Article

Research on the Project-based Talent Training Mode Based on Discipline Competition -- Taking Cyberspace Security as an example

Pengteng Huang [1], Gongjin Chen [1] and Yantao He [1,*]

[1] Guangdong University of Science and Technology, Dongguan, China
* Correspondence: Yantao He, Guangdong University of Science and Technology, Dongguan, China

Abstract: To address the persistent issues of disconnection between traditional curriculum systems and rapidly evolving industrial demands, insufficient practical capabilities among students, and a notable lack of hands-on practical experience among faculty members in application-oriented undergraduate cyberspace security education, this paper proposes an innovative, project-based talent cultivation model driven by discipline competition. Taking the widely recognized CTF (Capture The Flag) competition as the primary carrier, the proposed model systematically constructs a three-level progressive training framework consisting of "curriculum reform, campus practical competition, and enterprise cooperative practice." By strategically optimizing curriculum settings to align with real-world cybersecurity threats, innovating pedagogical teaching methods to foster active learning, and significantly strengthening faculty development programs, the educational environment is comprehensively upgraded. Furthermore, by improving dedicated practical laboratory platforms and establishing diversified, competency-based evaluation mechanisms, the deep and sustainable integration of industry and education is successfully achieved. Extensive practical results and empirical data demonstrate that this comprehensive model can effectively enhance students' core professional skills, stimulate their innovative thinking, and substantially boost their overall employment competitiveness in a highly demanding job market. Ultimately, this research provides a highly effective, referential path and actionable guidelines for cybersecurity talent cultivation in local universities, ensuring graduates are fully equipped to meet the complex security challenges of the modern digital landscape.

Keywords: cyberspace security; discipline competition; project-based teaching; industry integration; talent cultivation

Received: 30 January 2026
Revised: 25 March 2026
Accepted: 07 April 2026
Published: 13 April 2026

1. Introduction

Cyberspace has emerged as the fifth domain of sovereignty alongside land, sea, air, and space, with its security being intricately linked to national stability, societal harmony, and the protection of citizens' vital interests. The enactment and enforcement of laws and regulations such as the Network Security Law, Data Security Law, and Personal Information Protection Law have propelled the rapid development of China's network security industry. Forecasts indicate that by 2025, the demand for professionals in China's network security sector will surpass 3.4 million, with an annual growth rate of approximately 15%. Despite this, the number of graduates specializing in cyberspace security from Chinese universities remains below 100,000 annually. This gap highlights significant challenges, including the disconnect between theoretical knowledge and practical application, as well as insufficient engineering practice capabilities, which hinder the ability to meet the industry's demand for highly skilled applied professionals [1, 2].

As illustrated in Figure 1, subject competitions serve as a critical bridge between theoretical education and engineering practice, offering unique advantages in fostering students' innovation, teamwork, and problem-solving abilities in complex engineering scenarios. Among these competitions, the Capture The Flag (CTF) format has gained prominence since its inception at a global hacker conference in 1996. Over the past two decades, CTF has evolved into one of the most influential competitive formats in the field of global network security [3]. Studies have demonstrated that students who participate in discipline competitions exhibit approximately 30% higher employment competitiveness compared to their peers who do not engage in such activities. Furthermore, experience in competitions has become a significant criterion for enterprises in selecting network security professionals, underscoring the importance of integrating competitive experiences into talent development frameworks [4, 5].

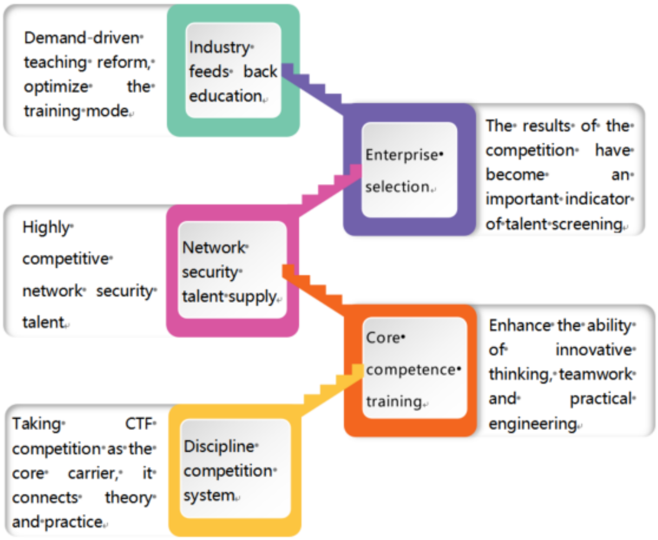

Figure 1. Correlation logic diagram of discipline competition and network security talent training.

