# AI-Enabled Three-Dimensional Intelligent Integration and Capacity Transition Model: A Generic Teaching Framework for Cybersecurity Courses

Yi Shen, Zulie Pan, Lu Yu *, Miao Hu

College of Electronic Engineering, National University of Defense Technology, Hefei 230037, China

*email: lulu071227@163.com

**Abstract.** As cybersecurity rises to the national strategic level, cultivating innovative and versatile cybersecurity talents with practical capabilities has become an urgent task for higher education. Cybersecurity courses face prominent challenges such as heterogeneous student knowledge structures, the contradiction between high motivation and high cognitive load, "selective participation" in class, and high frustration in practice. This study systematically constructs a teaching innovation system featuring "three-dimensional intelligence integration and capability leapfrogging." Guided by the value of "five synergies" in ideological and political education in courses, this system achieves a paradigm shift from "knowledge impartation" to "capability construction" and even "practice capability generation" by reconstructing progressive course resources, reforming the integrated teaching method of "learning, research, and practice" (deeply integrating AI dual-assist system and BOPPPS model), and implementing a comprehensive evaluation of "process-oriented, diversified, and capability-oriented." Teaching practice shows that this model effectively addresses common challenges in traditional teaching, significantly enhancing students' practical capabilities, innovative thinking, and professional qualities. It has yielded outstanding educational results and gained widespread social recognition, offering a systematic solution for cybersecurity talent cultivation in the new era that features well-supported replicability and scalability—with explicit minimum viable resource requirements defined and good scalability for institutions constrained by limited budgets and a shortage of expert instructors.

**Keywords:** Cybersecurity; Teaching Innovation; Capability Transition; Ideological Education; AI Empowerment; Practical Practice Capability

## 1 Introduction

In the context of the rapid development of digital economy and cybersecurity, cybersecurity education faces unprecedented challenges and opportunities. While traditional teaching models focus heavily on theoretical knowledge, they often struggle to bridge the gap between classroom learning and real-world practical requirements, especially


I. A. Khan et al. (eds.), *Proceedings of the 2026 5th International Conference on Educational Innovation and Multimedia Technology (EIMT 2026)*, Atlantis Highlights in Social Sciences, Education and Humanities 51,
https://doi.org/10.2991/978-94-6239-691-3_63

in fields characterized by fast technological iteration, high technical thresholds, and strong industry demand. In recent years, Artificial Intelligence (AI) has provided new possibilities for educational innovation, enabling more adaptive, personalized, and scenario-driven teaching environments.[7][8][9].

Against this backdrop, this study proposes a systematic teaching framework named "Three-Dimensional Intelligent Integration and Capacity Transition" (3D-II-CT), aiming to address the core dilemmas in cybersecurity training: the disconnection between knowledge acquisition and practical ability, the lack of integrated support in teaching resources, and the difficulty in evaluating complex competencies. Unlike single-course innovation, this framework seeks to offer a generalizable model that can be applied across multiple cybersecurity sub-disciplines, thereby enhancing both theoretical depth and industrial relevance.

## 2 Research Background and Core Challenges

Cybersecurity Courses typically exhibit heterogeneous academic backgrounds, varying levels of practical experience, and divergent learning motivations. These factors often lead to challenges such as uneven cognitive loads, selective participation in classroom activities, and difficulty in translating theoretical knowledge into security analysis and defensive development.

Furthermore, conventional cybersecurity teaching structures rely on rigid curricula and isolated resource modules, which fail to support comprehensive competency formation. In international cybersecurity education, similar issues exist—most existing AI-enabled teaching innovations focus on technical tools or resource construction, but lack a unified framework that integrates value guidance, resource support, and teaching/evaluation.

The 3D-II-CL framework constructed in this research responds to these challenges by emphasizing multidimensional integration, AI empowerment, and capacity progression. It goes beyond course-level improvements and targets the establishment of a sustainable teaching ecosystem applicable to various cybersecurity programs.

## 3 Constructing the "Three-Dimensional Intelligence Integration and Capability Transition" System

To address these challenges, we designed a systematic teaching innovation framework: **"Three-Dimensional Intelligence Integration and Capability Transition" System**. This system is centered on ideological education, with three dimensions: curriculum resources, teaching methods, and evaluation systems. The framework is illustrated in Figure 1.

