"Three-Dimensional Integration" Network Security Technology Teaching Reform Path Based on CTF Competition

Xiaoli Yu, Gang Qiu*
School of Information Engineering, Changji University, Changji, China
**Corresponding Author*

Abstract: In response to the current issues in network security technology teaching, such as abstract content, weak practical components, monotonous teaching methods, limited instructional scenarios, and insufficient digital literacy among teachers, this study proposes a "three-dimensional integration" teaching reform approach based on CTF (Capture The Flag) competitions. At the curriculum system reconstruction level, a tiered and progressive course module of "basic theory—attack and defense training—comprehensive drills" is established, with CTF competition question types organically integrated into the curriculum. In terms of assessment innovation, a diversified evaluation system of "problem-solving competitions + attack and defense competitions + project development" is introduced, and CTF competition results are incorporated into course credit recognition standards. Regarding teaching model reform, a case-guided Outcome-Based Education (OBE) teaching approach is implemented, while simultaneously promoting the regular training mechanism of CTF campus clubs. Practice has shown that this model significantly enhances students' learning interest through "competition-driven learning" and effectively improves the actual teaching outcomes of the course.

Keywords: Network Security Technology Curriculum Reform; CTF Competition-Driven; Attack and Defense Confrontation Training; OBE Teaching Mode; Competition Credit Conversion

1. Introduction

With the rapid development of next-generation information technologies, cyberspace has emerged as the fifth strategic domain after land, sea and space [1]. In recent years, the global cybersecurity landscape has become increasingly severe, with Advanced Persistent Threat (APT) attacks exhibiting new characteristics, including diversified methods and highly targeted objectives. In 2021, Colonial Pipeline, the largest fuel pipeline operator in the U.S., fell victim to a ransomware attack, disrupting fuel supply along the East Coast [2]. In 2022, Ukrainian government websites and critical infrastructure suffered large-scale cyberattacks, forming a "hybrid warfare" scenario alongside the Russia-Ukraine conflict [3]. In 2023, multiple Chinese research institutions uncovered long-term covert attacks by the "Volt Typhoon" APT group targeting critical infrastructure [4].

These incidents demonstrate that cyberattacks have evolved from mere technical challenges into significant threats to national security. Currently, China faces significant challenges in cultivating cybersecurity talent. According to authoritative statistics, the country's shortage of cybersecurity professionals is projected to exceed 3 million by 2027[5]. This gap stands in stark contrast to the requirements set forth at the 20th National Congress of the Communist Party of China, which emphasized the need to "thoroughly implement the strategies for invigorating China through science and education and strengthening the nation through talent development."

As a critical hub for talent cultivation, applied undergraduate institutions must urgently establish a network security technology talent training system that meets the demands of the new era. This is essential to provide robust human resources for safeguarding national cyberspace security.

Network security technology, as a specialized course for majors such as Computer Science and Technology and Network Engineering, is a highly comprehensive discipline that encompasses multiple theoretical subjects,

including Computer Networks, Computer Organization and Principles, Cryptography, Databases, and Operating Systems [6].

Currently, our institute adopts a "48+16" theory-practice model, where practical hours are relatively limited. Moreover, practical sessions are primarily designed independently by instructors, lacking a systematic and well-structured practical teaching framework. Over the past two years of teaching the network security technology, several issues have been identified, such as: abstract teaching content; weak practical components; monotonous teaching methods; limited teaching scenarios; insufficient digital literacy among instructors and so on.

After analyzing various teaching models, this study concludes that a CTF (Capture The Flag) competition-based learning approach is more suitable for network security technology education. Guided by the "learning through competition" philosophy, this research proposes a new teaching model for the network security technology course: Integrating network security technology work with CTF competitions in both form and content.

Establishing a practice-oriented teaching system that reforms teaching methods, assessment formats, and faculty development.

Cultivating students with solid theoretical foundations and hands-on problem-solving skills.

Through these pedagogical reforms, the study aims to enhance student engagement and interest in learning.