Currently, universities across China are actively exploring innovative approaches to cultivate cyberspace security talent [6]. These efforts include the implementation of digital collaborative teaching models, the establishment of multi-tiered competition systems encompassing subject competitions, industry-specific contests, and attack-and-defense drills, as well as the integration of foundational courses with CTF competition elements. However, application-oriented universities face unique challenges in systematically embedding subject competitions into the entire talent development process. The goal is to create a reproducible, project-based teaching model that aligns with the practical needs of the industry while addressing the specific characteristics of these institutions. This remains a critical issue requiring urgent attention and resolution to ensure the effective preparation of students for real-world demands in the network security field.

Taking the cyberspace security program at Guangdong University of Science and Technology as an example, this paper examines a project-based talent cultivation model rooted in discipline competitions. Leveraging the industrial backdrop of Dongguan, a renowned manufacturing hub, the study aims to provide both theoretical insights and practical guidance for the development of network security professionals in local application-oriented universities. By aligning educational strategies with regional industrial needs, this approach seeks to enhance the relevance and effectiveness of talent training programs, ultimately contributing to the broader advancement of the network security sector.

2. Status analysis and problem diagnosis

2.1. The contradiction between industry demand and talent supply is prominent

As the manufacturing hub of the Guangdong-Hong Kong-Macao Greater Bay Area, Dongguan city hosts a significant concentration of small and medium-sized enterprises.

With the rapid pace of digital transformation, the demand for cybersecurity professionals has surged dramatically. Local enterprises primarily seek network security specialists skilled in areas such as security operation and maintenance, penetration testing, and security development. These roles require graduates to possess both a robust theoretical foundation and advanced practical capabilities [5, 7]. However, the traditional methods of talent cultivation exhibit several critical shortcomings that hinder the alignment of educational outcomes with industry needs.

1. The curriculum structure in many institutions does not adequately align with the evolving demands of the industry. Current programs often emphasize theoretical instruction while neglecting hands-on training in areas such as Capture the Flag (CTF) competitions and real-world enterprise scenarios. Surveys reveal that approximately 65% of professional courses still rely on the conventional approach of "theoretical teaching combined with confirmatory experiments." This outdated methodology limits students' ability to apply their knowledge effectively to address practical cybersecurity challenges, leaving a gap between academic preparation and industry expectations.
2. Students frequently lack sufficient practical skills to excel in real-world cybersecurity environments. Cyberspace security is inherently a field that demands high levels of practical engagement, yet constraints such as inadequate experimental facilities and limited instructor expertise restrict students' exposure to authentic attack and defense scenarios. Data indicates that only 23% of students have participated in a comprehensive penetration testing project prior to graduation. While many students are proficient in using specific tools, they often lack the systematic thinking required for effective attack and defense strategies, which is essential for addressing complex security challenges.
3. The practical experience of teaching staff remains insufficient to meet the needs of application-oriented education. A significant proportion of instructors in network security programs come from purely academic backgrounds, with approximately 60% lacking hands-on experience in enterprise-level cybersecurity practices. This limitation hampers their ability to guide students effectively in high-level competitions and real-world projects, thereby restricting the development of students' practical competencies and innovative problem-solving skills.
4. The integration of competitive activities with formal teaching frameworks is not sufficiently developed. Many colleges and universities treat subject competitions as extracurricular endeavors rather than embedding them into the core curriculum. This disconnect results in a lack of synergy between competition outcomes and academic instruction. The absence of mechanisms to transform competition results into valuable teaching resources perpetuates the divide between competitive activities and professional education, undermining the potential benefits of a cohesive approach to learning and skill development.

