Exploration and Practice of a Research-Driven Teaching Model for Cyberspace Security Majors in Engineering Universities

Gonghao Duan*
School of Computer Science and Engineering, Wuhan Institute of Technology, Wuhan, Hubei, China
**Corresponding Author*

Abstract: China faces a shortage of over 3.2 million cybersecurity professionals, with a supply rate of less than 15% possessing both research experience and practical skills. However, cybersecurity education in engineering universities suffers from a disconnect between theory and cutting-edge technologies, and limited practical scenarios. This research focuses on addressing these challenges and leveraging these advantages. Its goal is to establish a comprehensive, integrated research model covering the entire freshman to senior year of university, adapting to the dynamic offensive and defensive nature of cybersecurity. The "focus" approach involves integrating individual research projects with individual courses, while the "comprehensive" approach involves integrating the entire curriculum with research resources. The research utilizes a literature analysis and case study methodology. Core achievements include: first, a phased system of "freshman enlightenment - sophomore integration - junior year practical application - senior year innovation," which reduces the research threshold by 80%; second, a three-dimensional mechanism of "laboratory openness - school-enterprise collaboration - faculty collaboration"; and third, a five-dimensional evaluation system of "student ability - teaching quality - research application - employment competitiveness + practical contribution." This model has proven effective: the winning rate of student CTF competitions has increased by 45%, the rate of matching employment has increased by 35%, the proportion of students employed by leading companies has increased by 22%, and the job adaptation period has been shortened to 1-2 months. Student research findings have been fed back into the course case library, with over 150 materials updated, forming a closed "research-teaching" loop and providing a replicable solution for cultivating cybersecurity professionals in engineering universities.

Keywords: Universities; Cyberspace Security; Scientific Research Feedback; Practice

1. Introduction

1.1 Background

The implementation of laws like China's Cybersecurity Law and Data Security Law has propelled the field into a phase of "legalization and systematization," driving surging demand for "practical and innovative" talent. According to the China Cybersecurity Talent Development White Paper (2024), the talent shortage now exceeds 3.2 million, with fewer than 15% of professionals possessing both "research project experience and practical attack-defense capabilities." This critical gap—defined as the difference between market demand and qualified supply—highlights a severe shortage of suitable talent, further underscored by the low qualified supply rate. The figures from the white paper translate to the following:

$$Talent\ Gap = 3200000 - (3200000 \times 0.15) = 2720000 \quad (1)$$

$$Qualified\ Supply\ Rate = (480000 / 3200000) \times 100\% \approx 15\% \quad (2)$$

This quantification underscores the urgent need for educational models that can effectively increase the output of qualified professionals. This talent gap is particularly prominent in emerging fields such as industrial control system (ICS) security, AI-driven attack and defense, and quantum communication security[1-3]. However, cybersecurity education in engineering universities still faces two core challenges. First, a significant gap exists between theoretical curricula and rapidly evolving technologies. While the cybersecurity field evolves every 3–6

months (e.g., with new AI-powered attack tools and ransomware variants), course materials often lag by 6–12 months. For instance, research on AI-generated content security testing takes nearly a year to be integrated into courses like "Artificial Intelligence Security," leaving graduates underprepared for current industry demands.

Second, practical training remains limited and often disconnected from real-world contexts. Most programs rely on simulated lab environments—such as DVWA and Metasploitable—which lack the complexity of real systems (e.g., multi-device coordination and dynamic defense). A Beihang University study on ICS security revealed that students trained only in virtual labs were 62% less efficient at identifying vulnerabilities in real industrial systems than those with research project experience. These issues stem from a fundamental misalignment between traditional teaching models and the fast-paced, offensive-defensive nature of cybersecurity. It is urgent to build a training path that is closer to the forefront of technology and practical needs [4]. Engineering colleges' cybersecurity research resources offer inherent advantages in addressing teaching challenges, reflected in three key dimensions:

First, high-level research platforms provide practical support. Most engineering universities operate key cybersecurity labs (e.g., national and provincial-level laboratories) equipped with specialized facilities such as vulnerability reproduction platforms, ICS testbeds, and live-fire cyber ranges. For example, Guangdong Polytechnic Normal University's Intellectual Property Big Data Key Laboratory offers low-threshold courses like "Vulnerability Data Annotation" and "Attack Traffic Classification," enabling over 200 undergraduates annually to engage in introductory research. Similarly, Beihang University utilizes experimental setups—including Siemens PLCs and Schneider SCADA systems—from a national key R&D project in its "Network Attack and Defense" course, achieving seamless reuse of research equipment for teaching.