2. Current Challenges in Network Security Technology Education

Over the past two years of teaching this course, five major issues have been identified in our network security technology curriculum: overly abstract content, weak practical components, monotonous teaching methods, limited teaching environments, and insufficient faculty expertise. These shortcomings collectively hinder the quality of network security technology education.

2.1 Overly Abstract Content

The current network security technology courses generally have the problem of focusing on theory and light on practice, overemphasizing basic and conceptual knowledge such as network protocols, encryption principles, firewall mechanisms, etc., —while failing to establish meaningful connections to real-world scenarios. Although this theoretical teaching method helps students to establish a certain basic knowledge system, due to the lack of real cases to support and practical training, it is often difficult for students to connect the knowledge they have learned with the complex network security problems in reality, resulting in the learning process becoming boring and tedious, the interest in learning has decreased significantly, and the degree of knowledge mastery is unsatisfactory.

For example, when explaining encryption algorithms, many courses only stay in the algorithmic process, mathematical formulas and the introduction of the basic principles of the level, the students may repeatedly memorize to master the basic structure of AES or RSA and the use of the method, but it is not clear that these encryption techniques in the real information system, how to deploy, how to be cracked by the attacker, and in what kind of scenarios should be selected to protect the security of data encryption. . This disconnect between knowledge and application makes students often clueless when facing real problems and lack the ability to solve real security vulnerabilities.

2.2 Weak Practical Components

The '48+16' teaching model allocates just 16 class hours for practical training—a proportion that is demonstrably insufficient to systematically cultivate students' applied network security technology skills. Currently, most experiments remain limited to instructor-led verification tasks, requiring students merely to follow predefined steps rather than engage in independent problem-solving. This approach fails to develop critical thinking or prepare learners for dynamic network attack scenarios.

Such theory-heavy, practice-light pedagogy prevents the curriculum from authentically reflecting the demands of real-world network security technology work. Consequently, graduates face significant competency gaps and struggle to adapt to industry requirements. Feedback from the industry also shows that many network security technicians who have just joined the workforce lack sufficient practical training during school, and show

insufficient coping ability in the face of real security incidents, which affects their professional competence. This also reflects that there is a certain disconnect between the current network security education and industry demand, and there is an urgent need to increase the comprehensive, practical teaching sessions to enhance students' hands-on ability and combat literacy.

2.3 Monotonous Teaching Methods

Currently, classroom instruction primarily relies on traditional lectures, with low levels of interactivity and student engagement. Teachers typically deliver theoretical knowledge through slides, while students passively absorb information. There is little use of case studies, red-blue team drills, or real-time attack-defense simulations—teaching methods essential for fostering practical abilities. This passive “spoon-feeding” approach does not cultivate students’ innovative thinking or adaptability, both of which are core competencies for network security technology professionals.

2.4 Limited Teaching Environments

Teaching is confined to regular classrooms and basic virtual labs, offering students no exposure to real working environments. They rarely operate enterprise-grade security tools such as SIEM systems or intrusion detection platforms, nor do they participate in large-scale cyber attack and defense exercises. Without immersive scenarios, students cannot grasp the dynamic nature of cyber threats or develop the practical response capabilities required in the field.

2.5 Insufficient Faculty Expertise

Currently, some teachers lack an in-depth understanding of the cutting-edge dynamics and technology development trends in the field of network security, especially in the application of emerging technologies and practical attack and defense mechanisms, there is a knowledge lag. At the same time, the teaching team generally lacks systematic knowledge and practical experience of CTF and other network security competitions, making it difficult to provide targeted guidance and support for students. As most teachers lack practical experience in the industry or authoritative professional certification, the course content is updated slowly, making it difficult to keep pace with the development of the industry. In addition, the school has not yet established a comprehensive teacher training system, and teachers mainly rely on independent study to update their knowledge structure, which leads to teachers' inability to cope with the rapidly evolving cybersecurity field. This directly affects the quality of teaching and weakens the ability of teachers to dynamically adjust the content and direction of teaching according to the needs of the industry.

