

Exploration and Practice of a Graded, Flat, and Flexible Teaching Model for Cultivating Cyber Defense and Offense Capabilities

Hui Shu^{1, a}, YunTian Zhao^{1, b *}, Fei Kang^{1, c} and WenJuan Bu^{1 d}

¹ Information Engineering University, Cambridge, Zhengzhou, China.

^a shuhui123@126.com, ^b yuntianzhao1105@163.com, ^c kfminnie@163.com,

^d buwenjuan_521@163.com

Abstract. In alignment with the educational requirements for the multifaceted nature of knowledge, the comprehensiveness of skills, the adversarial nature of practice, and the specificity of thinking in cyber defense and offense capabilities, this paper adopts a student-centric pedagogical philosophy. Guided by educational theories such as constructivism, connectivism, and group dynamics, we have established a graded, flat, and flexible teaching model. This model is characterized by a progressively challenging teaching framework, the construction of contextually linked case scenarios through a flat knowledge network, the organization of a multidimensional and elastic teaching process, and the support of skill training through multimodal hybrid collaboration. It synergistically transforms the relationship between teaching and learning across four dimensions: framework structure, content arrangement, process organization, and training methods. This systematic shift has led to a significant increase in the knowledge capacity and diversity of the curriculum, an optimization of the flexibility and adaptability of teaching organization, an enhancement of students' understanding and learning capabilities, an improvement in students' comprehensive skills and practical combat effectiveness, and the stimulation of innovative thinking and specific cognitive traits.

Keywords: cyber defense and offense capabilities, teaching model, flat knowledge links, adversarial practice, specialized thinking.

1. Introduction

Cyber defense and offense capabilities constitute the core essence of talent cultivation in the field of cybersecurity. Distinguished from traditional professional skill development, these capabilities encompass four fundamental attributes: the diversity of knowledge, the comprehensiveness of skills, the adversarial nature of practice, and the specificity of thought. The diversity of knowledge refers to a broad foundation that includes multidisciplinary areas such as computer science, security, cryptography, and communications, characterized by a complex structure and extensive content[1][2]. The comprehensiveness of skills indicates the necessity for an integrated application of various abilities in practical training, including system reverse engineering, code programming, vulnerability analysis and exploitation, software reverse engineering, algorithm analysis, and tool utilization[3][4]. The adversarial nature of practice highlights the constant strategic interaction and competition between opposing parties, which inherently requires the flexible and combined application of foundational skills[5]. Lastly, the specificity of thought suggests that the actual process of cyber confrontations often lacks a straightforward logical sequence, with the resolution of critical issues relying on unique cognitive methods such as 'formative thinking', 'leap thinking', 'inverse thinking', and 'bypass thinking'.

Teaching and training in cyber defense and offense capabilities require a gradual process that solidifies a multidisciplinary knowledge base, enhances the comprehensive application of skills, intensifies the rigor of practical confrontation, and stimulates unique thinking methods, thereby continuously improving the level of offensive and defensive capabilities. However, current conventional teaching and training models fall short of meeting these cultivation requirements, as reflected in four areas of 'inadequacy': First, the modular course structure, which combines knowledge units, fails to meet the integrated teaching needs of diverse knowledge. Second, the

assembly-style training model, which focuses on singular skills, does not meet the integrated training requirements for comprehensive skills. Third, the fragmented and one-sided teaching cases of offensive and defensive separation do not meet the practical confrontation capabilities cultivation oriented towards real combat. Fourth, the straightforward and procedural heuristic teaching does not meet the cultivation requirements for inspiring unique thinking.

The essence of the problem lies in a lack of profound understanding of the special nature of cyber defense and offense capability cultivation, a failure to systematically implement the advanced educational philosophy of 'student-centeredness'[6][7], and an inaccurate grasp of the core lever of capability construction through knowledge linkage. As a result, the teaching mode follows a step-by-step approach and is constrained by the overall distribution of teaching hours, leading to inefficiencies in the organization and arrangement of teaching content, the design and control of the teaching process, and the planning and deepening of teaching practice, resulting in low teaching efficiency, poor training effects, and insufficient capability cultivation.