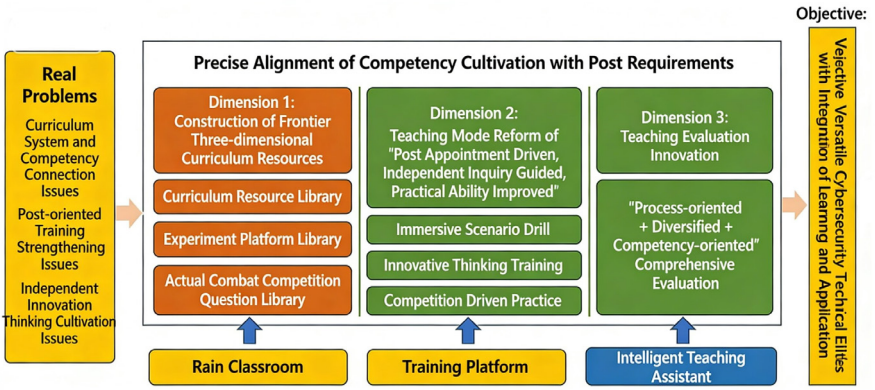


**Fig. 1.** "Three-Dimensional Intelligence Integration and Capability Transition" framework

## 3.1 Value Guidance Dimension: "Five Synergies" Ideological Education System

The course integrates ideological education through five synergies: value discourse, attack-defense case studies, adversarial thinking, legal literacy, and research innovation. This approach embeds national security awareness, ethical responsibility, and a "cybersecurity for national defense" mindset into technical training.

### 3.1.1 Integration of Value Deliberation.

This component guides students to recognize the critical importance of cybersecurity, understand the ethical values and social responsibilities inherent in technology, and establish a correct view of cybersecurity. It emphasizes cultivating a sense of patriotic duty in applying science and technology for national development, alongside fostering the confidence to pioneer innovation. The pedagogical approach involves integrating case studies that prompt moral reasoning, encouraging students to reflect on the dual-use nature of security analysis technologies and their broader societal impact, thereby developing a strong sense of professional ethics and mission.

### 3.1.2 Synergy through Attack-Defense Case Studies.

Take vulnerability analysis course for example, leveraging historical case studies as an educational mirror, this element involves in-depth analysis of the vulnerability principles behind typical incidents like the Stuxnet virus. It meticulously dissects the process, methodology, and mindset behind vulnerability discovery, aiming to inspire a sense of mission centered on "forging strong shields and strengthening networks."

### 3.1.3 Cultivation of Adversarial Thinking.

This dimension focuses on developing students' reverse engineering thinking, systems thinking, and strategic thinking within network security analysis, enabling a deep understanding of the essential nature of offensive and defensive adversarial dynamics.

It encourages "asymmetric" innovative thinking—finding unconventional paths—and a "ten years sharpening a single sword" spirit, which signifies persistence and long-term dedication to mastery. Teaching methods include red team/blue team exercises to foster a proactive and strategic mindset essential for modern cybersecurity challenges.

#### 3.1.4 Coordination of Legal Literacy.

Throughout network security analysis practices, the course integrates content from the *Cybersecurity Law of the People's Republic of China* and other relevant regulations. It guides students to deeply understand the legal connotations of "technology for good" and the legal boundaries of innovative activities. The objective is to cultivate professional integrity based on "using technology in accordance with the law" and to reinforce the legal consciousness that "institutional systems are practice capability." This is embedded via discussions on responsible network security analysis processes, cyber ethics, and the legal frameworks governing cyber operations, ensuring students appreciate the rule of law as a fundamental component of national cyber strength.

### 3.2 Resource Support Dimension: Restructuring Core Resources and Practical Platforms

#### 3.2.1 Core Resource Construction: Combination of Content Reconstruction and Teaching Resource Construction.

**1. Systematic reconstruction of teaching content**

Take vulnerability analysis course for example, based on the long-term technical accumulation of classic textbooks and teaching teams in the field of network security analysis, the course content is reconstructed into two interrelated parts: "Principles and Practice of Vulnerability Exploitation" and "Exploration of Automated Vulnerability Analysis Techniques". The former focuses on the cultivation of practical analysis skills for specific types of vulnerabilities such as buffer overflows, formatted strings, and UAF; the latter emphasizes the academic research ability cultivation in cutting-edge automated analysis techniques such as symbolic execution, fuzz testing, and taint analysis. The two parts complement each other, forming a systematic and in-depth knowledge map.

