DOI: 10.23977/curtm.2023.062013
ISSN 2616-2261 Vol. 6 Num. 20

Exploration of the Collaborative Education Model for Cyberspace Security Talents in the Context of New Engineering Based on Unity of Knowledge and Action

Guosheng Zhao[1], Jian Wang[2], Hailong Liu[1], Jing Li[1]

[1]*College of Computer Science and Information Engineering, Harbin Normal University, Harbin, 150025, China*
[2]*School of Computer Science and Technology, Harbin University of Science and Technology, Harbin, 150080, China*

Keywords: New Engineering; Cyberspace security; Unity of knowledge and action; Collaborative education

Abstract: In the information age, the importance of cyberspace security is increasingly increasing. How to promote the construction of cyberspace security majors and optimize the training mode of cyberspace security talents is a hot research issue. Starting from the teaching concept of unity of knowledge and action, this article first elaborates on the importance and existing problems of cultivating cyberspace security talents in the context of new engineering. Then, it introduces the requirements for cultivating cyberspace security talents, and finally proposes the construction of a collaborative education model for cyberspace security talents that integrates politics, schools, enterprises and research, which will provide experience and guidance for talent cultivation and teaching mode exploration of cyberspace security in the new engineering field.

1. Introduction

With the rapid development of information technology, network has penetrated into every aspect of people's life and become an important part of modern society. However, the ensuing information leakage, virus attacks, cyber crimes and other cyber security problems continue to appear, cyber security has become a special attention to the problem. There can be no national security without cyber security, and promoting the development of cyber security is an integral part of national development. The development of cyberspace security cannot be separated from the cultivation of talents. At present, the society has an increasingly strong demand for cyberspace security talents. Universities, as the cradle of talent training, should take the initiative to assume the responsibility of cyberspace security talents training.

China's Education Modernization 2035, promulgated in 2019, is the country's first programmatic document on the theme of education modernization, and "integration of knowledge and action" is written into China's education policy as a basic concept."Knowledge" represents the cognitive orientation and "action" represents the practical orientation [1]. The educational concept of "integration of knowledge and action" aims to break the barrier of separation between education and social practice. From the perspective of "integration of knowledge and action", there are still some problems in the current training mode of cyber security professionals in Chinese universities. Firstly, the current talent training mode weakens students' ability to accept the knowledge of cyberspace security and their desire to explore new knowledge. Secondly, practical teaching is not paid enough attention to. Most teachers engaged in the teaching of cyberspace security lack the practical ability of engineering, and there is a lack of sufficient school-enterprise cooperation bases and comprehensive experiments. In addition, cyber security attack and defense have two sides, not only need to strengthen the training of security personnel "knowledge", more importantly, it is necessary to deeply explore the training of security personnel "line". Collaborative education emphasizes that it is not only necessary to rely on universities to carry out theoretical and practical teaching for students, but also to cultivate truly high-level cyber space security talents with the help of government policies and enterprise platforms. Therefore, it is of great significance to explore the collaborative education mode of "integration of knowledge and action" for cyber space security talents under the background of new engineering.

2. Training objectives for cyber security personnel

Compared with traditional engineering talents, the emerging industries and new economy in the future need high-quality composite new engineering talents with strong practical ability, strong innovation ability and international competitiveness [2].Under the background of new engineering, the major of cyber space security should aim at cultivating well-developed cyber space security talents, which is reflected in the following aspects:

2.1 Interdisciplinary talents with interdisciplinary knowledge

Cyberspace security is a complex interdisciplinary subject arising in the context of information technology and social issues. It not only involves the knowledge of science and technology such as computer science and technology, mathematics, but also integrates the content of humanities such as law and management [3].Compared with the traditional computer specialty, the cyberspace security discipline is characterized by its huge and complex knowledge base and system, strong discipline comprehensiveness and fast technology update rate. In the case of limited class hours, it is difficult for students to comprehensively and systematically understand and master professional knowledge. It is necessary for training units to explore the teaching mode that integrates multiple means and guide students to take the initiative to study independently.