3. "Three-Dimensional Integration" Teaching Reform

3.1 Restructuring the Curriculum System

In alignment with the requirements of emerging engineering education and the talent cultivation objectives of related disciplines, and guided by the core principles of Outcome-Based Education (OBE)—"student-centered development, outcome orientation, and continuous improvement"—we have designed a "trinity" curriculum framework for the network security technology course based on the talent cultivation program design process.

Knowledge Objective: To master the basic principles and development trends of modern network attack and defense technologies, and to understand the security protection methods in major fields such as operating systems, Web services, and mobile applications. Understand the future trend of network security technology and its application in new types of combat.

Ability Objective: Through the combination of theory and practice, to have the ability to discover and investigate network security hidden dangers, to be able to solve common network security problems, and to have the ability to respond to actual combat, independent learning and innovative practice.

Quality Objective: Integrate into the Civic and Political Education, enhance the national security concept and the awareness of the rule of law, and establish the professional ideal of serving the country. Cultivate the spirit of science and professional identity, and enhance the network security practical literacy and sense of responsibility.

(1) To address the varying learning conditions across different classes and differences in training programs and syllabi, the curriculum is designed using a modular approach to

flexibly meet diverse teaching needs. Based on the revised syllabus tailored for four majors, at least three sets of multimedia courseware will be developed. The course content is restructured into three progressive modules—from basic to advanced, and from fragmented knowledge to comprehensive understanding: the basic theory module, the attack and defense practical training module, and the comprehensive application module. CTF competition questions are deconstructed into teaching cases and integrated into theoretical instruction to achieve the goal of "explaining concepts through competition.

(2) According to the situation of the institution and the available laboratory resources, the project-based network experiments are developed to meet the practical requirements of the students, create good experimental opportunities for the students, and exercise the students' ability to combine theory and practice. Verification experiments by students using virtual machines Vmware to build their own experimental platforms and ranges, mainly to do password cracking, network scanning, network protocol defects, phishing, SQL injection and other basic experiments, not only to exercise the ability of students to build their own hands to build ranges, but also able to build the experimental platforms in closed environments, to avoid the impact on the campus network; comprehensive experiments using the network security The comprehensive experiments utilize the network security training platform to carry out the form of attack and defense confrontation drill and CTP flag capturing match to further improve the students' practical ability, so that the students can consolidate the principles in the actual combat, get a sense of achievement in the experiments, and improve their learning interest.

(3) Combining the formation background, development history, research status, future trends, major engineering and scientific and technological development achievements, the deeds of scientists or exemplary figures, and the development of enterprises of the network security technology, students will be able to tap into the ideological and political education elements such as the sense of mission, sense of responsibility, patriotism, the spirit of struggle, and the spirit of pioneering and innovation that are embedded in it. By telling students about hot events of network security, China's national security strategy, the construction of China's network security legal system, and examples of China's Red Guest Warriors defending national information security, etc., we gradually build up students' awareness of network security, stimulate students' patriotic feelings, and integrate the ideological and political elements of the course into classroom teaching to cultivate students' awareness of the overall national security concept. In the teaching process, combined with the professional talent training program and the vocational quality requirements of the jobs that the students will be engaged in after graduation, we will targetively excavate the nurturing elements contained in the courses, improve the students' career development ability, enhance the pertinence and effectiveness of the courses' nurturing, and strive to make the students become composite talents in line with the needs of the society.

3.2 Evaluation Mechanism Innovation

To enhance the assessment of students' ongoing learning, stage-based evaluations—such as homework assignments, laboratory experiments, and chapter self-tests—are emphasized. The proportion of these (stage grades) in the overall course evaluation has been clearly defined. The comprehensive assessment model is implemented as follows: 60% final exam + 20% chapter tests + 10% experimental assignments + 10% regular performance, providing a more holistic reflection of students' learning outcomes.