2.2. Reference from domestic and foreign experience

Foreign countries have long been engaged in the cultivation of cyberspace security talents, developing a competition-driven training system that is relatively mature. Universities such as Massachusetts Institute of Technology and Stanford University in the United States incorporate network security competitions as practical components of their courses, allowing students to earn academic credits through participation. Additionally, these institutions have established close cooperation mechanisms with enterprises, where companies provide internship opportunities and practical projects for students. This collaboration significantly enhances the professional readiness of graduates, with a substantial proportion of students obtaining relevant certifications within a year of completing their studies. Such initiatives demonstrate the effectiveness of integrating academic learning with practical, industry-oriented experiences to foster high-quality talent in the field of cybersecurity [8, 9].

In recent years, domestic universities have actively explored innovative methods to integrate competition with teaching. For instance, Xidian University has developed a talent training model centered on cyber range simulations, introducing a "tower defense" competition system that emphasizes practical skills in both attack and defense scenarios. This approach focuses on cultivating the ability to transition between offensive and defensive strategies effectively. Similarly, Shanghai Overseas Chinese Vocational and Technical University has implemented a progressive competition training framework tailored to vocational undergraduates. This three-tiered system includes curriculum reform, on-campus training competitions, and school-enterprise collaborative practices, yielding notable achievements in national competitions. Zhejiang Wanli University has adopted an "innovation + competition" oriented curriculum structure, combining foundational courses with advanced training modules to align with regional industry demands. By partnering with leading enterprises, the university ensures that students acquire skills that meet specific market needs, resulting in significant success in discipline competitions, with students earning over 40 awards at provincial and higher levels. These examples highlight the growing emphasis on integrating competitive elements into academic programs to enhance the practical capabilities of cybersecurity professionals [10].

The integration of competition systems into the entire process of talent cultivation has proven to be an effective strategy for improving the quality of applied network security education. Establishing mechanisms that promote teaching through competition, encourage learning through competitive activities, and seamlessly blend competition with academic instruction enables institutions to better prepare students for real-world challenges. This approach not only enhances the practical skills of students but also fosters innovation and adaptability, which are critical for addressing the dynamic demands of the cybersecurity industry [1, 11].

3. Construction of project-based talent training mode

3.1. Overall design framework

This study, grounded in the principles of application-oriented undergraduate education, proposes a comprehensive talent training model that leverages project-based teaching and competition-driven learning. The model is designed to integrate theoretical knowledge with practical application, fostering a holistic learning experience. The "two-wheel drive, three-layer progressive, multiple collaboration" framework serves as the foundation for this approach, emphasizing the synergy between project-based teaching and competition-driven modules. The project-based teaching module utilizes real-world CTF competition topics and enterprise project cases to restructure course content and teaching methodologies. This approach enables students to engage in experiential learning, where they acquire knowledge and skills through active participation in practical tasks. By focusing on "learning by doing," students develop a deeper understanding of theoretical concepts and their applications in real-world scenarios. Complementing this is the competition-driven module, which establishes a structured mechanism to integrate classroom learning with competitive activities. Through a hierarchical and progressive competition system, students are motivated to enhance their learning and develop innovative thinking and practical abilities. This system not only stimulates intellectual curiosity but also prepares students for the challenges of professional environments. The integration of these two modules creates a closed-loop training system that seamlessly connects theoretical learning, practical training, and enterprise-level application [7, 12]. This interconnected approach ensures that students are equipped with the necessary skills and competencies to excel in their respective fields, bridging the gap between academic education and industry requirements. The model emphasizes collaboration among educators, students, and industry professionals, fostering a dynamic and interactive learning environment that promotes continuous improvement and innovation (As shown in Figure 2).