Secondly, research projects provide rich teaching material. Engineering universities undertake numerous vertical (e.g., National Key R&D Programs) and horizontal (e.g., corporate vulnerability assessments) cybersecurity projects. These cover core areas like vulnerability mining, emergency response, and AI security, and can be directly translated into course content. For instance, from a corporate project on "AI-generated content security detection," Beijing University of Posts and Telecommunications derived 18 Python practice cases—including model backdoor detection and adversarial sample generation—effectively enriching the "AI Security Practice" course. Qi'anxin cooperated with several engineering colleges in the horizontal project of "Enterprise Web Vulnerability Inspection", which was disassembled into a practical assignment for the "Web Penetration Testing" course, allowing students to directly contact the real vulnerability scenarios of enterprises[5]. Third, university-industry collaboration enhances resource integration. Engineering universities often partner with leading cybersecurity firms—such as Qi'anxin, Venusstar, and Huawei—to establish joint R&D centers, creating a closed loop from "industry needs to research to teaching." For example, Beijing University of Posts and Telecommunications co-published the textbook AI Security: Principles and Practices with 28 real research-based programming cases, now adopted by many universities. Similarly, Guangdong University of Technology introduced a "dual-supervisor system" where corporate experts and faculty co-guide students, boosting the practical outcome conversion rate by 37% compared to traditional models. If these scientific research resources can be effectively transformed into teaching resources, they can fundamentally solve the problem of "theoretical lag and single scenario" and provide solid support for the innovation of network security professional teaching[6]. "Research feeding into teaching" entails systematic integration of university research capabilities with cybersecurity education needs, moving beyond simple content inclusion to address core teaching challenges and maximize research value.

It replaces simulated exercises with real-world projects—like red/blue team operations and emergency response—enabling problem-based learning. For instance, a "three-tier practical system" at Guangdong Polytechnic Normal University raised CTF win rates by 45%, demonstrating how authentic scenarios improve operational skills.

This approach also shifts focus from knowledge transmission to competency development, fostering scientific problem-solving through

tasks like vulnerability verification and tool building. Students progress from understanding principles to tool application and innovation, aligning with engineering education's dual emphasis on practice and research. Thus, research-fed teaching is essential for producing qualified cybersecurity professionals.

1.2 Research Status

Leading universities integrate cybersecurity research into teaching via industry collaboration and practical resource use. Purdue's lab partners with firms like Intel and Microsoft to turn real projects (e.g., ICS vulnerability detection) into course tasks. A tiered participation system engages all levels: freshmen annotate data, sophomores screen vulnerabilities, and seniors develop exploits. Scenarios like simulated ransomware attacks are updated quarterly. Student-built tools are adopted by companies, closing the research-teaching-industry loop.

Imperial College incorporates topics like quantum security into courses, embedding research such as post-quantum cryptography optimization into labs where students use quantum key distribution devices. Real cases from GCHQ enhance incident response training, with simulations like large-scale DDoS drills.

Key insights:

Tiered tasks enable full-cycle skill development;

Deep industry collaboration in content and evaluation;

Focus on emerging fields like AI and quantum security.

These experiences provide important references for domestic research, but foreign models need to be adapted to local conditions based on the characteristics of scientific research resources and the demand for cybersecurity talents in China's engineering colleges [7].

Based on the current research status, there are still two core gaps in the current research on "research feedback teaching" in the cyberspace security major of engineering colleges: First, there is a lack of a systematic feedback system covering the entire training cycle. Existing research is mostly "single-point breakthrough" (such as single course, single grade), and has not formed a full-process design of "freshman enlightenment - sophomore integration - junior practice - senior innovation", resulting in limited coverage of scientific research feedback and inability to continuously support students' ability growth; at the same time, task design does not fully consider the ability differences of students in different grades, and the problems of high participation thresholds for lower grades and insufficient practical depth for higher grades are prominent[8, 9]. Secondly, existing models lack a feedback mechanism aligned with the distinctive features of cybersecurity—such as its dynamic attack-defense nature, rapid iteration, and strong practical emphasis. As a result, educational content often lags behind the research frontier, and practical training fails to adequately cover core domains like red-blue team exercises and emergency response. This gap leaves graduates poorly prepared for real-world industry demands.

