Journal of Human Resource Development (2024)
Clausius Scientific Press, Canada

DOI: 10.23977/jhrd.2024.060401
ISSN 2616-3357 Vol. 6 Num. 4

Exploration and Research of AI-based Cyberspace Security on the Personnel Cultivating—Taking Guangdong University of Science and Technology as an Example

Ma Haifei[1,2,a,*], Chai Wen Chuah[1,b], Fan Yong[1,c]

[1]Academy of Computer Science, Guangdong University of Science and Technology, Dongguan, China
[2]Key Lab of Education Block Chain and Intelligent Technology, Ministry of Education, Guangxi Normal University, Guilin, China
[a]Mhf0515@163.com, [b]aiwenchuah@gmail.com, [c]fanyong@gdust.edu.cn
[*]Corresponding author

Keywords: Cyberspace security; Artificial intelligence; Talent training; Application-oriented undergraduate

Abstract: Following limitations of cyberspace security professional teachers, unclear fostering goals and outstanding result under the background of artificial intelligence. Hence, to improve the quality of cyberspace security personnel training, this paper takes Guangdong University of Science and Technology as an example to discuss cyberspace security personnel training. We propose the following discussion from five aspects: optimize curriculum system, construct teacher team, emphasis discipline competition and scientific research, reform teaching method and build laboratory. It aims to grasp the new perspective of cyberspace security construction under the background of artificial intelligence, and build a new path to improve the quality of talent cultivating.

1. Introduction

The report to the 20th National Congress of the Communist Party of China clearly pointed out that China's economy should focus on promoting high-quality development, commit to building a modern industrial system, accelerate the process of new industrialization, and actively move toward the goal of being a cyber-power and a digital power [1][2]. In order to respond to the needs of high-quality economic development and enhance global competitiveness, we must adhere to the strategy of strengthening the country through talent and devote ourselves to cultivating top-notch innovative talents. Especially under the background of artificial intelligence, strengthening the cultivation of professionals in cyberspace security has put forward new challenges and requirements for the development of education, especially the development of higher education. However, at present, the cultivation of cyberspace security professionals in higher education in China is still in the stage of exploration and development. Since 2015, China has taken a series of important measures to implement the national security strategy and accelerate the training of high-level talents

in cyberspace security [3]. The Academic Degrees Committee of The State Council and the Ministry of Education added the first-level discipline of "cyberspace security" under the category of "engineering". Subsequently, Cyberspace Administration of the CPC Central Committee, the National Development and Reform Commission, the Ministry of Education and other departments jointly issued the opinions on strengthening the construction and talent training of cyberspace security [4]. In 2017, a ten-year demonstration project for the construction of first-class cybersecurity colleges was launched, aiming to form 4-6 high-level cybersecurity colleges. Since 2013, Guangdong University of Science and Technology has opened a network engineering (including the direction of network security) to meet the actual talent demand of Dongguan and the Guangdong-Hong Kong-Macao Greater Bay Area, and is committed to the cultivation of network security talents. In 2018, the network engineering major became the first-level undergraduate major construction point of Guangdong Province, and the IEET engineering education certification major. Faced with the strategic needs of the national network power, the traditional information security continues to evolve into cyberspace security. In 2022, the Ministry of Education approved in Guangdong University of Science and Technology the newly established undergraduate major of network security based on the existing network engineering (the branch of network security), focusing on the cultivation of cyberspace security talents. The fostering talent objective is based on Dongguan zone and the Guangdong-Hong Kong-Macao Greater Bay Area to adapt to the needs of regional economic and industrial development, to take the implementation of moral education as the fundamental task, to cultivate the comprehensive development of moral, intellectual, physical, beauty and labor. Specifically, at first, the fostering talent objective could be able to systematically master the basic theories and methods in cyberspace security, with a strong practice ability of innovation and engineering, independent learning ability, and good comprehensive quality. And then, high-quality application and innovation talents who are able to engage in the work of system design and analysis, security operation and maintenance from software or hardware, fostered talents could work in security planning and management related to cyberspace security in government agencies, internet enterprises, financial institutions, educational and scientific research institutions and other related fields. In recent years, with the wide application of artificial intelligence, large-scale parameters (above billion levels) and complex computing structures have brought profound changes from various fields, and also posed new challenges and opportunities for the traditional information security. For example, as an emerging specialty based on network engineering (network security branch), the development of cyberspace security in Guangdong University of Science and Technology started later than other mature majors, which is faced with challenges, such as limited teachers, unclear learning objectives and imperfect curriculum systems. It shows the characteristics of multi-disciplinary knowledge integration in the actual teaching. To address these shortcomings of cyberspace security, this paper introduces the new mode of "person-job matching, teaching students in accordance with their aptitude, classified training (PMCT)", and proposes the strategy of optimizing the personnel training objectives, curriculum system, teaching method reform and laboratory construction.

