Educational Research and Human Development
Print ISSN: 3007-6935
Online ISSN: 3007-6943
DOI: https://doi.org/10.61784/erhd3060

COMPETITION PRACTICE AND RESEARCH OF PROMOTING TEACHING BY COMPETITION: TAKE THE COURSE OF INFORMATION SYSTEM AND SECURITY COUNTERMEASURES TECHNOLOGY FOR AN EXAMPLE

Ling Zhao*, HongXia Hou, Shen Li, Rui Ma
School of Cyberspace Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, Shaanxi, China.
**Corresponding Author: Ling Zhao*

Abstract: With the explosive growth of talent demand in the field of cybersecurity, the traditional training model of "emphasizing theory over practice" in information security courses is no longer suitable for the core requirements of the industry for practical talents. Using the course "Information System and Security Countermeasures Technology" as a vehicle, this paper systematically analyze common pain points in current teaching practices, such as the disconnection between theory and practice, insufficient hands-on capabilities of students, and a monolithic evaluation system. It establishes a comprehensive teaching reform system that integrates "competition-driven teaching" and "competition-integrated education". After implementation across three student cohorts, the reform has significantly enhanced students' competition-winning rates, practical cyber defense capabilities, and teamwork skills. The research results demonstrate that the "competition-driven teaching" model can achieve a virtuous cycle of "teaching-competition-research-industry," providing theoretical reference for teaching reforms in network space security courses.
Keywords: Promoting teaching by competition; Integration of competition and teaching; Information Systems and Security Countermeasures Technology; Teaching reform; Cultivation of practical talents

1 INTRODUCTION

As the rapid development of the digital economy, cybersecurity has become a core area related to national sovereignty, economic development, and social stability. The state has clearly proposed to accelerate the cultivation of professional talents in cyberspace security and establish a talent evaluation system with practical ability as the core [1,2]. As a core course of the cyberspace security major, "Information Systems and Security Countermeasures Technology" undertakes the core task of cultivating students' mastery of system attack and defense principles, practical penetration ability and security protection thinking, and is a key link between theoretical knowledge and industrial practice. Traditional teaching of the "Information Systems and Security Countermeasures Technology" course has long suffered from three core pain points: First, the teaching content lags behind technological development, with many attack and defense technology cases still at the level of outdated vulnerabilities from ten years ago; second, the practical sessions are fragmented, with experiments mostly being verification operations, making it difficult for students to develop systematic practical thinking; and third, the evaluation system is singular, with the final grade still mainly based on written theoretical scores, failing to accurately measure students' practical attack and defense capabilities.

In recent years, many majors have begun to explore reform paths that integrate competition resources into daily teaching, but most practices still remain at the level of "selecting a few top students to participate," failing to cover all students and making it difficult to achieve the goal of using competitions to leverage the overall improvement of teaching quality. This article, based on years of teaching experience in cybersecurity, fully embeds the practical standards of cybersecurity competitions into the entire teaching process of the "Information Systems and Security Countermeasures Technology" course, constructing a complete reform system covering curriculum standard reconstruction, practical platform upgrades, teacher capacity enhancement, and evaluation system optimization. It explores a new talent training model of "teaching through competition" for all students, providing practical reference for the teaching reform of cybersecurity courses.

2 DEFINITION AND CORE LOGIC OF "PROMOTING TEACHING BY COMPETITION" REFORM

2.1 Definition

"Promoting Teaching by Competition" is not simply treating competitions as an additional part of teaching, but rather using the practical ability standards of competitions as the core anchor point to reverse-engineer the teaching objectives, content system, practical links, and evaluation methods of the course, achieving a paradigm shift of "competition standards entering the classroom and full coverage of practical abilities." For courses with strong practical attributes, such as "Information Systems and Security Countermeasures Technology," its core connotation is to transform the practical requirements of real attack and defense exercises into implementable content in daily teaching, allowing all

students to encounter industry-level practical scenarios in their course learning, ultimately achieving a virtuous cycle of "using competitions to drive teaching reform, using teaching to support ability improvement, and using abilities to adapt to industry needs."

2.2 Core Logic

This reform breaks the linear logic of traditional teaching "theory preceding practice" and constructs a closed-loop logical chain of "reverse anchoring to competition benchmarks, forward integration of teaching content, and bidirectional verification of competency outcomes". Initially, it comprehensively deconstructs the assessment dimensions of various mainstream cybersecurity competitions and extracts five core ability modules: Web security, binary security, cryptography, reverse analysis, and emergency response, which are taken as the core training objectives of the course; Subsequently, it reconstructs the theoretical content and practical system of the course around the five ability modules, and transforms typical questions in the competition into teaching cases and experimental projects of the course; Ultimately, through the hierarchical and progressive path of group competitions, school-level selection competitions, regional competitions, and national competitions in the course, it verifies the effect of students' ability training, and then uses the students' ability shortcomings exposed in the competitions to update the teaching content, forming a continuous iterative teaching optimization mechanism.