The core objective of this study is to construct a research-driven teaching model that spans the entire undergraduate journey and is tailored to the characteristics of cybersecurity education. Through phased system design and multi-dimensional resource integration, it aims to resolve the disconnects between theory and cutting-edge technology, between training and real needs, and between research and teaching—offering a practical solution for cultivating high-quality talent in cybersecurity.

2. Theoretical Basis

2.1 Core Content

The CDIO framework (Conceive–Design–Implement–Operate) emphasizes full lifecycle engineering practice, integrating theory with real-world contexts to develop systematic thinking and practical skills. Cybersecurity research—such as vulnerability discovery and defense system development—naturally aligns with CDIO's four stages, embodying its process-oriented educational philosophy.

2.2 Project-Based Learning (PBL)

Project-Based Learning (PBL) is driven by "real problems/tasks" and emphasizes that students complete challenging project tasks through independent exploration and group collaboration, building theoretical knowledge and improving practical skills in the process of problem solving. Its core is a closed-loop learning model of "task orientation - process exploration - output" [10-12]. For the "Malicious Code Analysis" course, a PBL teaching approach was designed based on the "Ransomware Family Tracing" longitudinal research project:

• Task Decomposition: The research project was

divided into three subtasks: Subtask 1: "Ransomware Sample Collection and Classification" (corresponding to the "Malicious Code Sample Acquisition" section), Subtask 2: "Sample Static Feature Extraction (e.g., PE Structure Analysis)" (corresponding to the "Static Analysis Techniques" section), and Subtask 3: "Dynamic Behavior Debugging and Family Association" (corresponding to the "Dynamic Analysis Tools" section).

• Process Guidance: Students worked in groups of three to independently review research literature (e.g., papers on virus tracing algorithms) and collaborate on the task. The teacher (research advisor) held regular "problem review meetings" to guide students in resolving technical difficulties encountered during debugging (e.g., developing anti-debugging mechanisms).

• Output: The teams submitted a "virus sample analysis report + feature extraction code." Excellent results were incorporated into the research project "Ransomware Feature Library" and reused as case studies in subsequent teaching.

2.3 Situated Cognition Theory

The theory of situated cognition emphasizes that "knowledge construction stems from interactions in real-world situations." It argues that learning cannot be separated from specific contexts. Learners must be placed in real-world environments consistent with knowledge application, and through interaction with the environment and others (such as collaboration and feedback), "contextualized cognition" is formed. Its core learning logic is "real-world scenarios - interactive practice - knowledge internalization." The core characteristics of cybersecurity, involving dynamic attack and defense, and real-time confrontation, dictate that theoretical teaching divorced from real-world scenarios cannot cultivate practical skills. The theory of situated cognition addresses this pain point[13-15].

3. Design of a “Research Feedback Teaching” Model for Cybersecurity Majors in Engineering Universities

3.1 Subtask Decomposition: Precise Connection between Scientific Research and Curriculum

Focusing on the ICS vulnerability mining "protocol analysis → tool development → vulnerability verification" technology chain, combined with the "principles → tools → practice" teaching line of "Network Attack and Defense", three experimental subtasks are disassembled in Table 1. Breakdown of experimental subtask 1.

Table 1. Breakdown of Experimental Subtask 1

Subtask number	Subtask Name	Corresponding course chapters	Core association logic
1	ICS protocol analysis and vulnerability identification	Chapter 3 "TCP/IP Protocol Vulnerabilities and Analysis"	Identifying ICS protocol (Modbus, etc.) vulnerabilities based on TCP/IP principles
2	ICS protocol fuzz testing tool development	Chapter 6 "Attack Tool Principles and Development"	Develop testing tools based on the "input mutation - monitoring" logic
3	ICS Vulnerability Verification and Exploitation Reproduction	Chapter 9 "Practical Penetration of Industrial Environments"	Simulate industrial scenarios to verify vulnerabilities and reproduce attack chains

3.2 Subtasks " Teaching - Research - Output " Three-Dimensional Correspondence

3.2.1 Subtask 1: Protocol parsing and vulnerability identification

Teaching Objectives: Master the ICS protocol (Modbus, S7comm) frame structure, be able to analyze traffic using Wireshark, and identify vulnerabilities using TCP/IP principles.