This research establishes the GFF(Graded, Flat, Flexible) teaching model, characterized by a progressive difficulty framework, contextual case construction with flat knowledge links, multi-dimensional flexible process organization, and multi-modal collaborative capability training support. This model synergistically transforms the relationship between teaching and learning across four levels: framework structure, content arrangement, process organization, and training methods. It effectively implements a student-centered teaching philosophy, significantly enhancing teaching efficiency and quality with both theoretical significance and practical value.

2. GFF(Graded, Flat, Flexible) Teaching Model

We have conducted exploratory research and in-depth practical implementation in the reform of the teaching model by focusing on four key areas: proposing a novel teaching paradigm, reshaping the structure of teaching content, optimizing teaching organization methods, and innovating in teaching practice models.

2.1 Creating a GFF Teaching Model

Innovation in teaching models must be preceded by theoretical research. Constructivist educational perspectives posit that knowledge is a product of learners' construction and interpretation within contexts[8]-[11]. Students transition from being passive recipients of information to active processors, shifting from objects of knowledge dissemination to constructors of knowledge meaning. The core of the scientific method for knowledge construction based on the "student-centered" approach lies in three key elements:

- **Meaning:** This involves enabling students to deeply recognize the significance of knowledge, thereby gaining the motivation to learn and understanding the need for learning.
- **Context:** This entails learning within contexts to enhance interest, comprehend the application of knowledge, and grasp its essence.
- **Collaboration:** This encourages collaborative learning within teams to improve efficiency, reinforce immediate complementary capabilities, and foster mutual inspiration across diverse roles.

Connectivist learning theory views learning as the process of establishing and reconstructing knowledge nodes and relationships within a network structure[12]-[14]. Contextual cases that encapsulate the intrinsic logical structure of knowledge can facilitate students' internalization of a unique cognitive schema in the field of defense and offense. This not only aids in knowledge acquisition but also in mastering learning methods and enhancing learning capabilities.

Group dynamics theory[15]-[17], although a mature theory and method for studying group behavior development in the field of social psychology, can be aptly applied to teaching as a methodological guide for the autonomous learning advocated by constructivist education. This includes clear goals, role division, defined responsibilities, interest stimulation, and communication.

Based on these theories, we created a GFF teaching model, as illustrated in Figure 1.