3 PAIN POINT ANALYSIS OF TRADITIONAL COURSE TEACHING

This study, through questionnaires and in-depth interviews, ultimately identified four core problems during the traditional teaching model:

3.1 Severe Disconnection Between Teaching Content and Industry Practice

The survey results show that 60% of students believe that the teaching content of traditional courses is outdated. Many attack and defense cases still revolve around classic vulnerabilities from before 2018, completely failing to cover emerging technologies such as cloud-native security and large-scale security, which are currently mainstream in the industry. At the same time, the knowledge points in traditional teaching content are fragmented, lacking logical connections between various attack and defense techniques, making it difficult for students to develop a systematic attack and defense mindset after completing all chapters.

3.2 Severely Lacking in the Practical Application of the Training Component

Traditional course experiments are mostly pre-set verification operations. Students only need to follow the steps in the experiment manual to get the pre-set experimental results, with no room for independent exploration. 65% of students reported in the questionnaire that after completing all the course experiments, they were completely at a loss when they first encountered real CTF competition problems. At the same time, traditional experimental environments are mostly simplified virtual ranges, which prevent students from experiencing the confrontation in real attack and defense, and make it difficult to develop practical skills in troubleshooting and debugging scripts.

3.3 Significant Deficiency in the Practical Skills of the Teaching Staff

The iteration speed of cybersecurity attack and defense technologies is extremely fast. Many university teachers have long been engaged in theoretical research and lack practical attack and defense experience in front-line security companies. This results in classroom teaching being limited to theoretical explanations and failing to impart practical operational skills and thinking methods to students. At the same time, traditional teaching and research activities are mostly centered around theoretical teaching and lack a collective lesson-refinement mechanism for practical attack and defense, making it difficult for teachers' practical teaching abilities to be systematically improved.

3.4 The Course Evaluation System Cannot Measure True Ability

The final grade of traditional courses consists of 60% closed-book written exam and 40% daily performance. The written exam mainly focuses on memorizing attack and defense principles and vulnerability definitions, and cannot assess students' practical operational abilities. Although the daily performance includes process grades such as assignments, quizzes, and lab reports, it cannot determine whether students have truly completed the work independently. This evaluation model directly leads students to focus their energy on memorizing theoretical knowledge points, neglecting the training of practical skills, ultimately resulting in a mismatch between "high scores in written exams and low scores in practical exams."

4 CONSTRUCTION OF THE "TEACHING THROUGH COMPETITION" SYSTEM FOR TEACHING REFORM

In response to the above four core pain points, this study constructs a complete "Promoting Teaching by Competition" system from four dimensions: curriculum standards, practical platforms, teacher training, and evaluation system [3,4].

4.1 Reconstructing the Curriculum Standard System of the Three Alignments

Using the assessment standards of cybersecurity competitions as the core anchor, the Curriculum Standard System of the three alignments is established to achieve full alignment between competition requirements and curriculum training objectives:

First, the competition content is fully aligned with the core professional knowledge points. All the problems from the National Undergraduate Information Security Competition, the National CTF League and other mainstream competitions in the past five years have been fully broken down and classified into five major modules: Web security, binary security, cryptography, reverse analysis and incident response. The core knowledge points corresponding to each module have been extracted and incorporated into the theoretical teaching syllabus of the course.

Second, the competition assessment points are fully aligned with the core professional competencies. The practical ability requirements for contestants in the competition are transformed into the competency training objectives of the course, clearly requiring students not only to master the theoretical principles of vulnerabilities, but also to be able to independently complete the entire process of vulnerability reproduction, exploitation, and protection.

Third, the overall competition standards are fully aligned with the talent training standards. The comprehensive ability requirements of cybersecurity competitions are fully integrated into the overall training objectives of the course. In addition to attack and defense technical skills, students' innovative thinking on vulnerabilities, teamwork skills, and resilience under pressure during attack and defense confrontations are simultaneously cultivated.