• Research Assignment: Assist in capturing real enterprise ICS traffic, classify and annotate key fields, analyze vulnerabilities against the IEC 62443 standard, and produce a preliminary report.

• Student Outputs: Annotated traffic packets, an ICS Protocol Analysis Report, and a Vulnerability List.

3.2.2 Subtask 2: Fuzz testing tool development

• Teaching Objectives: Understand fuzz testing logic, master Python socket programming, design mutation strategies for ICS protocols, and package automated tools.

• Research Assignment: Based on the vulnerabilities identified in Subtask 1, identify test areas, develop tools, and test them in a Siemens S7-1200 PLC simulation environment, documenting abnormal use cases.
• Student Outputs: Tool source code (including comments), Development Manual, and Fuzz Testing Report.

3.2.3 Subtask 3: Vulnerability Verification and Exploitation

• Teaching Objectives: Master PLC register reading and writing, and PoC writing techniques, enabling students to simulate industrial scenarios and design exploitation plans to mitigate destructive risks.
• Research Assignments: Verify vulnerabilities in an authorized test environment, develop a PoC to simulate a production line shutdown, replicate the attack chain, and provide defensive recommendations.
• Student Outputs: PoC code, vulnerability verification video, and Exploit Analysis Report.

The experimental results are shown in Table 2. Experimental subtask 3 breakdown:

Table 2. Experimental Subtask 3 Breakdown

Subtasks	Core teaching objectives	Core scientific research tasks	Core student outputs
1	Master ICS protocol analysis and vulnerability identification methods	Capture/annotate ICS traffic and analyze vulnerabilities	Marking traffic packets, ICS Protocol Vulnerability List
2	Master Python Socket programming and fuzz testing logic	Development tools, testing PLC simulation environment	Tool source code, Fuzz Testing Report
3	Master ICS vulnerability exploitation and PoC writing	Verify vulnerabilities and reproduce attack chains	PoC code, Vulnerability Exploitation Analysis Report

3.3 System Design Logic

Starting from the cybersecurity professional curriculum system, we adhere to the training rhythm of "freshman enlightenment → sophomore integration → junior practice → senior innovation", take the "basic cognition - core skills - practical ability - results output" of cybersecurity as the main line of ability, rely on the deep integration of engineering scientific research resources (laboratory projects, school-enterprise projects) and teaching carriers, and realize "the whole process of scientific research feeding back to teaching"[16].

The experimental results are shown in Table 3. Network Security Course Settings

Course design incorporates core vertical project modules, such as “Detection Algorithm Optimization” from ransomware research and “Adversarial Defense” from AI security. Industry collaborations include tailored ICS protection solutions and a research-oriented thesis topic pool. The environment integrates thesis writing, research application, and enterprise solution delivery.

The experimental results are shown in Table 4. Visualization table of the entire process system

Table 3. Network Security Course Settings

grade	Knowledge Reserve	Participation threshold	Adaptation tasks	Capacity development focus
Freshman	Introduction to Network Security, Computer Networks	Can use Wireshark and basic data processing	Filter traffic, check fields, and organize documents	Build ICS security awareness and familiarize yourself with scientific research standards
Sophomore	"Python Programming" "Network Attack and Defense" first 6 chapters	Know Python basics and fuzz testing principles	Independent analysis of single-type protocols and auxiliary tool development	Strengthen programming/tool skills and connect theory and practice
Junior year	"Network Attack and Defense" full course, "Practical Penetration"	Proficient in ICS protocols and capable of independent development/penetration	Lead vulnerability analysis, independent development tools/PoC	Cultivate scientific research and practical innovation capabilities

Table 4. Visualization Table of the Entire Process System

stage	Research resources	Teaching carrier	Cybersecurity characteristic capability goals
Freshman	Vulnerability data annotation and enterprise science popularization projects	Introduction to Cybersecurity, Scientific Research Sharing Session	Basic tool usage + professional knowledge
Sophomore	Malicious code/protocol security subtasks, school-enterprise case library	Core experimental courses, research-driven experiments	Single subtask execution + scientific research logic understanding
Junior year	"Red-Blue Confrontation" project, ICS test platform	Emergency response/penetration practical courses, CTF training	Actual attack and defense + vulnerability report output
Senior year	Ransomware detection and AI security issues	Graduation project and achievement transformation	Innovative achievements (papers/tools) + job adaptation

