. Dr Ruan has published more than 100 papers in academic journals and academic conferences. As the research team leader, he has completed 11 research projects supported by the national government and the provincial government of China. Dr. Ruan is the owner of 4 patents. Dr Ruan was electromagnetic compatibility (EMC) commission member of CIE and CIC, and was a TPC member of 2012 Asia-Pacific Conference on Electromagnetic Environment (CEEM'2012) and CEEM'2015. Dr Ruan was awarded 2015 Guizhou Province Third Prize of Science and Technology Advancement, and 2014 Third Prize of Science and Technology Advancement of Guizhou Universities and Colleges. Prof. Ruan is advisor of graduates both in Guizhou University and in Guizhou Normal University, having more than 10 graduate students, teaching graduate level classes on RF and microwave technology, principles and design of electromagnetic compatibility (EMC), and Tera Hertz technology. Prof. Ruan has been assigned to be an advisor of Ph D graduates since 2017. Dr. Ruan was a reviewer of China Communications, Chinese Journal of Radio Science, the Journal of Tianjin University, Chinese Journal of Physics, and the like. Prof. Ruan is a member of Chinese Institute of Cyber Space Security.

Zhang Luyang, Special Fellow of Dalian Foreign Studies University, Special Expert of Technical Committee of Big Data Security Laboratory of Guizhou Normal University, Member of Competition and Exercise Committee of China Cyberspace Security Association, Popular Science Worker of Chinese Academy of Sciences. Excellent in artificial intelligence, computer vision, network security and fields, etc.

Zhao Yang received her bachelor's degree from Jilin University in 2019. Her main research interests are network security and education data.