4.2 Building a Layered and Progressive Practical Teaching Platform

Around the course's ability training objectives, a three-tiered progressive practical teaching platform is built: "Basic Verification - Comprehensive Confrontation - Industry Practice":

The first layer is a basic verification experimental platform. Based on an open-source target range system, a dedicated basic experimental environment is built for the course, transforming the knowledge points of each chapter into corresponding small experimental target machines. The platform has built-in detailed operation guidance and error prompt mechanisms, allowing students to independently troubleshoot problems when encountering operational obstacles and gradually develop the habit of independently debugging attack and defense scripts [5,6].

Second, a comprehensive adversarial competition platform. Deploy a CTF competition platform supporting real-time multiplayer competition. After each teaching unit, organize a one-hour small-class competition to allow students to complete attack and defense tasks in a timed environment, simulating the tense atmosphere of a real competition.

The third layer is an industry practice-oriented training platform. In cooperation with local cybersecurity companies, real-world attack and defense exercise scenarios are introduced, building complex network target ranges including cloud servers and IoT devices, transforming real-world emergency response and penetration testing projects into comprehensive training content for the course.

Simultaneously, relying on the platform, a student self-training mechanism is established, opening the platform to all students 24 hours a day, uploading a large number of competition questions, operation tutorials, and problem-solving strategies. Students can choose training questions according to their own ability level to achieve personalized ability improvement.

4.3 Innovating a "Three-Dimensional Collaborative" Teacher Training Mechanism

To address the pain point of insufficient practical skills among teachers, a three-dimensional collaborative teacher training system of "in-school lesson refinement - enterprise practice - competition experience" is established to comprehensively improve teachers' practical teaching abilities [7]:

First, The "Attack and Defense Teaching and Research Community" is established within the school. A teaching and research team composed of course leaders, backbone teachers, and outstanding participating students is formed to conduct a "one lesson, multiple refinements" teaching and research activity once a week, collectively discussing the latest technologies in competitions and operational skills in practice, and jointly refining the teaching cases and experimental projects of the course.

Second, a teacher enterprise practical training rotation system is established. Partnerships have been established with leading local cybersecurity companies, requiring course instructors to undergo at least three months of full-time practical training in the companies' attack and defense technology departments every two years to accumulate front-line practical experience.

Third, support teachers in improving their capabilities through competitions. Teachers are encouraged to participate in various cybersecurity competitions, experiencing the competition's question logic and ability requirements as contestants, and addressing their shortcomings in practical skills during the competition process.

4.4 Establishing a Process Evaluation System Covering the Entire Cycle

Completely break away from the traditional "one exam determines the grade" evaluation model and establish a process-oriented evaluation system covering the entire learning cycle of the course [8,9]. The final course grade consists of four parts:

1) Daily training grades (30%): Scoring is based on students' daily experimental operation data recorded on the practical platform, directly quantifying the time students spend completing experiments, the completeness of operational steps, and the degree of independent exploration.
2) Class Competition Score (30%): The cumulative score of the four small-unit competitions organized during the course, fully simulating the scoring rules of CTF competitions, and ranking and scoring students based on their answer scores.
3) Final Comprehensive Attack and Defense Drill Score (30%): The final exam will no longer be a closed-book written exam, but will directly use the scores of the Xi'an University CTF Regional League internal selection competition as the scoring basis for this part.
4) Innovation and Expansion Achievements (10%): Additional bonus points are set up. Students can receive corresponding bonus points for their self-discovered real campus vulnerabilities, practical experience in participating in local enterprise security projects, and awards in provincial or higher-level cybersecurity competitions.

5 PRACTICAL EFFECTS AND DATA ANALYSIS OF TEACHING REFORM

This round of teaching reform has been implemented for three consecutive sessions in our school's Information Countermeasures Technology major, covering 210 students. Through multi-dimensional data comparison, the actual effectiveness of the reform has been verified.

5.1 Significantly Improved in Students' Practical Ability

Compared with the data of the three cohorts of students before the reform, the average course score of students after the reform increased from 72.3 points to 78.7 points, and the excellent rate of 90 points or above increased from 11.2% to 27.5%. More importantly, students' practical attack and defense capabilities have achieved a leapfrog growth: before the reform, less than 15% of students were able to independently complete a complete Web penetration test chain after the course ended, while after the reform, this proportion increased to 42.4%.

5.2 Explosive Growth in Competition Awards

Before the implementation of the reform, students in our school's Information Countermeasures Technology major won fewer than 10 awards in provincial or higher-level cybersecurity competitions each year, mainly third prizes. Since the implementation of the reform three years ago, students have won a total of 17 national-level awards in the National College Student Information Security Competition, 12 first prizes and 23 second prizes in provincial cybersecurity competitions, and the total number of competition awards has increased by 187% compared with before the reform. More importantly, the scope of participating students has been greatly expanded. Before the reform, only a small number of top students were selected to participate. After the reform, more than 60% of the students taking the course have participated in at least one school-level or higher cybersecurity competition, truly achieving the goal of full competition coverage.