3.4 Laboratory Resource Opening Mechanism

Focusing on the needs of cybersecurity professionals, we offer three types of specialized resources: ① Vulnerability reproduction platforms (Vulhub, Metasploitable); ② Industrial Control System (ICS) testing platforms (Siemens S7-1200 PLC, Schneider SCADA system); and ③ Red-Blue confrontation simulation environments (enterprise-level intranet topology, traffic monitoring equipment). Based on real-world enterprise needs, we offer two types of teaching resources: ① Enterprise attack and defense case studies (e.g., SQL injection emergency response for e-commerce platforms, ICS vulnerability inspections for manufacturing); and ② Horizontal project subtasks (e.g., enterprise intranet security assessments, malicious code sample analysis). The specific operational process is as follows:

• Syllabus Co-development: At the beginning of each semester, research advisors and course instructors jointly develop a "Research-Teaching Integration Syllabus" (e.g., integrating the "Ransomware Feature Extraction" research subtask into the "Malicious Code Analysis" lab);

• Joint Guidance: When students participate in research, course instructors answer theoretical questions (e.g., syntax issues in code development), while research advisors provide technical guidance (e.g., feature extraction algorithm optimization);

• Research Feedback: After mutual review, student research results (e.g., tool code, lab reports) are updated into course teaching cases (e.g., using a "student-developed ransomware detection script" as practical training material).

4. Practical Cases and Effect Analysis

4.1 Project Source

"Security Inspection of College Websites" is a longitudinal research project initiated by the Provincial Department of Education. Its core goal is to conduct security inspections on 128 official websites of 32 undergraduate colleges in the province (including key business sub-sites such as the Admissions Office and the Academic Affairs Office), focusing on checking high-risk vulnerabilities such as SQL injection, XSS, and file upload, forming a "College Website Security Risk Report" and assisting in repairs, providing technical support for network security protection of the education system.

4.2 Course matching goals

This project enhances the "Web Penetration Testing" course by:

Replacing virtual labs with real-world detection scenarios;

Developing advanced tool skills (e.g., SQLMap, Burp Suite) and report writing through subtasks;

Fostering research-oriented problem-solving and connecting theory, tools, and practice.

4.3 Implementation Process

4.3.1 Project deconstruction: precise matching of scientific research tasks and course chapters

The overall task of "University Website Security Inspection" was broken down into four subtasks corresponding to the course chapters, and the relationship between "teaching objectives - scientific research outputs" was clearly defined, as shown in the Table 5.

4.3.2 Collaboration model based on capability

Taking into account the programming

foundation and tool usage skills of the Class of 2022 (junior year), a "vulnerability type grouping + research assistant leadership" architecture is adopted:

• Grouping Logic: 8 small groups of 3-4 people will be set up, each with 1-2 members. Each group will focus on 1-2 subtasks (e.g., Groups 1-2 will be responsible for SQL injection detection, Groups 3-4 will be responsible for XSS vulnerability scanning), to avoid overlapping tasks.

• Research Assistant Configuration: One student with proficiency in tool usage and experience in CTF competitions will be selected from each group to serve as a research assistant. This person will be responsible for coordinating the division of labor within the group (e.g., "1 person will use Burp Suite for packet capture and scanning, 2 people will use SQLMap for vulnerability verification, and 3 people will record data") and liaising with the project team (to provide feedback on technical difficulties encountered during detection).

• Skill Matching: Students with weaker foundations will be prioritized for "initial vulnerability screening" (e.g., using Burp Suite for passive scanning to identify suspicious URLs), while students with stronger skills will be responsible for "in-depth vulnerability verification" (e.g., writing custom payloads to circumvent website protection rules). This ensures full participation and that the difficulty of the tasks matches their abilities.

Table 5. Task List

Subtask number	Subtask content	Corresponding to the "Web Penetration Testing" course chapter	Scientific research output requirements
1	SQL injection vulnerability detection and verification	Chapter 3 "SQL Injection Principles and Exploitation"	Output a list of SQL injection vulnerabilities for each website (including vulnerability URL, exploit payload, and risk level)
2	XSS vulnerability scanning and exploitation	Chapter 4, "Cross-Site Scripting (XSS)"	Submit XSS vulnerability verification screenshots (including stored/reflected distinctions) and exploit demonstration videos
3	File upload vulnerability detection	Chapter 5 "File Upload Vulnerability Defense and Bypass"	Record the upload path and bypass methods of vulnerable websites (such as suffix disguise, MIME type tampering)
4	Security vulnerability report writing	Chapter 8, "Web Penetration Testing Reporting Standards"	Write a single website vulnerability report (including risk analysis and repair suggestions) according to the project requirements