In the design of practical content, in addition to including modules intended for individual completion, group-based collaborative tasks are also incorporated to promote project-based learning through teamwork, thereby enhancing students' cooperative and communicative abilities. After completing the experimental projects assigned by the instructor, each group is required to present their results as a team, encouraging peer comparison, discussion, and knowledge sharing. Teachers evaluate the overall performance of each group based on predefined assessment criteria and also introduce multiple evaluation methods, such as peer assessment and group self-assessment.

Furthermore, a diversified evaluation system combining "problem-solving competitions + attack-defense challenges + project extensions"

has been implemented, with CTF competition outcomes integrated into the course grading framework. Students who achieve outstanding results in relevant competitions or vocational skill certification exams may receive bonus points in the course. An appropriate incentive mechanism has also been established to encourage active participation in professional practice activities, ultimately improving students' overall competence and hands-on capabilities.

3.3 Teaching Mode Reform

In the first classroom teaching, the case-led Outcome-Based Education (OBE) model is adopted, with the core theory of network security technology as the main line, and the teacher plays a leading role in systematically explaining network security fundamentals, attack and defense mechanisms, and related knowledge around real cases to help students build a solid theoretical system. Teaching design is always learning outcome-oriented, emphasizing that students understand the knowledge points through cases and are able to apply them to practical problem solving.

At the same time, we actively expand the construction of the second classroom, encourage students to utilize the catechism platform and all kinds of online resources to carry out independent learning, and give full play to the subjectivity and learning initiative of students. Through the in-depth integration of "offline theoretical lectures + online extended learning", a blended teaching mode in line with the OBE concept is formed to ensure that each teaching link serves the clear learning objectives and ability output.

The experimental part of the course relies on network security special tools to build an attack and defense experimental environment, combines with the project-based teaching methodology, transforms typical topics in CTF competitions into teaching cases, and designs multi-level and modular experimental tasks around real network attack and defense scenarios. Through Web penetration, reverse analysis, vulnerability mining, password cracking, and other close to the actual combat case training, to enhance the students' comprehensive combat capabilities in complex situations.

In this process, students act as project participants and problem solvers, working collaboratively in teams to complete various attack-and-defense challenges. Teachers serve as facilitators, providing technical guidance and inspirational insights at key stages to help students transition from passive knowledge recipients to active explorers and practitioners. This shift significantly enhances teaching effectiveness and student competency development, fully embodying the OBE principle of being "student achievement-oriented." The core teaching philosophy of OBE—placing student learning outcomes at the center of instruction—is thus effectively realized.

To address the issue of weak self-directed learning among some students, the teaching process has been deeply integrated with intelligent teaching platforms such as Rain Classroom and DingTalk. These tools enable real-time interaction between teachers and students, as well as comprehensive management of the entire learning process. By adopting diverse instructional formats—such as "knowledge explanation + attack-defense practice + group discussion," "independent study + peer support + teacher-student Q&A," and "team-based experimental design + mutual evaluation between teachers and students"—the teaching organization is enriched, student participation is enhanced, and learning enthusiasm is significantly boosted. This approach further promotes the diversification of teaching modes and supports a more dynamic and interactive learning environment.

3.4 Establishment of CTF Campus Club and Cyber Security Competition Teams

Based on the concept of "mutual learning and common progress, hand in hand growth", the club is committed to creating a platform for students to practice their practical skills and further enhance the influence and participation of network attack and defense technology on campus. More students who are interested in network security will come together to form a good learning community, collide ideas in communication, and improve skills in cooperation.

The club actively undertakes the publicity and organization of various network security technology competitions, encourages and guides interested students to participate in them, and continuously expands the mass base of network security technology learning.

Considering that CTF competitions have higher requirements for knowledge reserves and technical skills, the club selects and organizes teams mainly for sophomores so that they can enter the state as early as possible on the premise of having certain basic knowledge. Students are trained in groups according to their interests and expertise, such as Web security, reverse engineering, vulnerability mining, cryptanalysis, and other directions, to realize personalized development paths and enhance learning efficiency.