2.2 Applied talents with the ability to solve practical problems

The discipline of cyber security pays special attention to practical operation. Cyber security personnel not only need to master the necessary theoretical knowledge, but also need to have the ability to solve practical problems, and be competent in the development, maintenance and management of cyber security. Practice is not only the application of theoretical knowledge, but also an important means to improve practical ability and independent thinking ability. Through practical operation, students can deepen their understanding of inner knowledge, improve their practical ability and enhance their professional competitiveness.

2.3 High quality talents with social responsibility and moral awareness

Cyberspace security is closely related to law and grey industry interest chain [4]. In personnel training, attention should be paid not only to the cultivation of students' professional skills, but also to the cultivation of students' character. Therefore, the major of cyber space security should pay attention to the ideological and political work of the curriculum, and do a good job in guiding students' thoughts and shaping their values. Teachers should strengthen the sense of social responsibility and mission of network security personnel.

3. Problems facing the training of cyber security personnel

3.1 Disciplinary Barriers

Discipline barrier is a common problem in cyberspace security education. The field of cyberspace security involves multiple disciplines such as computer science, law, policy, and management, and the boundaries between these disciplines can result in students being exposed to only specific areas of knowledge while neglecting other important aspects. This may make students' knowledge one-sided and difficult to fully understand and solve network security problems. There is a need to promote collaboration between disciplines and bring teachers from different disciplines together to design interdisciplinary courses. For example, computer science and law faculty can work together to create a cybersecurity law course that allows students to gain technical and legal knowledge. This helps to develop a more well-rounded cybersecurity professional.

3.2 Technical update lag

Technology in the field of cyberspace security is evolving rapidly, but many teaching materials and courses struggle to keep up with this rapid change. This results in students graduating with knowledge and skills that are outdated and unable to effectively address the latest cybersecurity challenges. Universities should establish a continuous updating mechanism, regularly review and update course content, actively cooperate with excellent cybersecurity companies, understand the latest trends and technologies, and ensure that courses are relevant to practical applications.

3.3 Lack of mentor guidance

The Cyber security major requires students to have a wide range of knowledge and skills, covering network architecture, cryptography, vulnerability analysis, threat intelligence, risk management, and ethics. The mentorship system helps students build a solid foundation in this complex field and provides personalized guidance to help students gain a deeper understanding of security principles and practices, guide research interests, develop professionalism, and ultimately produce better, well-rounded cybersecurity professionals to meet the growing cyber threats and challenges.

3.4 Insufficient experimental facilities

At present, there are still some shortcomings in the network security laboratory facilities in universities. First, outdated equipment can make it impossible to simulate and analyze the latest cyber attacks and threats effectively. Second, limited resources, including budgets and access to new equipment, software, and data sets, limit lab expansion and upgrades. In addition, the lack of diversity is also a problem, and the inability to simulate different types of network topologies, operating systems, and applications limits the professional development of students and researchers. To address these issues, lab management teams and stakeholders need to work together to ensure lab facilities remain modern, meet academic needs, provide students and faculty with adequate resources and technical support, while fostering collaborations with other institutions to ensure that the Cybersecurity Lab can effectively train cybersecurity professionals and conduct cutting-edge research.

4. Multi-party cooperative education mode under the unity of knowledge and action

In the existing social environment and education system, colleges and universities are the main battlefield of talent training. It is difficult for most colleges and universities to dynamically grasp and adjust the current situation of social demand and industrial development. In the network space security personnel training system under the background of new engineering, it is difficult to achieve the goal of personnel training in a real sense by relying solely on one party. With the help of government, school, enterprise and research forces to build a multi-party collaborative education model can effectively improve the efficiency and quality of cyber security personnel training.

First, schools should attach importance to the demonstration and leading role of discipline competitions. College teachers should take high-level competitions as the starting point, carry out teaching reform, integrate the resources of various disciplines, set up a teacher-led network space security group, and actively participate in high-level discipline competitions held by the government and enterprises. In the competition, students' practical ability is exercised, their desire for knowledge is stimulated, and traditional passive learning is transformed into active learning. At the same time, it is also conducive to strengthening the communication between colleges and universities and the government and network security enterprises, helping colleges and universities to clarify social needs and industrial development trends, and training applied cyber space security talents.