4.3.3 Closed-loop linkage of "classroom theory - after-class research"

The course adopts a three-phase transition model: "Theory First, Research Practice, and Review and Consolidation":

• Phase 1 (Classroom Theory): During the corresponding chapter teaching, core knowledge points are explained in conjunction with project subtasks. For example, when teaching "SQL Injection," the use of "Possible Injection Points on a University Academic Affairs Office Website" is used as an example to demonstrate the use of SQLMap parameters such as --dbs and --tables, and clarify the "Operational Specifications for Research Subtasks";

• Phase 2 (After-Class Research): Students use their after-class time (8-10 hours per week) to conduct inspections. Research assistants summarize group progress daily, and teachers solve technical problems through online Q&A groups (e.g., "How to adjust SQLMap parameters to bypass a website after enabling WAF");

• Phase 3 (Classroom Review): A "Research Review" session is held every two weeks, where each group reports on subtask progress (e.g., "Completed SQL injection testing on 15 websites, found 3 high-risk vulnerabilities") and shares solutions to typical problems (e.g., "By analyzing website source code, we found XSS vulnerabilities"). The vulnerability was caused by not filtering special characters"), and the teacher combined the course knowledge points for comments to strengthen the connection between theory and practice.

4.4 Students' "Practical Understanding" Results

4.4.1 Independently overcome technical difficulties not covered in the course and

improve problem-solving skills

While testing a university website, a team found standard SQL injection tools ineffective. By analyzing response headers (GB2312 encoding) and source code (iconv transcoding), and researching wide-byte techniques, they modified payloads with characters like %df to successfully exploit a wide-byte SQL injection flaw—a vulnerability beyond standard coursework. This experience elevated their skills from tool usage to principle-based optimization, and their solution was added to the course's case materials.

4.4.2 Scientific research results feed back into curriculum resources, forming a virtuous cycle of "teaching-scientific research"

Students in the Class of 2022 inspected 89 university websites, submitting 63 valid vulnerability reports. Twelve were adopted by the Provincial Department of Education for their clarity and actionable solutions, assisting three universities in remediation. Fifteen typical cases—such as stored XSS and file upload vulnerabilities—were curated by instructors and integrated into the "Web Penetration Testing" course lab materials. This transition of students from learners to resource co-creators validates the effectiveness of research-informed teaching and motivates continued participation.

$$Adoption\ Rate = (12/63) \times 100\% \approx 19\% \quad (3)$$

An adoption rate of 19% for vulnerability reports is a strong indicator of success, confirming that the research-driven tasks produced outcomes that met professional standards and provided direct value to the education system's cybersecurity.

5. Conclusion and Outlook

5.1 Research Conclusions

This study explores the "research-driven teaching" model for cybersecurity majors in engineering universities. Combining the major's dynamic attack and defense capabilities and strong practical application with the engineering advantage of closely integrating research and practice, this study establishes a feasible feedback loop by building a phased teaching system, designing a resource linkage mechanism, and implementing typical practical cases. The core contributions and key insights are as follows:

5.1.1 Construct a full-chain feedback model of "research - curriculum - practice - employment" to solve the dual pain points of professional teaching

This model employs a four-year "enlightenment–integration–practice–innovation" structure, where freshmen build foundations via open lab projects and seniors undertake vertical research for graduation. Backed by a tripartite support system—open labs, industry collaboration, and faculty synergy—it incorporates resources such as ICS test platforms and real enterprise attack-defense cases, shifting research use from fragmented to fully integrated.

Empirical outcomes confirm efficacy: a 19% adoption rate for student vulnerability reports (12 of 63 adopted by the Provincial Department of Education) and a 28% increase in course satisfaction, validating the integrated approach. The model's positive reception by students is a critical measure of its success. The increase in student approval, likely measured through comparative course evaluations, was significant:

$$Satisfaction\ Improvement = (Satisfaction\ After - Satisfaction\ Before) = 28\% \quad (4)$$

This 28% increase in course satisfaction serves as a strong subjective metric, complementing the objective performance data and verifying that the full-chain design is not only effective but also positively received by the learners it is designed to benefit.

