The Feasibility Exploration of Cyberspace Security Talent Training Program Under the Background of Digital Transformation

Li Tan[a*], Zikang Liu[b], Tianli Yuan[c], Feifei Wang[d], Dongfang Li[e]

School of Computer and Artificial Intelligence, Beijing Technology and Business University, Beijing, China

[a*]tanli@th.btbu.edu.cn, [b]btbu_lzk@163.com, [c]yuantianli@st.btbu.edu.cn, [d]wangfeifei08271@163.com, [e]lifang233333@163.com

Abstract. To address the current primary challenges in cybersecurity talent cultivation in China—specifically, the significant gap between the vast demand for cybersecurity professionals and the inadequate training capacity of universities, as well as the discrepancy between the low quality of cybersecurity talent and the rapid development of internet technologies—this paper closely aligns with the national and Beijing's digital transformation strategies in economic development, alongside the digital transformation of our school's business studies. It aims to explore feasible implementation methods for cultivating cybersecurity talents, consolidate the security foundation of digital economy development, and assist in the sustained and healthy development of the national economy.

Keywords: Teaching Reform, Cyberspace Security, UNDERGRADUATE

1 Introduction

During the "14th Five-Year Plan" period, China's digital economy has entered a new phase of deepened development. This transformation has elevated the concept of security from traditional network security to a more extensive digital security paradigm. In this context, cybersecurity is increasingly seen as a processual factor, evolving into a digital security system with broader coverage and more extensive protective boundaries. Digital security integrates the concepts of security from both application and foundational professional fields, extending its scope to digital business, application scenarios, and other areas of digital integration. This evolution is in response to new security situations and challenges, aiming to ensure the safety of digital development[1].

The essence of cybersecurity concepts, technology products, and industry structure are all poised for pivotal changes. However, the key to reform, innovation, and development lies in talent cultivation. Currently, China's undergraduate cybersecurity

Y. Kuang et al. (eds.), *Proceedings of the 2024 5th International Conference on Education, Knowledge and Information Management (ICEKIM 2024)*, Atlantis Highlights in Computer Sciences 22,
https://doi.org/10.2991/978-94-6463-502-7_27

talent training has not yet established a universal and efficient talent cultivation scheme. This paper aims to research, analyze, and demonstrate plans from various aspects such as training programs, curriculum systems, and talent cultivation positioning. Our objective is to develop a cybersecurity talent cultivation plan and feasible path that aligns with our school's training objectives and serves the economic and social development of the capital city. This effort will implement national security strategies, accelerate the cultivation of cybersecurity talents, fill the domestic cybersecurity talent gap, and solidify the security foundation for the development of the digital economy, ensure the sustained and healthy development of the national economy in a safe and stable environment.

2 Related Work

Currently, the strategic position and importance of cybersecurity have been highly recognized by the international community. Cultivating high-quality cybersecurity talents and increasing the research and implementation of core cybersecurity technologies has become an important protective barrier for building a world important talent center and innovation highland. there is a serious shortage of cyber-security talents in China, which has become a major bottleneck restricting the trans-formation and development of China's digital economy.

However, the cultivation of cybersecurity talents in China is still in its early stages, and a comparative analysis of existing cybersecurity talent training programs shows that there are still challenges in many aspects:

- Limited Availability and Capacity of Cybersecurity Programs, few higher education institutions offer cybersecurity-related majors. The lengthy duration of academic programs leads to outdated knowledge structures. Lack of high-quality and experienced teachers[2].
- Lack of Adequate Simulation Environments and Equipment, most universities with cybersecurity programs lack the necessary simulation environments and experimental equipment. Cybersecurity, being a complex discipline that integrates multiple fields, requires not only strong theoretical foundations but also extensive practical support[3].
- Absence of a Systematic and Effective Training and Evaluation System. A comprehensive, mature, and effective cybersecurity talent training and evaluation system is yet to be developed.
- Inadequate Meeting of Students' Learning Needs. Traditional higher education models, based on academic disciplines and conservative teaching methodologies, fail to meet the rapidly evolving societal demands and technological advancements[4]. For example, with the emergence of new technologies such as artificial intelligence, big data, and dynamic perception, network security technology needs to be continuously innovated.

3 Methodology

To address the identified challenges in cybersecurity talent cultivation, our proposed approach encompasses a multifaceted strategy that focuses on faculty development, practical platforms, curriculum and training systems, and integration of industry, education, and research.

Figure 1 succinctly illustrates our proposed solution and measures. schools aim to enhance the quality of education through measures such as strengthening faculty expertise, refining curriculum structures, and innovating teaching methodologies. Government and enterprises collaborate closely with schools to offer more practical opportunities for students. this trilateral partnership establishes a platform for holistic talent development.