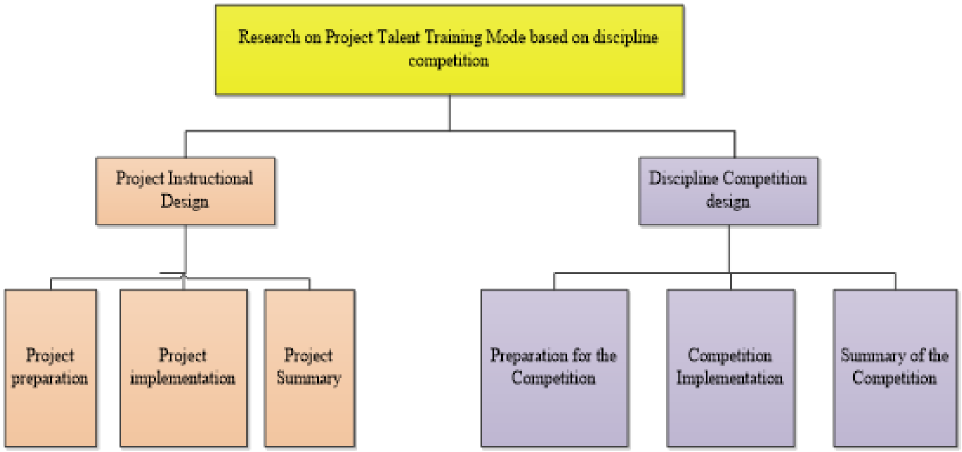

Figure 2. Project-based talent training mode

3.2. Three-level progressive training system

The three-level progressive training system, as outlined in Table 1, is structured to align with the principles of the project-based talent training mode. This system is designed to facilitate a gradual and systematic development of skills and competencies, ensuring that learners progress through clearly defined stages. Each level within the system builds upon the previous one, fostering a cumulative learning experience that integrates theoretical knowledge with practical application. By adopting this approach, the training system aims to enhance the adaptability and problem-solving abilities of participants, preparing them for complex, real-world challenges [13, 14]. Furthermore, the framework emphasizes the importance of continuous improvement and iterative learning, encouraging participants to refine their expertise over time. This structured methodology not only supports the cultivation of specialized skills but also promotes a holistic understanding of the subject matter, ensuring comprehensive professional growth.

Table 1. Core implementation contents and requirements of the three-level progressive training system

Level of training	Core of construction	Specific implementation Measures	Quantify duration/ requirements
Basic Layer (Curriculum Teaching reform)	Optimization of curriculum system, innovation of teaching methods, development of teaching resources	1. Add practical courses such as Web Security Practice and CTF Competition Special Skills; 2. Adopt the "flipped classroom + project-driven" teaching mode; 3. Jointly develop CTF practical tutorials and case bases; 4. Adjust the course sequence and construct a progressive course structure	The new courses will last from 32 to 48 hours per semester
Advanced Level (school training competition)	Practice platform construction, guidance team	1. Set up CTF simulation competition environment, and deploy platforms such as i Spring and DVWA; 2. Set up a competition guidance team of 5 to 8 school teachers and 2 to 3 enterprise	Weekly training + monthly evaluation + season

	formation, hierarchical and classified training	experts; 3. Divided into "basic group/improvement group" training, set up CTF interest clubs; 4. Establish a normalized training mechanism	competition, senior "mentoring" lower grade
Actual combat layer (school-enterprise cooperation)	Off-campus base construction, enterprise project introduction, high-end actual combat participation	1. Establish off-campus practice bases with at least 2 local network security enterprises; 2. Introduce real enterprise projects such as safety assessment of industrial control system in manufacturing industry; 3. Select outstanding students to participate in national offensive and defensive drills/network protection action; 4. Technical lectures are held regularly by enterprise experts	The cumulative duration of enterprise practice is ≥1 month

3.3. Construction mechanism of teaching staff

Table 2 illustrates the establishment of a comprehensive three-in-one mechanism designed to enhance the development of teaching staff through a combination of training, temporary employment, and incentive measures. This approach aims to address the multifaceted needs of educators by providing structured professional development opportunities, fostering adaptability through temporary assignments, and motivating performance through well-designed incentive systems. The training component focuses on equipping teachers with advanced pedagogical skills and subject-specific expertise, ensuring they remain updated with the latest educational methodologies. Temporary employment serves as a dynamic strategy to integrate diverse experiences into the teaching workforce, enabling educators to adapt to varying institutional environments and challenges. Incentives are strategically implemented to recognize and reward outstanding contributions, thereby promoting a culture of excellence and continuous improvement [15, 16]. Together, these elements form a robust framework that supports the sustainable growth and professional advancement of teaching personnel within the educational system.