Second, schools should attach importance to school-enterprise cooperation and promote the integration of production and education. Companies are often at the forefront of cybersecurity technology and can provide schools with the latest technology and trend information, helping to keep the curriculum in step with industry needs and enhance students' social competitiveness. At the same time, enterprises can also provide career guidance and development support to help students plan their career path and provide students with practical job opportunities. Together with well-known IT enterprises in the field of cyber space security, such as 360, Qi Anxin, Green Alliance, Anheng, Deep Trust, Qiming Star and Tianrongxin, etc., in combination with digital economy policies and collaborative education regulations, we implement classified and differentiated training for students with different career development plans [5], and jointly build a long-term mechanism of collaborative education between government, university and enterprise research throughout the four-year university life.Schools should clear specific collaborative ways, establish a reasonable enterprise access system, and ensure that the multi-party collaborative education cooperation mode is controllable and measurable. Through multi-party cooperation and communication, the personnel training model is constantly adjusted, the teaching syllabus and teaching content that meet the needs of society are further standardized, and the evaluation system of the achievement degree of collaborative education goals is established to ensure that the multi-party collaborative education cooperation model is controllable and measurable.

Third, we should attach importance to the collaborative education of science and education and promote the integration of science and education.First of all, interdisciplinary research and education should be encouraged, and cooperation between professional teachers and teachers of humanities and social sciences such as management and law should be promoted to help students develop knowledge backgrounds in various fields.Secondly, in cooperation with enterprises and governments, colleges and universities should build professional cyberspace security laboratories, strengthen the construction of scientific research platforms, create a good scientific research environment, improve the scientific research incentive system, and form a good scientific research atmosphere, so that students who are interested in scientific research can continuously improve their independent learning ability and practical ability in academic research. Finally, it is necessary to actively develop the undergraduate tutor system, which can provide students with personalized guidance, strengthen the communication between teachers and students, carry out two-way choice between tutors and students, and guide students to carry out academic research, course learning and career planning, and help students improve academic ability and professional quality.

5. Conclusion

The construction of cyberspace security and personnel training are in line with the national strategic policies and policies, and are the only way to master the initiative in cyberspace in the new era. As an important institution to cultivate talents, colleges and universities should be guided by the educational concept of "integration of knowledge and practice", not only keep pace with The Times in "knowledge", but also innovate in "practice", and pay attention to the integration of production and education, science and education. Through the construction of a multi-party collaborative education mechanism of government, university, enterprise and research, it can not only solve the dilemma of decoupling the content of college teaching from The Times, but also train students' practical ability in an all-round way and cultivate applied cyber space security talents who meet the needs of society and the requirements of The Times.

Acknowledgments

This work was supported by Heilongjiang Province Higher Education Teaching Reform Research Project (No.SJGY20220351); Research Achievements of the 2023 Key Project of the Education Science Plan of Heilongjiang Province(No. GJB1423438).

References

[1] Guo Yuanxiang. Unity of Knowledge and Action: Implication of the categories of "knowledge" and "action" and its educational guidance [J].Journal of Central China Normal University (Humanities and Social Sciences Edition), 2019, 62 (05):185-194.

[2] Wang Qiaoying, Huang Xiangfeng, Wang Zhiwei et al.Exploration on the teaching mode of discussion course in the background of new engineering [J]. Journal of Chengdu Normal University, 2021, 37(07):45-51. (in Chinese)

[3] Shang Lei. Research and Practice on Training model of Applied Network Security Talents under the background of new engineering [J].Computer Knowledge and Technology,2019,15(13):191-192+194.

[4] LI Panpan, Zhu Rong, Du Xuan et al. Exploration on Training model of applied talents for sustainable competitiveness in Cyberspace security [J]. Journal of Computer Education, 2019(10):121-124.

[5] Zhang Hao, Guo Wenzhong, Dong Chen et al. Cybersecurity personnel training model under the background of new engineering [J]. Computer Education, 2021(08):91-95. (in Chinese)