2. PMCT mode

PMCT mode is a new teacher teaching and student learning mode, which aims to foster student demands of society. Traditionally, the structure of "3.5 years of on-campus learning +0.5 years of internship" was optimized to the new model and concept of "person-job matching, teaching students in accordance with their aptitude, and classified training" (PMCT) of "three years of on-campus deep learning + one year student selection". The mode of PMCT has three branches to achieve the way of fostering talent. The first branch is that for students who are interested in further education,

PMCT can provide a perfect promotion mechanism to help students further education. The second branch is that for students who choose employment, PMCT can improve their employment competitiveness through the practical education mode of person-job matching. The third branch is that for entrepreneurial students, PMCT provides a comprehensive entrepreneurship education system, professional and entrepreneurial integration training and entrepreneurial practice courses. The benefits are as follows: First of all, the time structure of PMCT is adjusted to extend the time of practical learning, so as to provide students with more time for career exploration, further education entrance examination preparation or entrepreneurial attempt. Thus, PMCT enhances the practicality and periods of education. Secondly, according to students' interests and career planning, the new PMCT model emphasizes on providing differentiated training paths. Therefore, personalized education strategies can help students to develop in the field they are good at and love, to improve the quality of education and students' satisfaction. Finally, in response to employment, the new PMCT model can increase students' employment adaptability and competitiveness by strengthening practical teaching, personalized training and closely docking with industry needs. 3. The fostering of AI-oriented cyberspace security talents in recent years, the application of AI has posed new challenges and opportunities for the traditional network security field, especially in data privacy and security protection [3].

3. Reform Strategy under PMCT mode

The major of cyberspace security is developed from the original network engineering (network security) for Guangdong University of Science and Technology, inheriting the characteristics of traditional network security. Therefore, in the context, the talent fostering of cyberspace security needs to adapt to this trend of the times, and creatively integrate the artificial intelligence (AI)[6] with the talent cultivating of cyberspace security. Focusing on the cultivation of network security compound professionals with AI background as the goal. To achieve this goal, this paper mainly reflected in the curriculum system, teacher team construction, discipline competition scientific research, teaching method reform and laboratory construction from multi-dimensions.

3.1 Curriculum System Construction

In the curriculum system of cyberspace security major, the basic compulsory courses cover the core knowledge of computers, such as program design, computer network, operating system, computer composition and data structure. In the professional compulsory courses, students need to master advanced mathematics, linear algebra, discrete mathematics, probability theory and mathematical statistics, and information security mathematics foundation. The core courses are divided into two directions: one is network attack, the other is web security, which each direction is supported by three core courses to deepen students' professional skills in specific fields. Following the school's educational concept of PMCT, cyberspace security implements a classified training strategy in the senior year to improve students' employment competitiveness, further education ability and entrepreneurial innovation ability. To strengthen students' AI technology in the field of network security, we first integrated into the special courses of artificial intelligence, such as python programming, artificial intelligence foundation, web crawler and data related security mining courses, to understand and apply emerging technologies. The cyberspace security requires 160 credits, including 44 credits of general education compulsory courses and 10 credits of general education elective courses. Specially, covering mathematics, natural science and engineering foundation required for engineering and technology work in cyberspace security. These courses can provide humanistic quality, correct values, social responsibility, cross-cultural communication and expression.

3.2 Strengthen Teaching Staff

Based on teacher's professional background in information security, we have established teaching staff. However, these teachers originate from network engineering or software engineering, which leads to the lack of systematic professional knowledge system[5]. Traditionally, information security and cryptography education focuses on theoretical research and disregards practical application, which leads to the common shortcomings of teachers in practical operation. However, with the increasing penetration of AI technology, the weakness of these teachers not only directly limits the quality of curriculum construction and the output of scientific research results, but also hinders the improvement of teaching effectiveness, which has a significant mismatch with the demand for cultivating application-oriented undergraduate talents. Therefore, strengthening the construction of teaching staff, especially improving teachers' practical ability, has become the core element to promote the development of network security profession. Thus, we adopt the "external introduction and internal cultivation" (EIIC) strategy to optimize the structure of teachers. At external introduction, we focus on teachers following three points: attracting with dual professional backgrounds of AI and network security, absorbs talents with rich practical experience to join the teaching team from industry and enterprise, and hires industry experts as adjunct professors to promote the deep integration of teaching and practice. In terms of internal cultivation, teachers are encouraged to actively participate in top-level academic conferences, so as to improve their professional literacy. The internal motivation of teachers for personal professional development was stimulated by the implementation of the "old guide new" model. In addition, we cooperate with similar universities to hold academic exchange activities, such as funding a number of key teachers to visit, study and train in top academic institutions in China. We encourage teachers to learn and adopt advanced teaching ideas and methods. These measures not only deepened teachers' understanding of job responsibilities. In daily teaching and research activities, teachers share the recent industry trends and cutting-edge technology development trends each period, and integrate them into teaching practice subtly, in order to achieve the educational goal of applying what they have learned.