5.3 Significantly Improved Industry Adaptability

According to employment data statistics from the past three years, the employment rate of graduates in the cybersecurity field has increased from 38% before the reform to 60%. A large number of students have joined the attack and defense technology departments of leading domestic cybersecurity companies, with more than 50% of graduates choosing to stay and work for local security companies in Xi'an. Feedback data from companies shows that the practical learning cycle for our graduates has been shortened from the traditional 3-6 months to less than 1 month. Students are highly familiar with the security scenarios of local universities and manufacturing companies in Xi'an and can directly start working on projects without additional local scenario training. The ability to exploit vulnerabilities and respond to emergencies has been highly praised by the technical leaders of the enterprise.

5.4 Comprehensively Enhanced in Students' Learning Initiative

According to a questionnaire survey, 91% of students believed that the "teaching through competition" model significantly increased their interest in the course, and 87% of students indicated that they would proactively log in to the practical platform for attack and defense training after class. Students' learning mode has shifted from the traditional "teacher tells me to learn" to "I want to practice proactively". A large number of students spontaneously formed attack and defense interest groups after the end of the course, participating in various online attack and defense drills in their spare time. Based on the local competition ecology built by the course, a strong atmosphere of practical learning was formed among students.

6 CONCLUSIONS

This article takes the course of "Information Systems and Security Countermeasure Technology" as the carrier to explore the construction of a teaching reform system of "promoting teaching through competition and integrating

competition and teaching". After three years of practical verification, it effectively solves the core pain point of traditional network security courses that "emphasize theory over practice", achieves comprehensive improvement of students' practical ability, competition results, and industry adaptability, and provides a replicable practical paradigm for the teaching reform of engineering courses with strong practical attributes.

In the future, we will further deepen the depth of reform: firstly, introduce large model AI teaching assistants to empower practical teaching, accurately locate students' ability shortcomings based on their operational data, and provide personalized practical training guidance for students; The second is to further deepen cooperation with cybersecurity enterprises, transform more real attack and defense projects of enterprises into teaching content of courses, and achieve seamless integration between course teaching and industry practical experience; The third is to promote the model of "promoting education through competition" to other core courses in the field of cybersecurity, and build a talent cultivation ecosystem that integrates competition and education covering the entire profession, in order to cultivate more high-quality practical cybersecurity talents for the country.

COMPETING INTERESTS

The authors have no relevant financial or non-financial interests to disclose.

FUNDING

Xi'an University of Posts and Telecommunications 2025 School-level Teaching Reform Research Project "Competition Practice and Research of Promoting Teaching by Competition - Taking the Course of Information Systems and Security Countermeasures Technology as an Example" (Project No.: JGA202520).

REFERENCES

[1] Wang J. Exploration and practice of training network security practical talents. Computer Education, 2024(7): 123-127.

[2] Wei Y X, Zhao Y X, Jiang J S. Innovative Practices and Optimization of the Integration Mode of Competition-Education in Local Application-Oriented Universities. Research and Practice on Innovation and Entrepreneurship Theory, 2025, 8(21): 47-49

[3] Liu H F. Integrating education with competitions: Construction and practice of teaching innovation system of "promoting teaching with competitions" in colleges and universities. Journal of Higher Education Research, 2025, 48(2): 78-83.

[4] Zhang X L. Exploration of Innovative Thinking Training Course Construction and Teaching Mode from the Perspective of "Integration of Competition and Teaching" . Science and Education Culture, 2026, (5): 81-84.

[5] Zhang Y. Research on teaching reform of information security course based on CTF competition. Cyberspace Security, 2023, 14(11): 98-102.

[6] Liu L. Research on Teaching of "Cybersecurity and Management" Course Driven by "Four-Dimensional Integration" of Competition-Education Integration. Computer Knowledge and Technology, 2025, 21 (25): 146-148.

[7] Zhao L. Construction of network attack and defense practice teaching system in virtual range environment. Experimental Technology and Management, 2025, 42(1): 212-216.

[8] Chen Z L. Exploration of Teaching Innovation in Experimental Courses of Analog Electronic Technology under the Perspective of Competition-Education Integration. Scientific and Educational Journal, 2025, (24): 38-40.

[9] Li N. The Construction of the Talent Cultivation Model of "Promoting Education through Competitions" under the Background of New Engineering. Higher Engineering Education Research, 2024(3): 156-160.