Table 2. The three-in-one construction mechanism of "training + temporary employment + incentive" for teachers

Dimension of construction	Specific implementation content	Quantitative requirements	Objectives of construction
Special training promotion	1. Select teachers to participate in the special training of network security discipline competition; 2. Encourage teachers to obtain professional certifications such as CISP and CISSP; 3. Organize teachers to	2 to 3 teachers are selected each year, and the duration of competition training is ≥2 weeks	Improve teachers' double teacher quality and CTF competition

	participate in industrial technical exchanges		guidance ability
Enterprise suspended duty training	1. Establish a teacher enterprise temporary duty system, and select teachers to participate in actual projects in network security enterprises; 2. The full-time teacher completed the project practice report and shared it in the school	1 to 2 teachers are selected each semester, and the temporary tenure is ≥1 month	Make up for the lack of practical experience of teachers and update the technical reserves of the industry
Establishment of incentive mechanism	1. Set up a teacher competition guidance reward fund and give material rewards; 2. The results of the competition guidance shall be included in the additional points of the professional title evaluation; 3. Organize regular teaching seminars and share competition guidance experience; 4. Set up teaching quality awards to recognize outstanding teachers in reform	Special awards will be given to excellent instructors in provincial/national competitions	Stimulate the enthusiasm of teachers in teaching reform and competition guidance

3.4. Diversified evaluation system

Table 3 outlines the index and proportion of the diversified evaluation system for the cyberspace security specialty. This system is designed to comprehensively assess various aspects of student performance and program effectiveness [17]. It incorporates multiple dimensions to ensure a holistic evaluation of both theoretical knowledge and practical skills. By integrating diverse evaluation criteria, the system aims to foster a balanced development of technical expertise, teamwork, and innovative thinking among students.

Table 3. Diversified evaluation system index and proportion of cyberspace security specialty

Object of evaluation	Evaluation dimension	Proportion of indicators	Evaluation subject	Purpose of evaluation
Student	Competition results (CTF problem solving, attack and defense performance)	40%	Teacher, enterprise mentor	Assess the ability of actual combat operation and competition response
	Coursework (Mastery of	20%	Teacher	Assessment of basic theoretical knowledge reserve

	theoretical knowledge)			
	Group project report (scheme design, document writing)	20%	Teacher, enterprise mentor	Assessment of engineering practice and documentation ability
	Usual classroom performance (teamwork, innovation ability)	20%	Teacher, classmate	Assessment of comprehensive literacy and classroom participation
Teacher	Student evaluation	—	Student of course selection	Assessment of classroom teaching effect and student recognition
	Peer evaluation	—	Professional teachers on campus	Examine the rationality of teaching methods and curriculum design
	Enterprise feedback	—	Cooperative Enterprise Mentor	Assess the matching degree of practical teaching and industrial demand

1. Student evaluation reform has introduced a multifaceted assessment framework. This framework allocates 40% of the evaluation to competition results, which include problem-solving abilities in Capture the Flag (CTF) challenges and performance in attack and defense scenarios. Another 20% is based on course assignments, emphasizing the mastery of theoretical knowledge. Group project reports, which account for 20%, focus on engineering document writing and scheme design, while the remaining 20% evaluates classroom performance, highlighting teamwork and innovation skills. To ensure a comprehensive understanding of student progress, learning files are established to document their growth trajectory. These files capture their achievements in course learning, project practices, competition participation, and other relevant activities, providing a detailed record of their academic and practical development.
2. Teachers' teaching evaluation is conducted through a comprehensive mechanism that integrates feedback from students, peers, and enterprises. This evaluation process is carried out at the end of each semester to assess teaching quality. The results are directly linked to performance metrics, ensuring accountability and encouraging continuous improvement. To further motivate educators, a teaching quality award has been established to recognize outstanding contributions to project-based teaching reform. This initiative not only incentivizes excellence but also fosters a culture of innovation and dedication among teaching staff (As shown in Figure 3).