**2.Construction of multi-dimensional teaching resources**

Build a multi-dimensional teaching resource system that integrates "online + offline" approaches[3]. Offline resources include authoritative planning textbooks, courseware and lesson plans that are dynamically updated to follow cutting-edge technology; online resources primarily rely on secure training platforms and Rain Classroom to build a knowledge base including online courses, micro-video courses, papers, etc., providing students with personalized and differentiated learning support.

#### 3.2.2 Practical Resource Platform.

Relying on the network security training platform, we have constructed a three-tier basic experiment library for vulnerability analysis courses, consisting of "standardized

experiments, customized experiments, and typical vulnerability reproduction". Standardized experiments focus on basic skill training, customized experiments emphasize personalized ability cultivation, and typical vulnerability reproduction focuses on real-scenario simulation. Through this progressive design, students are helped to gradually consolidate their practical foundation and meet the differentiated needs of students with different levels of foundation.

### 3.3 Teaching Implementation Dimension: Integrated "Learning-Research-Practice" Reform

#### 3.3.1 AI Dual-Assistant System Empowers Teaching Throughout the Entire Process.

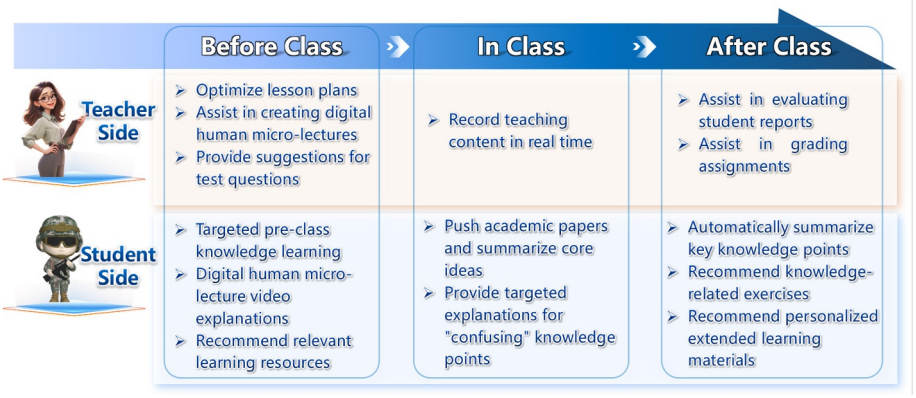


**Fig. 2.** AI Dual-Assistance System: Covering the Entire Teaching Cycle

In response to the heterogeneous knowledge bases of students and the demand for personalized guidance, an AI dual-assistance system (AI student assistance + AI teacher assistance) has been developed and deployed (As shown in Figure 2), integrating throughout the entire teaching process[6][12]. The system has constructed a knowledge base and course micro-videos closely corresponding to the curriculum content, providing comprehensive teaching support for the core teaching links of cybersecurity analysis, and integrating multiple AI-enabled intelligent roles including AI lecture partners, AI tutoring mentors and AI learning assistants.

The AI-assisted learning system can provide personalized learning path recommendations, adaptive exercises, and intelligent question answering based on students' learning behaviors and knowledge mastery. The AI-assisted teaching system can assist teachers in homework grading, learning behavior analysis, and teaching decision support. This system effectively solves the problems of insufficient personalized guidance and delayed teaching feedback in traditional teaching, achieving large-scale individualized instruction.

### 3.3.2 Classroom Teaching Design Focusing on Cultivating Innovation Consciousness.

In classroom instruction, we emphasize the cultivation of students' innovative consciousness. By comprehensively utilizing the BOPPPS model and flipped classroom[1][2], and relying on practical training platforms, we fully engage students in classroom participation while fostering their independent thinking ability and innovative consciousness (As shown in Figure 3). Through group discussions, inter-group competitions, and other activities, we promote students' independent exploration and guide them in the use of large model tools[4]. We seamlessly integrate ideological and political elements to cultivate students' scientific thinking, incorporating principles such as network security management laws and regulations constraints, and the "countermeasures" inherent in network security analysis techniques.