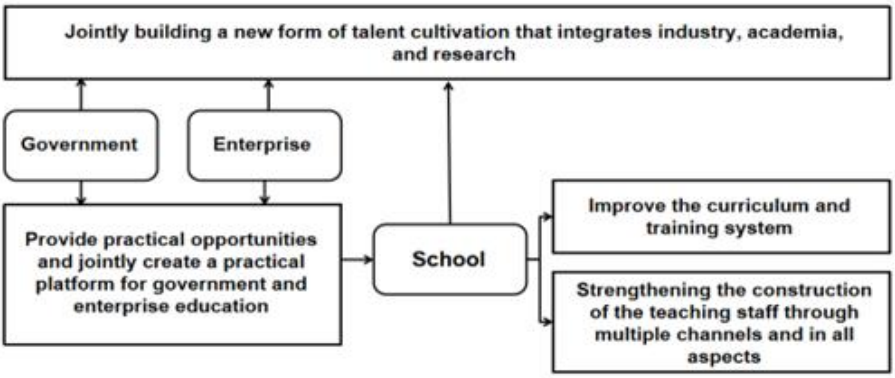

Fig. 1. The proposed reform plan structure diagram

3.1 Faculty Development

Due to the relative weakness of cybersecurity teaching staff, the disconnect between talent cultivation and industry development, and the lack of a tiered talent training system, it's crucial to enhance the training of current faculty to align their quality and level with the objectives of engineering education. Planned training and skill development for young core teachers, such as "Training Courses," "Intensive Courses," and "Advanced Study Courses," should be conducted. These should combine online and offline methods and integrate theory with practice for comprehensive teacher training, thereby enhancing teaching, engineering practice, and design development capabilities.

3.2 Practical Platforms:

Collaborate with national cyberspace authorities to introduce advanced experimental equipment and create virtual network practice environments. Integrating basic principles, offensive and defensive tactics, and testing methods into an interactive virtual simulation system on course websites, thus creating an excellent offensive and

defensive training platform[5]. Treat participation in cybersecurity competitions as one of the evaluation criteria of outcome-based education, integrating students' "in-class + extracurricular + drill + competition" experiences to promote comprehensive cultivation of undergraduate innovation and practical abilities, and quickly building a cybersecurity talent system.

3.3 Curriculum and Training Systems

Firstly, clarify the training objectives and graduation requirements for cybersecurity majors in universities. For example, at Beijing Technology and Business University, focus on disciplines related to business digital transformation, consumer big data center construction, and information and network security issues in food and light industry internet applications. Other universities should also combine their excellent disciplines, focus on promoting interdisciplinary integration, achieving coordinated development[6].

Secondly, based on the training objectives, improve the professional curriculum system based on characteristic course groups. Cyberspace security is a comprehensive discipline that involves various knowledge such as mathematical theory and computer science. In line with the training strategy of emphasizing the foundation and broadening the scope for undergraduate students, based on the school's own characteristics, the direction of cybersecurity majors is expanded, and the scale of relevant professional talent training is reasonably determined. A comprehensive training platform for cybersecurity talents across disciplines such as science, engineering, and management is constructed.

Finally, update the teaching approach and form a student-centered training philosophy. The cybersecurity major is an innovative and rapidly developing field that requires an open mindset and reform of existing training models in order to enable rapid talent growth. Teachers should actively adapt to the rapid development of network technology and the changing needs of educational concepts, constantly update their teaching concepts and ideas, transform from traditional academic authority roles to auxiliary and guiding students in learning, select suitable teaching content, strategies, and evaluation methods based on target needs and actual student sources, and achieve true personalized teaching.

3.4 Integration of Industry, Education and Research

Cybersecurity talent has its uniqueness, with an asymmetry in offensive and defensive capabilities, and a lack of practical scenarios in schools, leading to a gap between students' theoretical knowledge and practical skills. To bridge this gap, it's essential to "open up" the specialization to capable cybersecurity enterprises, reserving space for collaborative education. The cybersecurity major, as an innovative practical application major, has both the humanistic attributes of management majors in the digital economy era and the engineering attributes of computer science and technology. Under the dual attributes, the development of outcome oriented talent training programs and teaching models in cyberspace security majors is scientific and

feasible, aligning talent training programs with international education concepts and complying with relevant regulations on engineering education certification.