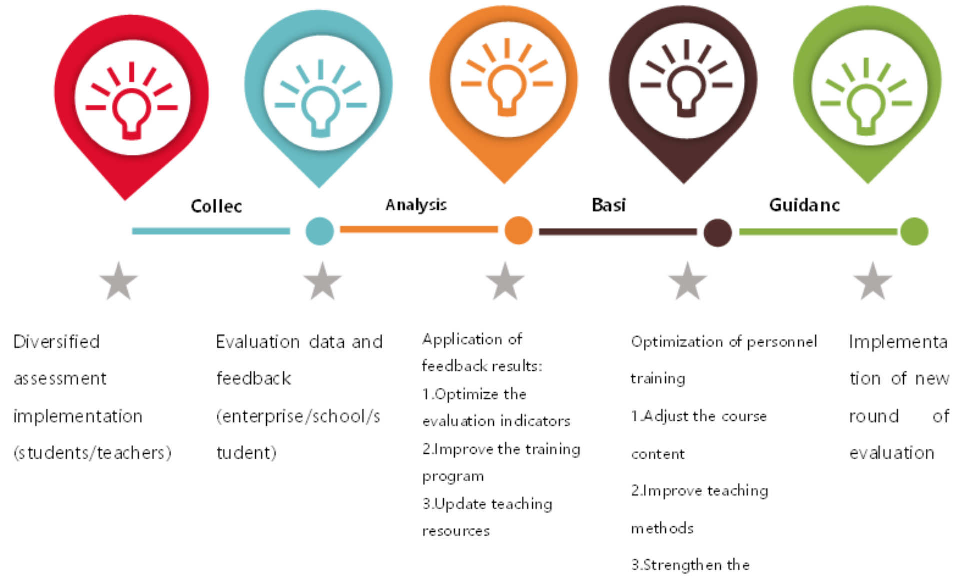

Figure 3. Feedback mechanism for teaching evaluation

A feedback and improvement mechanism has been established to ensure the continuous enhancement of the training program. Regular feedback is collected from enterprises regarding the capabilities of graduates, enabling timely adjustments to the talent training program and course content. Additionally, follow-up surveys of graduates are conducted to evaluate the long-term effectiveness of the training model. This approach creates a closed-loop system of continuous improvement, ensuring that the program remains aligned with industry needs and effectively prepares students for professional challenges.

4. Practice results and discussion

4.1. Implementation Effect

This study focuses on the students enrolled in the cyberspace security program at Guangdong University of Science and Technology, specifically those from the 2023 and 2024 academic cohorts [12]. The teaching reform practice implemented within this program has yielded significant and measurable outcomes. These results are reflected in various aspects, including the enhancement of students' core competencies and their overall competitiveness in the employment market. Furthermore, the reform has contributed to notable achievements in academic and professional domains, such as improved performance in discipline-specific competitions and advancements in teaching research practices. The data presented in Table 4 and Table 5 provide a detailed statistical analysis of these improvements, showcasing the effectiveness of the reform measures in fostering both academic excellence and practical skills among the students. By aligning the curriculum with industry demands and emphasizing hands-on learning experiences, the reform has successfully bridged the gap between theoretical knowledge and practical application, ensuring that graduates are well-prepared to meet the challenges of the rapidly evolving cyberspace security field.

Table 4. Statistics of improving students' core competence and employment competitiveness after the implementation of teaching reform

Improving metrics	Concrete results	Compared with the previous level of improvement
Core course results	The average scores of core courses such as Network attack and Defense Technology and Cryptography have been significantly improved	15%
Tool operation capability	The proportion of students who are proficient in more than 3 network security tools such as Wireshark and Nmap	80% or higher
Local employment ratio	The proportion of graduates employed in network security enterprises in Dongguan	18%
The proportion of graduates employed in network security enterprises in Dongguan	The proportion of students who have obtained at least one vocational qualification certificate such as CISP and NISP before graduation	60%
Graduate starting salary	The average starting salary of graduates majoring in cyberspace security	22%

Table 5. Statistics of the results of discipline competition and teaching research practice