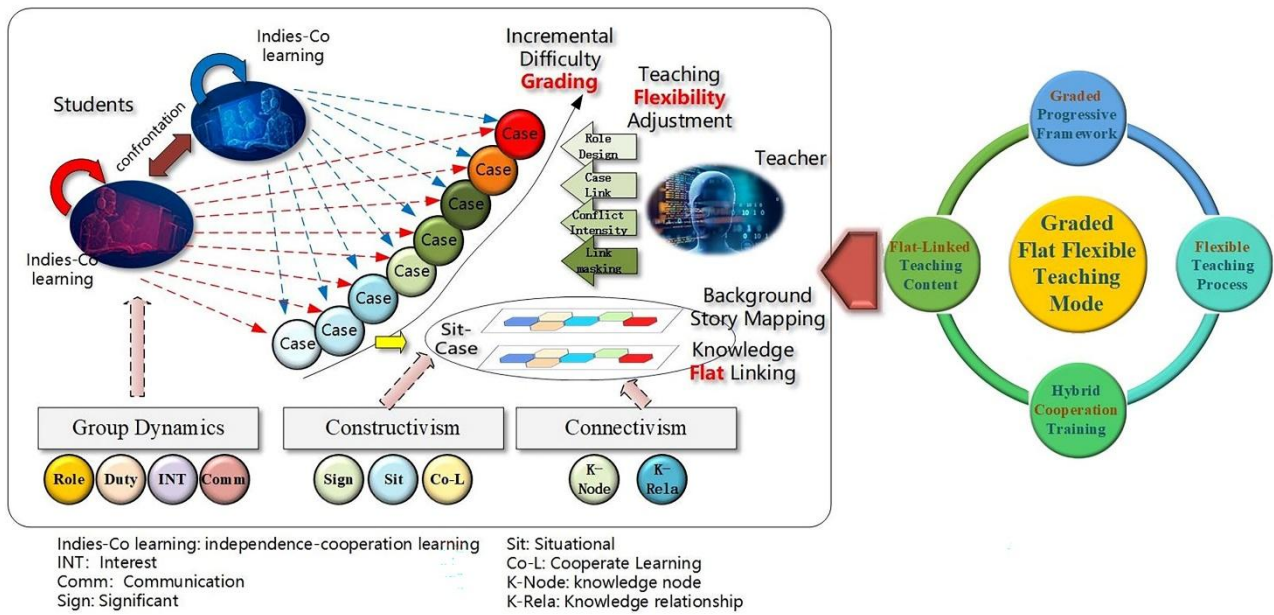


Fig. 1 GFF Model

The essence of a flat structure lies in the interconnectedness of multiple knowledge points, which forms the core principle of teaching scenario design. Grading is based on the fundamental pedagogical principle of gradual progression, guiding the learning of cases from basic to advanced levels, and from simplicity to complexity. Flexibility reflects the dynamic regulation of the learning process by teachers according to the students' learning conditions.

In the cultivation of cyber defense and offense capabilities, the leading role of teachers is not manifested in the direct imparting of knowledge and teaching of skills, but in the design of scenario cases rich in knowledge linkages, the construction of a well-connected group of scenario cases, the flexible arrangement and regulation of the teaching process, and the heuristic guidance of knowledge and skill learning. Concurrently, students truly become the subjects of learning, conducting collaborative inquiry-based learning autonomously under the guidance of teachers, and continuously enhancing their skill levels.

2.2 Constructing Contextual Case Groups Based on Malicious Sample Screening

Guided by the new teaching paradigm, the design of a teaching scenario case must encompass background, context, a collection of knowledge points, and flat relational links, thereby forming a situational teaching plane. A group of teaching cases that meet the overall teaching and training requirements for cyber defense and offense capabilities is composed of numerous situational teaching planes (teaching cases) that are rich in knowledge, progressively skillful, and naturally interconnected. The design of a scientifically sound and rational graded flat case group has become a key issue in research.

In the field of cybersecurity, the MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework is a widely recognized and authoritative model for depicting cyber attack tactics and techniques[18]. It defines a comprehensive knowledge system for cyber defense and offense, dividing attacks into 14 interlocking and closely related tactical stages, from reconnaissance to impact. For each tactic, it summarizes all known techniques of cyber attacks, totaling over 240, and provides corresponding defensive strategies and methods for each type of technique. Guided by the ATT&CK model is an inevitable choice for case design.

From the perspective of the ATT&CK model, the continuous eruption and evolution of malicious code in cyberspace are the automatic realization of cyber attack techniques under specific intentions, the natural linkage of battle technique knowledge points at different levels and with related attributes, and the technological innovation driven by the critical importance in the multi-intensity offensive and defensive game. Each outbreak and demise of typical malicious code

is a fascinating story related to the discovery, exploitation, and mitigation and repair of vulnerabilities in cyberspace. Therefore, using malicious code as the prototype for case design perfectly fits the core concepts of meaning construction and situational design under the constructivist educational view and is the best material for case design.

We combine automated reverse analysis technology of malicious code and AI-based code screening technology to extract battle techniques from 2TB of collected malicious code samples. According to the diversification of knowledge, the complexity of technology, and the difficulty of offense and defense, the samples are graded, classified, and selected to extract 108 malicious code case examples, including 10 categories such as Bootkit and Rootkit, macro viruses, file viruses, ransom and mining viruses, Android viruses, Trojans, script viruses, worms, atypical viruses, and advanced APT malicious samples. By organizing case elements, including offensive and defensive task scenarios, a collection of knowledge points, knowledge point difficulty, analysis and practical operation tool collection, analysis skill collection, analysis complexity, tool operation comprehensiveness, programming skill collection, programming language and environment, programming complexity, and knowledge point coupling degree, a group of teaching cases and corresponding teaching materials have been formed. Overall, it covers all known cyber attack techniques, with each case having a focused special battle technique knowledge link, explicit differentiation between different cases in technical knowledge points, and the technical upgrades and evolution of malicious code as the connecting surface for different cases. At the same time, the project team has divided knowledge points according to the difficulty of offense and defense, as the grading criteria for malicious code cases, making the case group orderly and organized in a progressive manner, facilitating the gradual teaching work. Figure 2 shows the number of knowledge points of different basic difficulties in the current case group.