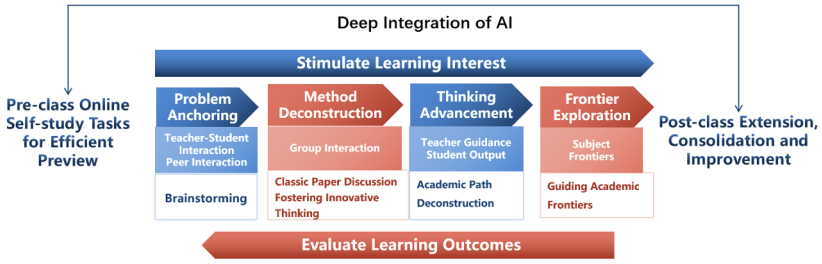


**Fig. 3.** Deep AI Integration: A Full-cycle Learning Framework

### 3.3.3 Innovation in the "Promoting Learning through Competitions and Enhancing Abilities through Practical Operations" Model.

Innovate the practical teaching model, following a progressive approach of "basic skill training → competition topic practice → real-world environment refinement", to conduct network security analysis and practice. On the one hand, relying on the experimental resources of the training platform, gradually enhance students' practical abilities; on the other hand, actively organize students to participate in well-known domestic and international cybersecurity competitions such as the "Strong Network Cup", and introduce real-world network security analysis tasks into the curriculum, allowing students to refine their practical skills through practice.

In addition, a "competition-learning mutual nurturing" mechanism has been established, which integrates excellent problem-solving ideas and techniques from competitions into classroom teaching. Real network security cases discovered by students are transformed into teaching resources, forming a virtuous cycle.

## 3.4 Evaluation Feedback Dimension: "Process-Oriented + Diversified + Capability-Driven" Comprehensive Evaluation Innovation

Revolutionizing the traditional singular outcome-based evaluation approach, a comprehensive evaluation system featuring "process-oriented, diversified, and capabil-

ity-driven" has been established[5] (As shown in Figure 4). Process evaluations employ various forms: security debugging and analysis assignments assess students' technical practical abilities; research-based practical projects evaluate students' innovative thinking and scientific research capabilities; pre-class self-study tests gauge students' autonomous learning effectiveness; and classroom question answering and discussion participation reflect students' classroom engagement[10]. These diversified process evaluation methods comprehensively track students' learning processes and developmental trajectories.

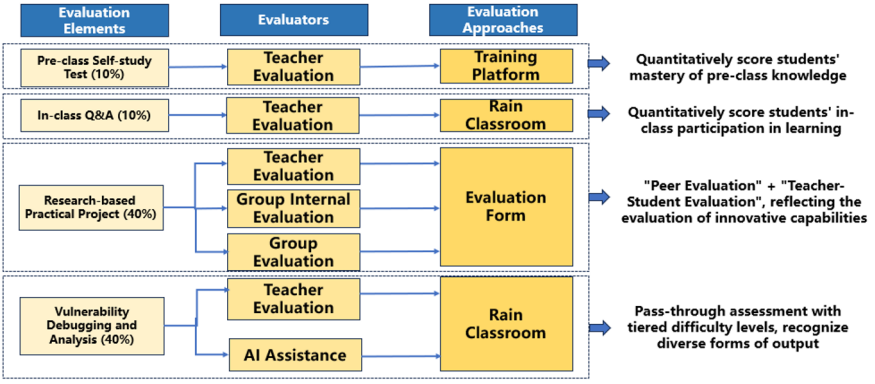


**Fig. 4.** Composition of Process Assessment Scores

The summative evaluation primarily consists of subjective and open-ended questions, emphasizing the assessment of students' proficiency in flexibly applying knowledge and their ability to tackle complex problems. The design of the test questions underscores contextualization and practicality, demanding that students comprehensively utilize their acquired knowledge to analyze real-life network security cases and propose solutions, thereby reflecting the effectiveness of cultivating higher-order thinking skills.

## 4 Implementation Outcomes and Dissemination

Since its implementation, this innovative teaching system has achieved remarkable multi-dimensional outcomes in terms of student development, teaching improvement, and social influence, which fully validates the effectiveness and advancement of the “Three-dimensional Intelligence Integration and Capability Leap” model for cybersecurity talent cultivation. In terms of student performance, systematic training has significantly enhanced students’ theoretical knowledge, practical skills, and innovative capabilities.

In regard to teaching development and reform promotion, the system has effectively elevated the professional level of the teaching team and the quality of curriculum construction. The teaching team has presided over provincial and ministerial teaching reform projects, won multiple provincial teaching achievement awards, and cultivated

several outstanding teachers with high-level academic titles. Meanwhile, the teaching resources and innovative model have been adopted by multiple universities, and the reform experience has been shared through educational papers and international conferences, resulting in prominent social benefits and extensive industry influence.