Type of results	Specific Results	Quantity/award level
Winning the discipline competition	Award of cyberspace security competition above provincial level	A total of 8 awards (1 first prize and 2 second prize in Guangdong Province competition, 2 third prize in South China Division of National Competition)
The actual combat drill won the prize	Dongguan city "Dongguan shield" network security attack and defense drill	Honorary title of Excellence
Teaching Research Papers	Network security personnel training, project-based teaching related teaching research papers	Published 3 articles
Teacher Teaching Competition	University-level teaching competition	Two second prize winners

Competition Director Honor	School-level excellent competition instructor	1 person
Construction of Teaching Resources	CTF competition question bank development	More than 100 lanes

4.2. Innovation and Characteristics

1. The optimization of the curriculum system through industry-education integration involves conducting thorough research on regional industrial demands. This process aims to accurately identify the relationship between the core skills required for Capture the Flag (CTF) competitions and the capabilities needed for enterprise roles. By establishing a progressive curriculum system that transitions from foundational knowledge to specialized skills and practical combat scenarios, the teaching content is seamlessly aligned with industrial requirements. This approach ensures that students are equipped with relevant skills that directly correspond to the needs of the workforce, fostering a more effective and targeted educational experience.
2. The practical teaching model emphasizes collaboration between schools and enterprises, innovating a dual-scene training pathway that combines campus-based simulations with real-world enterprise scenarios. On-campus training utilizes the CTF platform to provide consistent and structured practice, while school-enterprise partnerships introduce advanced practical experiences, such as working on real projects and participating in network protection activities. This dual approach addresses the gap between theoretical teaching and real-world applications, ensuring that students gain hands-on experience in environments that closely mirror professional settings. By bridging this disconnect, the model enhances the relevance and effectiveness of practical teaching methods.
3. The innovation of a multi-subject evaluation system introduces a comprehensive mechanism for assessing both students and teachers. For students, the evaluation incorporates competition outcomes, project results, and performance throughout the learning process, providing a holistic view of their capabilities. For teachers, the system integrates feedback from students, peers, and enterprise collaborators to assess teaching quality. This multi-dimensional evaluation framework encourages active participation in practical teaching by both students and educators, fostering a culture of continuous improvement and collaboration. The system's design ensures that all stakeholders are motivated to contribute to the enhancement of educational practices.

4.3. Limitations and Prospects

This study acknowledges several limitations that need to be addressed. Firstly, the model demands high levels of expertise from educators and requires advanced hardware environments, which may pose challenges for some institutions attempting to replicate it. Secondly, managing personalized guidance and risk control for large-scale student participation remains an area requiring further exploration. Lastly, the quantitative indicators and the reliability and validity of the evaluation system need refinement to ensure robust and accurate assessments. Addressing these limitations will be crucial for the broader adoption and effectiveness of the proposed model.

Future research will focus on several key directions to enhance the current framework. One priority is the development of an intelligent evaluation system for assessing CTF competition abilities, utilizing knowledge graphs to create precise profiles of students' skills and recommend personalized learning pathways [3]. Another area of exploration is the integration of artificial intelligence tools into cybersecurity training, combining AI with security education to create innovative training methodologies. Additionally, efforts will be made to deepen collaborations with security enterprises in the Guangdong-Hong Kong-Macao Greater Bay Area, aiming to establish a regional alliance for cybersecurity talent development. These advancements are expected to significantly improve the effectiveness and scalability of the model.

5. Conclusions

In light of the challenges associated with cultivating cyberspace security talent in applied undergraduate colleges and universities, this study introduces a project-based talent training model centered on subject competition. The proposed framework establishes a three-tier progressive system encompassing curriculum teaching reform, on-campus training competitions, and school-enterprise cooperative practices, thereby fostering a deep integration of production and education. This approach has demonstrated its effectiveness in enhancing students' professional skills, fostering innovative thinking, and boosting their employment competitiveness. Furthermore, it provides a practical pathway for local colleges and universities to develop high-quality network security professionals aligned with industry demands. Beyond immediate benefits, this model holds broader implications for similar application-oriented institutions, offering a replicable strategy to address the growing need for skilled cybersecurity experts. By bridging the gap between academic training and industry requirements, the framework contributes to the sustainable development of regional network security industries. Future research could explore the scalability of this model across diverse educational contexts and investigate its long-term impact on workforce readiness and industry innovation. Additionally, refining the integration mechanisms between academic institutions and enterprises may further enhance the effectiveness of this approach, ensuring that it remains adaptable to evolving technological and market trends.