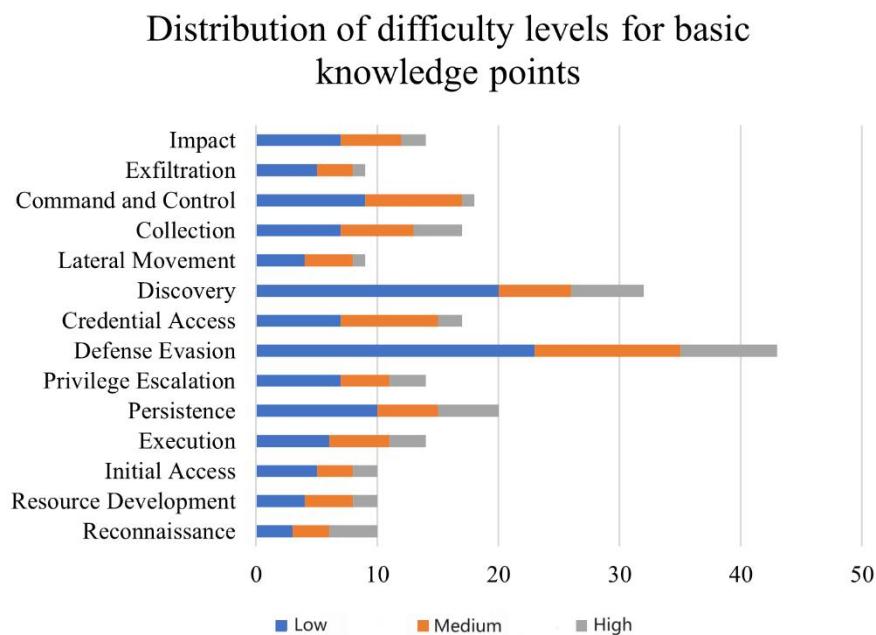


Fig. 2 Knowledge Point Basic Difficulty Distribution.

2.3 Organizing Multi-dimensional Contextual Case Flexible Teaching

The innovative graded flat case group provides a foundational content basis for innovative teaching activities. The regulation and organization of the teaching process around the case are key to enhancing teaching efficiency and effectiveness, representing a significant challenge to the teacher's own offensive and defensive professional capabilities, as well as their ability to flexibly arrange and organize teaching activities.

Inspired by group dynamics theory, we regard the student group as a "learning community" and extract six elements that optimize group learning behavior: goals, roles, responsibilities, interests, communication, and cohesion. To this end, we have designed a basic situational case teaching organization method: based on the teaching class, the teacher first lectures to the students on the case background, points out the basic knowledge points around the case, and clarifies the teaching goals and offensive and defensive responsibilities of the case. On the one hand, the case background stimulates the students' curiosity and interest in learning, and on the other hand, it allows students to understand the basic learning path and practical methods. Then, according to the characteristics of the case's offensive and defensive confrontation, the class students are organized into red and blue teams to carry out cooperation and confrontation around the target system and reverse analysis of malicious code, offensive and defensive code programming, and tool operations. At the same time, based on the students' knowledge foundation and ability, combined with the offensive and defensive stages, students are assigned situational roles, that is, each student focuses on specific knowledge points in the learning process of the case, and through cooperation and communication with other students, takes into account other knowledge points in the case. After completing the cooperative offensive and defensive arrangements, students conduct exploratory learning and discussion through independent cooperative research and practice, and jointly complete the construction of knowledge links and systems. In each round of situational case learning, the teacher is the behind-the-scenes organizer, confidence supporter, and team cohesion enhancer of group learning. More importantly, through "key points" guidance, the learning role is guided to strengthen "learning confidence," traverse "knowledge fog," and get out of the "situational predicament." The teacher guides the students to deeply understand the meaning of the knowledge at each stage of offensive and defensive in a step-by-step learning process, and to master the learning methods and corresponding skills in the overall knowledge construction.