## 5 Conclusion

The "Three-Dimensional Intelligence Integration and Capability Leap" teaching innovation system constructed in this paper has effectively addressed common challenges in the teaching of network security analysis courses through systematic teaching reforms and practices. It has facilitated a leapfrog development for students, transitioning them from knowledge acquisition to capability building, and ultimately to practice capability generation. Teaching practice has shown that this model has achieved remarkable results in enhancing students' practical skills, innovative thinking, and professional ethics.

However, with the rapid development of artificial intelligence technology and the increasingly complex cybersecurity landscape, curriculum construction still faces new challenges and opportunities[11]. Moving forward, we will focus on continuously deepening teaching reforms in the following aspects:

(1) Deepen AI technology empowerment: comprehensively carry out curriculum reforms empowered by AI, and focus on building high-quality AI courses; construct a vertical large model in the field of network security analysis, develop an intelligent curriculum resource framework based on digital human technology, and create an immersive and interactive intelligent learning environment.

(2) Optimize the practical teaching system: Conduct in-depth research on the actual needs of positions, optimize and update immersive course scenarios, create a practical teaching system that better meets the job requirements, and further enhance the relevance and adaptability of talent cultivation.

(3) Expand international cooperation and exchange: Strengthen cooperation and exchange with internationally renowned universities and security institutions, introduce international cutting-edge curriculum resources and teaching concepts, and enhance the internationalization level and influence of curriculum construction.

(4) Improve the evaluation and feedback mechanism: Establish a more scientific and comprehensive learning evaluation system, introduce learning analytics technology, achieve precise monitoring and evaluation of the learning process, and provide data support for teaching improvement.

Through continuous innovation and improvement, we aspire to build this course into a top-tier hub for cybersecurity talent cultivation both domestically and internationally, making greater contributions to the cultivation of cybersecurity talents in the new era.

## References

1. Guo Jianpeng. Flipped Classroom Teaching Model: Variation-Unification-Revariation [J]. China University Teaching, 2021, (6): 77-86.

2. Guo Jianpeng. Flipped Classroom Teaching Model: Variation and Unification [J]. China Higher Education Research, 2019, (6): 8-14.
3. Zhong Yuehui, Peng Weiqiang, Xie Weicong. Design of Online-Offline Hybrid "Golden Course" in Open Education Based on the Concept of "Consistent Construction" [J]. Guangdong Open University Journal, 2023, 32(4): 31-37.
4. Mei Tao. Design and Application Reflection of Flipped Classroom in University "Aesthetics" Course [J]. Education and Teaching Forum, 2025, (31): 17-20.
5. Wang Yunlu, et al. Research on the "Thinking-Teaching-Production-Evaluation" Four-in-One Evaluation System for Innovative Practical Ability of Cyberspace Security Talents [J]. Evaluation and Management, 2023, (3): 38-41, 54.
6. Ma Zhiqiang, et al. Application Analysis of DeepSeek in Domestic Universities: Policy Drive, Scenario Practice, and Risk Response [J]. China Education Informatization, 2025, 31(4): 23-33.
7. Zhu Biao Kai, et al. Practical Research on "Dual-Track" Hybrid Teaching Reform in the Context of Big Data: A Case Study of Cybersecurity and Law Enforcement [J]. Higher Education Journal, 2024, (22): 136-139.
8. Li Chunyuan, et al. Research and Practice on the Cultivation Model of Cybersecurity Graduate Talents Under the Background of Emerging Engineering Education [J]. Heilongjiang Education, 2024, (5): 84-87.
9. Zhang Lyuyang, et al. Innovation and Practice of a Talent Cultivation Model Integrating Science and Education in Cybersecurity [J]. Information Security Research, 2023, 9(9): 921-927.
10. Yuan Jie, et al. Research on the Quality Evaluation System of Cyberspace Security Talent Cultivation [J]. Industry and Information Technology Education, 2025, (9).
11. Yimei Yang, et al. Research on China's Innovative Cybersecurity Education System Oriented Toward Engineering Education Accreditation [J]. Information, 2025, 16(8): 645.
12. Cong Liu, et al. The Application of Artificial Intelligence in Engineering Education: A Systematic Review [J]. IEEE Access, 2025, 13: 17895-17910.