Funding: This work was supported by the Quality Engineering Project of Guangdong University of Science and Technology under Grant Nos. GKZLGC2025043 and GKZLGC2025028.

References

1. X. Chen, F. Ruan, L. Zhang, and Y. Zhao, "Design of cyberspace security talents training system based on knowledge graph," *International Journal of Digital Crime and Forensics (IJDCF*, vol. 12, no. 4, pp. 44-53, 2020.
2. G. Zhao, J. Wang, H. Liu, and J. Li, "Exploration of the Collaborative Education Model for Cyberspace Security Talents in the Context of New Engineering Based on Unity of Knowledge and Action."
3. J. Sui, Z. Hua, H. Zhu, and S. Shen, "Training mechanism of engineering education and innovation talent based on courses-competitions combination," *Nanotechnology for Environmental Engineering*, vol. 7, no. 3, pp. 833-841, 2022.
4. G. Chen, X. Li, X. Zhang, and G. Reniers, "Developing a talent training model related to chemical process safety based on interdisciplinary education in China," *Education for Chemical Engineers*, vol. 34, pp. 115-126, 2021.
5. A. Y. Lebid and N. Y. A. Shevchenko, "Cultivation of the skills of design thinking via the project-based method as a component of the dual model of learning," 2020.
6. W. Yang, X. Ma, R. Lian, and W. Zhang, "Research on the Optimization of the Three-In-One Talent Training Mode of Learning-Research-Application: Based on AI Technology," 2025.
7. G. Xu and C. Zhao, "Evaluation system and application of classroom teaching reform of Bridge Engineering based on classroom simulation subject competition learning," *Innovation*, vol. 7, no. 2, pp. 17-21, 2023.
8. G. Zhao, J. Wang, B. Fu, and Y. Yao, "Exploration of the Ideological and Political Construction Model for Cyberspace Security Talents in the Context of New Engineering Based on Unity of Knowledge and Action."
9. J. Vićić, "The other means? Examining the patterns and dynamics of state competition in cyberspace," Ph.D. dissertation, University of Cincinnati, 2021.
10. F. C. Domingo, "Conquering a new domain: Explaining great power competition in cyberspace," *Comparative Strategy*, vol. 35, no. 2, pp. 154-168, 2016.
11. M. Dunn Cavelty and A. Wenger, "Cyber security meets security politics: Complex technology, fragmented politics, and networked science," *Contemporary Security Policy*, vol. 41, no. 1, pp. 5-32, 2020.
12. H. I. Langø, "Competing academic approaches to cyber security," in *Conflict in Cyber Space*, Routledge, pp. 7-26, 2016.
13. A. Conklin, "Cyber defense competitions and information security education: An active learning solution for a capstone course," in *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06)*, vol. 9, pp. 220b-220b, Jan. 2006.

14. J. Collier, "Cyber security assemblages: A framework for understanding the dynamic and contested nature of security provision," *Politics and Governance*, vol. 6, no. 2, pp. 13-21, 2018.
15. A. B. Woszczynski and A. Green, "Learning outcomes for cyber defense competitions," *Journal of Information Systems Education*, vol. 28, no. 1, pp. 21, 2017.
16. B. J. Nakayama, "Information vs the cyberspace domain," *Journal of Cyber Policy*, vol. 7, no. 2, pp. 213-229, 2022.
17. H. Ning, Y. Lin, W. Wang, H. Wang, F. Shi, X. Zhang, and M. Daneshmand, "Cyberology: Cyber–physical–social-thinking spaces-based discipline and interdiscipline hierarchy for metaverse (general cyberspace)," *IEEE Internet of Things Journal*, vol. 10, no. 5, pp. 4420-4430, 2022.