5.1.2 Innovate the implementation path of "step-by-step participation + practical orientation" to lower the threshold for scientific research and strengthen practical capabilities

A tiered participation system matches tasks to student skill levels—freshmen handle ICS traffic labeling, while juniors conduct independent vulnerability verification. Evaluation metrics reflect practical contributions, such as red/blue team exercise involvement and emergency response performance.

Participants also achieved 35% higher employment rates and 22% more placements at top cybersecurity firms, confirming the strong link between research experience and employability. These outcomes validate the effectiveness of the tiered, practice-oriented approach. The improvement rate, calculated by comparing post-intervention metrics against the baseline, demonstrates the model's impact:

$$CTF\ Winning\ Rate\ Improvement = 45\% \quad (5)$$

$$Employment\ Matching\ Rate\ Improvement = 35\% \quad (6)$$

$$Top-Company\ Employment\ Rate\ Improvement = 22\% \quad (7)$$

These quantitative results provide concrete evidence that the model successfully addresses the practical skill shortcomings of traditional teaching methods.

5.2 Future Outlook

Leveraging rapid technological iteration and university research strength, this model integrates cutting-edge trends like AI attack-defense into courses such as "AI Security" and "AI Penetration Testing." Students develop and test algorithms in lab environments before applying them in real-world scenarios like e-commerce penetration tests.

Emerging areas including quantum key distribution (QKD) and post-quantum cryptography (PQC) are incorporated using university testbeds. Learners simulate attacks like quantum signal interference and contribute data to ongoing research.

Industrial challenges such as ICS/IIoT security are broken down into course tasks. Students analyze protocol vulnerabilities, replicate attacks in simulations, and develop defenses. Outcomes are fed back as updated teaching cases, closing the loop between industry needs and educational content.

References

[1] China Cybersecurity Industry Alliance. China Cybersecurity Talent Development White Paper (2024). Beijing: China Cybersecurity Industry Alliance, 2024.

[2] Wang Jian, Li Na. Exploration of Research Feedback Teaching Path for Cyberspace Security Majors in Engineering Colleges. Computer Education, 2023, (8): 45-50.

[3] Zhang Wei, Liu Min. Research on the Lagging Problem of Cybersecurity Course Content Update. Research on Higher Engineering Education, 2022, (5): 132-137.

[4] Keinonen M. Using Military Cyber Operations as a Deterrent. International Conference on Cyber Warfare and Security, 2023.

[5] Tang R, Zhang W. Comparative Legal Perspectives on Cyberspace Security Governance: A Review of Frameworks and Implication. Journal of Computer Science Research, 2025, 7(1): 1-10.

[6] Guangdong Polytechnic Normal University. Intellectual Property Big Data Key Laboratory Research and Education Report (2023). Guangzhou: Guangdong Polytechnic Normal University, 2023.

[7] Crawley E F, Malmqvist J, Östlund S, et al. Rethinking Engineering Education: The CDIO Approach. New York: Springer, 2007.

[8] Thomas J W. A Review of Research on Project-Based Learning. The Journal of Engineering Education, 2000, 89(3): 205-215.

[9] Qi'anxin Technology Group. White Paper on Collaborative Cybersecurity Talent Training between Schools and Enterprises. Beijing: Qi'anxin Technology Group, 2023.

[10] Hurk N V D, Treur J, Roelofsma P H M P. Organizational Learning for Safety and Security Through Cyberspace: Adaptive Modelling of the Implementation of Environment Health and Safety Standards. Studies in Systems, Decision and Control, 2024:351-372.

[11] Imperial College London. Quantum Communication Security Teaching Practice. IEEE Transactions on Education, 2022, 65(3): 312-318.

[12] Lave J, Wenger E. Situated Learning: Legitimate Peripheral Participation. Cambridge: Cambridge University Press, 1991.

[13] Song Xiaolu. Research on industrial data enhancement technology and deep latent variable modeling method based on machine learning. Beijing University of Chemical Technology, 2025.

[14] Xu Yuanyuan. Research on the application of open courses in cloud computing environment. East China Normal University, 2013.

[15] Karimi A. Reflections on the development of problem-based history teaching in the context of cyberspace Journal of Social Studies Education Research, 2021, 2(4):1-32.

[16] Wang Shenglan, Peng Shuang. The impact of technology-enhanced learning environment on student development. China Education Informatization, 2025, 31(03): 107-117.