At the same time, the club will plan to organize members to participate in various high-level events, including but not limited to: Electronic Data Forensics Competition, National Student Information Security Competition, domestic and international famous CTF events such as “Strongnet Cup”, “WCTF World Hacking Competition” and so on. The team will be organized according to the situation of team building. According to the team building situation, we reasonably arrange students at different stages to participate in the corresponding level of the competition, from the primary competition to the high-level competition step by step, to test the learning results in the actual combat, enhance the sense of honor and sense of belonging, and stimulate the motivation for continuous learning.

In order to enhance the practical skills of members in network security technology, CTF Campus Club carries out regular weekly technical sharing sessions, mainly focusing on the exchange of network security technical knowledge, the use of tools, and thematic analysis. Once a month, CTF Campus Club organizes special training to systematically explain the cutting-edge knowledge of a certain security direction and help improve skills. Centralized training is organized before the competition to strengthen teamwork and real-world resilience. Through the regularized training mechanism, the professionalism and competitive level of students are steadily improved.

3.5 Teacher Team Building

In order to guarantee the smooth progress of the teaching reform of network security courses and improve the teaching quality and combat level, it is crucial to build a “dual-teacher” teaching team with reasonable structure, good quality and combat ability.

First of all, strengthen the cultivation of teachers' professional ability. Encourage teachers to participate in all kinds of network security-related professional training, technical seminars, and industry conferences to systematically learn cutting-edge security technologies, and at the same time, support teachers to obtain authoritative certification qualifications to enhance their professional authority in the field of network security.

Secondly, we promote teachers' participation in enterprise practice and school-enterprise cooperation. By going to network security enterprises to practice or participate in actual project development, they can enhance their understanding of industry dynamics, job requirements and technology trends, so as to better integrate theoretical knowledge and practical skills into classroom teaching.

Again, we place significant emphasis on enhancing teachers' competitiveness. Given that the course integrates elements of CTF and other cybersecurity competitions, it is essential for instructors to have a deep understanding of competition rules, question design, and problem-solving strategies. To achieve this, we organize participation in high-level CTF events or on-campus simulation training camps during holidays, allowing teachers to accumulate valuable hands-on experience. Teachers are also encouraged to lead student teams in competitions, thereby strengthening their ability to guide and mentor effectively.

Through the above measures, we gradually build a high-quality network security teacher team that understands both theory and practice, and has both teaching ability and real-world experience, so as to provide a solid guarantee for the construction of the curriculum and the cultivation of talents.

4. Effectiveness of Practice

The “Three-Dimensional Integration” network security technology teaching reform based on CTF competition adheres to the teaching concept of “teacher-led, student-led” and closely matches the actual needs of the development of vocational ability. This mode effectively stimulates students' learning initiative, improves hands-on practical ability and teamwork consciousness, reflects the teaching innovation of promoting teaching and learning by competition, and has achieved

good results in the teaching of network security-related courses.

Relying on the course program, the college has established the CTF Campus Club, which has recruited nearly 100 members as of June 2025. The club utilizes evening self-study periods to conduct activities aimed at promoting cybersecurity knowledge while organizing live attack-and-defense demonstrations on weekends and holidays to enhance students' understanding and interest in cybersecurity. In addition, the club regularly holds weekly online training sessions, primarily conducted on platforms such as "Attack and Defense World" and "CTFHub", where members engage in hands-on practice. These activities are complemented by monthly participation in various online CTF competitions, further strengthening students' practical and combat skills.

Members of the club have participated in six important events, including: the 14th National College Students Information Security Competition (CISCN) Innovation and Practice Ability Competition, "Hecheng Cup" CTF Cyber Challenge, the 5th "Strong Network Cup" National network security technology Challenge, and the West Lake network security technology Challenge 2021. The "West Lake Sword 2021 China Hangzhou Cyber Security Skills Competition", the 4th "Red Hat Cup" Cyber Security Competition and the 3rd Meituan College Cyber Security Challenge. We achieved excellent results in the competitions, winning the second prize of the 14th CISCN Northwest Region, the third prize of the West Lake Sword network security technology Skills Competition, and the 23rd place in the national information security triathlon, which fully demonstrated the practical achievements of the teaching reform and the construction of associations.