3.3 Organized Diversified Discipline Competitions and Research Innovation

In order to cultivate high-quality application and innovation talents in cyberspace security, it is crucial to organize diverse discipline competitions. To organize the diversity of competitions. A network security attack and defense from school-level competition has been specially set up in addition to the traditional CTF and AWT attack and defense competitions. Relying on the professional laboratory platform, we design a series of network security related problems for selecting excellent students to participate in province-level and nation-level competitions. Moreover, to cultivate student innovation ability and forward-looking thinking, we also focus on the integration and innovation competition of AI and cybersecurity, which applies cutting-edge artificial intelligence methods to the field of cybersecurity. And then, by encouraging students to participate in college students' innovation and entrepreneurship projects, work closely with teachers to complete scientific research projects, write relevant papers and complete the conversion of scientific research results.

3.4 Teaching Method Reform

In the reform of teaching methods, for the "network attack and defense technology", "Web security" and other practical courses, actively explore and implement the new teaching mode of "independent learning, cooperative learning, inquiry learning, classroom project-based learning".

This model aims to lay a solid foundation for classroom project practice through in-depth preview and exploration after class. At the same time, it applies project-based learning to closely combine theoretical knowledge with practical operation to improve students' comprehensive quality and innovation ability. Moreover, Chaoxing Learning, as an information teaching tool, provides learning resources and convenient learning platform for students in curriculum implementation. This tool can provide teachers with comprehensive and timely student learning data by recording students' learning trajectories and interactions. These data consist of multi-view index, such as participation, task completion, assignment quality. Thus these data provide strong support for teachers to evaluate students' learning process, making the evaluation more objective, accurate and comprehensive. Further, to emphasize the evaluation of students' learning process, we explore the core element of how to improve the quality of teaching. Therefore, the multiple evaluation methods are adopted to promote students' in-depth understanding and firm mastery of the course content, for example, assignment submission, practical operation display, experimental report writing and oral defense. These methods can provide teachers with timely and valuable feedback.

3.5 Attach importance to Laboratory Construction

Network security is a science that pays attention to actual combat. So it needs to carry out teaching and research work supported by real data, and laboratory construction is an important position to ensure that students can carry out practical operation. Due to the wide scope of cyberspace, there are some challenges, such as the lack of constructing scientific environment, limited verifying innovative technologies, the lower scientific research output. To solve these problems, we introduce school-enterprise foundation joint technical research to jointly complete teaching and research tasks. Under the guidance of the network security Development Center of the Ministry of Industry and Information Technology, the foundation focuses on talent fostering, training certification, network maintenance services and network security science popularization education in digital security, and at the same time, we build a "digital one-stop" network security talent cultivating system. 360 Digital Security Science industry-education Integration Innovation foundation has been established, which is jointly built by Guangdong University of Science and Technology, 360 Digital Security Technology Group and Guangzhou Tengke Company Technology. Hence, through the network attack laboratory, digital security simulation shooting range research studio and other infrastructure and a series of operational services, the innovation foundation builds a linkage development mechanism between higher education and industrial clusters, and creates a network security talent training foundation that integrates talent training, scientific research, technology innovation, enterprise services, student entrepreneurship and other functions.

4. Conclusion

This paper is mainly explored AI-based cyberspace security on the personnel cultivating, taking Guangdong University of Science and Technology as an example, which proposes "person-job matching, teaching students in accordance with their aptitude, classified training" (PMCT) to guide building cyberspace security major. Faced with new challenges era of artificial intelligence, such as the limitations of teacher knowledge, inappropriate teaching methods and lack of outstanding output. We introduce the background of cyberspace security construction in detail. We propose reform multi-view measures, for example, the curriculum system, teacher team construction, discipline competition scientific research, teaching method reform and laboratory construction. The results show that cyberspace security has reached a new level in an era of AI.

Acknowledgments

This work is supported by Quality Project of Guangdong University of Science and Technology "Specialty of Cyberspace Security" (GKZLGC2024355); Teaching, science, Innovation, Teaching and Learning Benefit Project Team project "Cyberspace Security Science and Education Integration Innovation Team Based on OBE concept" (GKJXXZ2023040); 2023 Dongguan Social Development Science and Technology Project "Research on Cross-modal Feature Extraction and Video Person Re-Identification "

References

[1] WU J .Development paradigms of cyberspace endogenous safety and security[J].Science China(Information Sciences),2022,65(05):264-266.

[2] WU J, LI J, JI X. Security for cyberspace: challenges and opportunities[J].Frontiers of Information Technology & Electronic Engineering,2018,19(12):1459-1461.

[3] He L,Ren Q,Ma B, et al.Anti-Attacking Modeling and Analysis of Cyberspace Mimic DNS[J].China Communications, 2022,19(05):218-230.

[4] Quan R,Jiangxing W,Lei H .Performance Modeling Based on GSPN for Cyberspace Mimic DNS[J].Chinese Journal of Electronics,2020,29(04):738-749.

[5] Smith L K, Southerland S A. Reforming practice or modifying reforms? Elementary teachers' response to the tools of reform[J]. Journal of Research in Science Teaching: The Official Journal of the National Association for Research in Science Teaching, 2007, 44(3): 396-423.

[6] Zhai X, Chu X, Chai C S, et al. A Review of Artificial Intelligence (AI) in Education from 2010 to 2020[J]. Complexity, 2021, 2021(1): 8812542.