To enhance the flexibility and efficiency of teaching organization, the project team has integrated an adaptable organizational approach into the basic situational case teaching method, which is reflected in four specific aspects:

- **Adaptive Role Assignment:** Considering the varying foundational abilities of students, the project team flexibly adjusts the roles in collaborative learning. In situational case teaching, role assignment clarifies the key knowledge and skills to be learned. Teachers must accurately understand the students' foundations and their grasp of specific knowledge points during teaching, and timely assign different roles. This ensures that each student covers different aspects of the knowledge points in the case group learning and allows students of varying abilities to follow an optimized learning path tailored to their individual needs.
- **Adjustment of Case Progression:** In response to the learning pace of students' offensive and defensive knowledge, the project team moderately adjusts the pre-set connections between cases. It has been observed that the learning curves of different classes vary, and the pre-set case collections may involve some repetitive learning or too large a span, making it difficult to adapt to actual teaching. Teachers need to select appropriate subsequent cases from the situational case group based on the overall learning situation of the current case, supporting a smooth upward curve of knowledge and skill learning.
- **Regulation of Adversarial Intensity:** Based on the observation of students' "wolf-like" spirit in offensive and defensive games, the project team dynamically adjusts the intensity of the situational case confrontation. Teachers need to leverage their understanding of cyber offensive and defensive knowledge and difficulty, as well as their practical experience in combating a large number of malicious codes. They should adjust the difficulty of the knowledge points in the current situational case and intensify the confrontation according to the "hunger" and "passion" of the student group and individuals. This stimulates the students' enthusiasm for overcoming difficulties, enhances their practical combat capabilities, and also helps guide students out of the fatigued learning troughs in the learning cycle.

- **Innovation in Knowledge Linkage:** To meet the training requirements for students' innovative thinking, the project team randomly conceals knowledge links in situational cases. The training and cultivation of specific thinking are challenging issues in teaching research. Inspired by the self-supervised concealment training methods in the field of artificial intelligence, the project team, based on the flat knowledge linkage of situational cases, moderately and randomly conceals knowledge points and links in the case during the advanced learning stage. This encourages students to reconstruct the knowledge links of the case using formative, speculative, detour, and bypass thinking modes, or to independently explore and discover new linkage paths, thereby activating thinking and enhancing the innovation of learning.

2.4 Practicing Hybrid Collaborative Cyber Offense and Defense Training

The meticulously crafted and orchestrated cases provide the designed scenarios and learning objectives for capability training, while the state-of-the-art practical training platforms offer a collaborative learning scaffold for students to climb towards their goals. The project team relies on the teaching and experimental environment to support the mixed collaborative practical training for the cultivation of offensive and defensive capabilities, with specific practices as follows:

- **Practical Training Condition Assurance:** We have customized 108 sets of virtualized network scenarios and virtual node operating environments for the collection of malicious codes in the case group, providing a knowledge base and supporting verification environment for self-directed learning of malicious code expertise, and equipped with a CTF-based training process supervision and role skill scoring scheme, laying a solid environmental foundation for offensive and defensive capability practical training. Relying on environments for malicious code development, reverse analysis, multidimensional detection, and confrontational analysis, we have provided students with the necessary analysis and development environments for practical case scenarios.
- **Mixed Collaborative Practical Training:** Guided by the GFF teaching model, we organize students into red and blue teams, and assign roles according to the stages of offensive and defensive tactics. Red team students, in line with the case scenarios, carry out the development, integration, and verification of malicious code in a modular team collaboration manner. Blue team students, also in line with the case scenarios, collaborate on defensive tasks such as code reverse engineering, log analysis, protocol detection, and defense rule setting. Teachers observe the progress of each role through the competition system, assess the progress of capabilities, and provide immediate guidance to red and blue team students, organizing online exchanges. In each round of case training, the red and blue team grouping and role division are mixed and arranged, guiding the ability to improve step by step.

3. Application Practice

We have adopted an iterative research and development approach, leveraging the course 'Principles and Detection of Malicious Code' as a focal point. We have designed a new curriculum structure based on a teaching model that rationally arranges knowledge points, naturally connects cases, and gradually increases difficulty. We have completed the design of 108 typical situational cases of malicious code and continuously optimized the flexible teaching organization model. This model has been actively applied in practice among 12 batches of third-year undergraduate students majoring in Cyberspace Security, achieving significant teaching effects in improving students' learning efficiency and capabilities.