5. Conclusion

Through the curriculum reform, a relatively scientific and mature teaching model based on "learning through competition" has been developed, along with valuable teaching experience. Students, centered around classroom instruction and supported by a blended online-offline learning approach, have benefited from the integration of online educational resources and CTF training platforms. This reform has shifted the focus of teaching, effectively guiding and supporting students in improving their self-learning abilities. It has also transformed students' learning methods, promoting independent and inquiry-based learning, while enhancing teamwork and collective awareness.

However, CTF competition content also involves knowledge from other courses such as databases, computer communication networks, computer architecture, cryptography, and operating systems. Therefore, it is recommended that future efforts expand the project to include interdisciplinary curriculum reforms, integrating multiple related courses to jointly promote the application and transformation of CTF competition outcomes.

In addition, many instructors involved in the course are not originally trained in network security technology. Their limited professional background in this field has had a certain impact on teaching effectiveness. Due to a lack of specialized faculty, the teaching workload is heavy, and there are few opportunities for teachers to attend further training or professional development programs.

Moreover, the revision cycle for teaching plans, syllabi, courseware, and lab manuals is relatively long. Throughout the teaching process, it's essential to continuously summarize feedback and gradually refine these materials. This course represents an attempt at implementing a "learning through competition" model, shifting the focus from teacher-centered instruction to student-centered learning. During lectures, efforts are made to collect relevant cases that illustrate the negative impacts of network security technology issues, enabling students to understand these implications within practical contexts. However, there was less emphasis on setting up specific opportunities for teacher-student discussions aimed at guiding students towards discovering solutions for network security technology problems and enhancing their ethical standards. Recognizing the necessity, urgency, and importance of strengthening network security technology awareness is crucial.

Finally, since the establishment of the CTF club, it has been observed that the majority of core members are juniors and seniors. Considering the sustainability of the club's operations, it is important to vigorously recruit freshmen and sophomores into the club and

select new core team members from among them. Innovations in activity formats are also necessary to prevent member attrition caused by monotonous study and training sessions. At the departmental level, active support and guidance should be provided to promote various activities and enhance the standardized management of the club. The goal is to transform the CTF club into a cradle for nurturing and selecting talented CTF competitors, ensuring its continuous development and success.

Acknowledgments

Fund Project: 2023 Xinjiang Uygur Autonomous Region Undergraduate Education Teaching Research and Reform Project. Project name: Exploration and practice of first-class professional construction of network engineering. Project code: XJGXZHJG-202341.This research was also supported by the following funding sources at Changji University: (1) Key Laboratory of Artificial Intelligence and Computing Power Applications, (2) Talent Special Project on Illegal Signal Detection and Recognition

References

[1] Wu, H., Li, X. D., Cheng, X. K., et al. (2024). A survey on APT attack detection technologies. Telecom World, 31(02), 61-63.

[2] Turton, W. (2021, May 8). Colonial Pipeline halts operations after cyberattack. Bloomberg. https://www.bloomberg.com/news/articles/2021-05-08/colonial-pipeline-halts-operations-after-cyberattack.

[3] European Union Agency for network security technology. (2022). Cyber threats during the Russia-Ukraine war. https://www.enisa.europa.eu/publications/cyber-threats-russia-ukraine-war.

[4] Mandiant. (2023). APT activity targeting critical infrastructure in East Asia. https://www.mandiant.com/resources/reports/apt-east-asia

[5] Xiong, Q. C., Chen, G., Du, Q. P., et al. (2023). Exploration of practical teaching in cyber attack and defense based on cyber range platform. Journal of China Multimedia & Network Teaching, (02), 13-16.

[6] Ying Z, Leian L. Practice of Teaching Reform of Network Security Technology Course under the Background of Internet+. International Journal of Information and Education Technology, 2019, 9(5):370-37