Specific measures include inviting quality enterprises to deeply participate in cybersecurity talent cultivation. Strengthen collaboration in every aspect, such as training objectives, course setting, textbook compilation, laboratory construction, practical teaching, research projects, and joint training bases. Continuously deepen the integration of cybersecurity industry and education to establish a long-term mechanism for integration. Invite enterprise personnel to participate in course construction, make practical courses more relevant. Engage teachers in enterprise project development to enhance their practical abilities. Optimize practical teaching content and link it through a project-driven approach to form a teaching model oriented towards actual project development.

4 Analysis

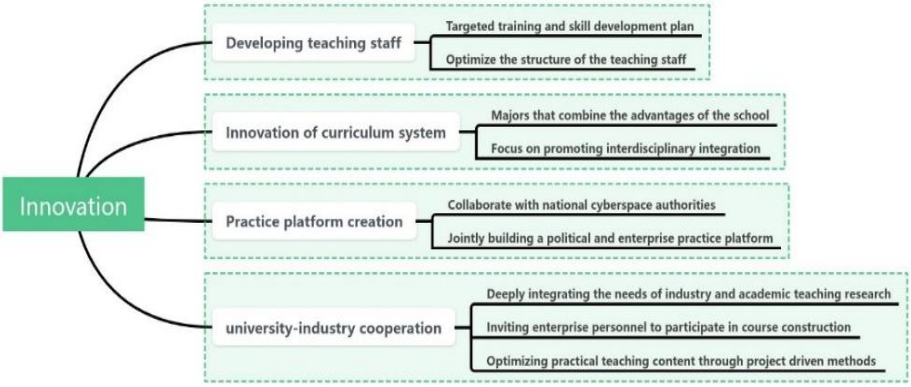

Fig. 2. Advantages of the proposed solution

To evaluate the novelty of our proposed training plan, we conducted a comprehensive comparative analysis with existing cybersecurity training programs in China. From Figure 2, it is clear that our proposed solution has advantages in various aspects. Our approach not only focuses on improving the teaching level of existing teachers, but more importantly, stimulates the academic and teaching enthusiasm of young core teachers through targeted training and skill development plans. Enhance the teaching and engineering practice abilities of teachers. Our curriculum system innovation is mainly reflected in updating the professional curriculum system based on the characteristics of the school and industry needs, with a focus on promoting interdisciplinary integration. Compared to most other universities, our practical platform is to collaborate with the national cyberspace management department, establish a realistic practical environment, and enable students to feel the real cyberspace security threats we face. Our integration of industry, academia, and research is not just superficial cooperation, but also emphasizes deep integration. By

establishing a long-term cooperation mechanism, invite professionals from enterprises to participate in course construction, making the courses more practical and targeted.

5 Conclusion

This paper addresses the current state and challenges of undergraduate cybersecurity talent cultivation in Chinese universities, in light of the severe situation in network security. Aiming to explore a systematic, mature, and effective implementation plan for cultivating cybersecurity talents, thereby solidifying the security foundation for the development of the digital economy. The proposed educational reform plan is significant for implementing national security strategies and accelerating the cultivation of cybersecurity talents. It also holds substantial practical importance in filling the domestic gap in cybersecurity talent and establishing a robust security foundation for the growth of the digital economy.

Acknowledgment

This work is supported by the school level education reform project of Beijing Technology and Business University(jg225109).

Reference

1. Huang, Y. and Y. Zhou. Research on the development path of digital security in China. in The 38 th National Computer Security Academic Exchange Conference. 2023. Changsha, Hunan, China.
2. Zhang, S. and H. Liu, Research on the training mode of cyberspace security talents for new engineering. Network Security Technology and Application, 2023(09): p. 93-94.
3. Miloslavskaya, N., A. Tolstoy, and A. Migalin. "Network Security Intelligence" Educational and Research Center. in 10th IFIP WG 11.8 World Conference on Information Security Education (WISE). 2017. Rome, ITALY.
4. Tian, F.P. and Ieee. Research on Education Big Data Security Strategy under Network Environment. in IEEE 6th International Conference on Big Data Analytics (ICBDA). 2021. Xiamen, PEOPLES R CHINA.
5. Xia, P. and Ieee. Reform of Network Security Technology Practice Teaching System Based on Virtual Simulation Training Platform. in 16th IEEE International Wireless Communications and Mobile Computing Conference (IEEE IWCMC). 2020. Electr Network.
6. Chychkan, I.V., S.O. Spasiteleva, and Y.D. Zhdanova, THE EDUCATIONAL ENVIRONMENT FOR FORMING SECURE BASE BEHAVIOR IN CYBERSPACE OF FUTURE PROFESSIONALS IN ECONOMICS AND MANAGEMENT. Information Technologies and Learning Tools, 2021. **84**(4): p. 354-375.