As shown in Figures 3 and 4, after adopting the GFF teaching model, each student has mastered an average of 20-30 situational cases and nearly 160-190 offensive and defensive knowledge points. Moreover, the learning cycle for case studies has been significantly shortened as the teaching

progresses, and the overall volume of knowledge learned is more than 2.8 times that of traditional teaching models. The comprehensive offensive and defensive skills, centered around reverse analysis, vulnerability exploitation and mitigation, shell scripting and parsing, script development and detection, network penetration and prevention, and host attack and defense, have been significantly enhanced in various types of scenarios and environments.

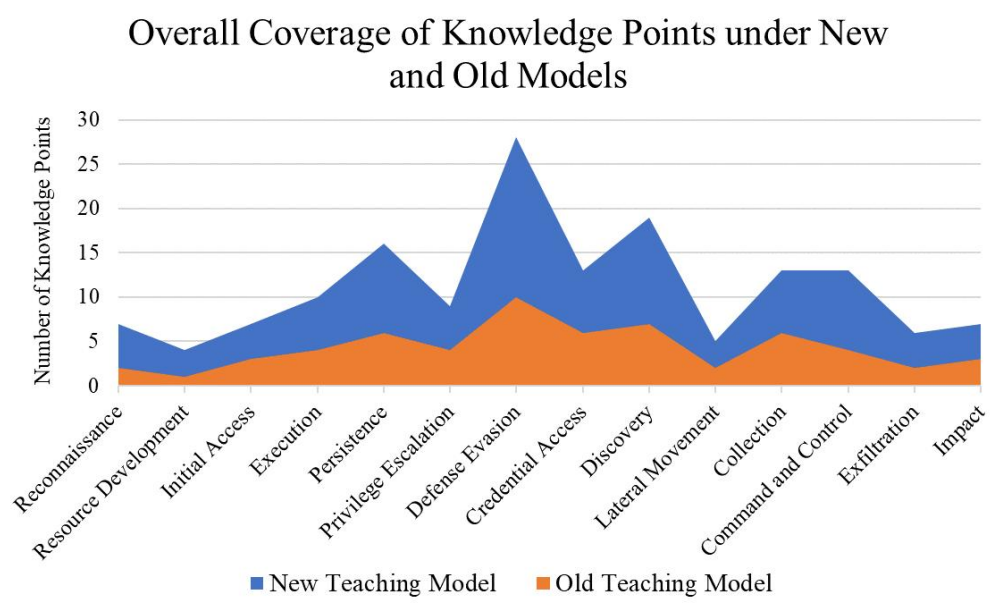


Fig. 3 Coverage of course knowledge points under the guidance of New and Old Teaching Models

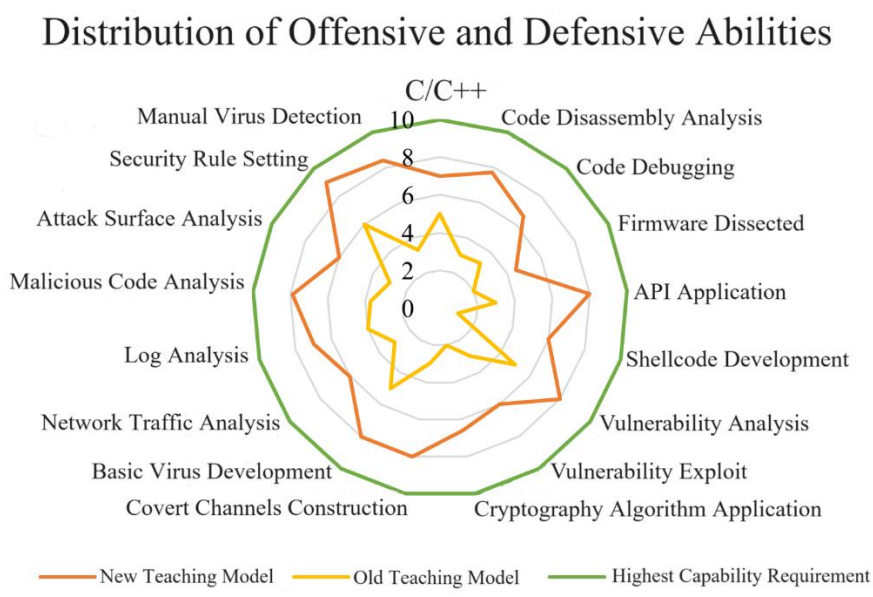


Fig. 4 Comprehensive Skills Training under the Guidance of New Teaching Models

4. Summary

The GFF teaching model, guided by contemporary educational theories, represents an innovative approach to education. It significantly expands the knowledge capacity and diversity of the curriculum by providing a graded progression of situational case groups. By encouraging collaborative learning within these flat-structured, interconnected knowledge scenarios, the model enhances students' understanding and integrated application of knowledge. The efficiency of teaching activities is improved through flexible adjustments, particularly by modulating the intensity of confrontation to enhance combat capabilities and by concealing knowledge links to

stimulate innovative thinking, which are considered 'masterstrokes' within the teaching model. Furthermore, mixed collaborative practical training consolidates practical skills. The introduction of this model profoundly transforms the relationship between teaching and learning, fully mobilizing and stimulating the self-learning of student groups, thereby fundamentally enhancing teaching efficiency. It holds significant theoretical guidance and practical application value for the cultivation of cyber defense and offense capabilities.

References

- [1] Zhao, Guosheng, et al. "Exploration of the Collaborative Education Model for Cyberspace Security Talents in the Context of New Engineering Based on Unity of Knowledge and Action." *Curriculum and Teaching Methodology* 6.20 (2023): 79-83.
- [2] Bin-Xing, Fang. "A hierarchy model on the research fields of cyberspace security technology." *Chinese Journal of Network & Information Security* (2015).
- [3] The Cyberspace Security Talent Education Alliance of China. "Guidelines for the Training System of Technical Talents in Cyberspace Security Engineering (Version 2.0) (in Chinese)". 2019.
- [4] Cabaj, Krzysztof, et al. "Cybersecurity education: Evolution of the discipline and analysis of master programs." *Computers & Security* 75 (2018): 24-35.
- [5] Schneider, Fred B. "Cybersecurity education in universities." *IEEE Security & Privacy* 11.4 (2013): 3-4.
- [6] Amri, Faisal, and Nur Ekaningsih. "ENHANCING STUDENTS' COGNITIVE ABILITIES THROUGH STUDENTS-CENTERED LEARNING (SCL)." *Kajian Linguistik Dan Sastra* 2.2 (2018): 141-146.
- [7] JuMing Zhao. "Open the Black Box: The Scientific Basis of Learning and Development - Research on Student Centered Undergraduate Teaching Reform in the United States Part 2 (in Chinese)". *Research in Higher Education of Engineering*. Issue 3, 2017.
- [8] O'Connor, Kate. "Constructivism, curriculum and the knowledge question: tensions and challenges for higher education." *Studies in Higher Education* 47.2 (2022): 412-422.
- [9] Fatimah, Siti, Didin Nurul Rosidin, and Abas Hidayat. "Student-based learning in the perspective of constructivism theory and Maieutics method." *International Journal Of Social Science And Human Research* 5.5 (2022): 1632-1637.
- [10] Efgivia, M. G., Rinanda, R. A., Hidayat, A., Maulana, I., and Budiarto, A. "Analysis of constructivism learning theory." *1st UMGESHIC International Seminar on Health, Social Science and Humanities (UMGESHIC-ISHSSH 2020)*. Atlantis Press, 2021.
- [11] KeKang He. "Constructivism - Theoretical Basis for Reforming Traditional Teaching (Part 1). (in Chinese)" *E-education Research* Issue 3, 1997.
- [12] Alam, A. "Connectivism learning theory and connectivist approach in teaching and learning: a review of literature." *Bhartiyam International Journal Of Education & Research* 12.2 (2023).
- [13] Downes, Stephen. "Connectivism." *Asian Journal of Distance Education* 17.1 (2022).
- [14] HaiPeng Wan, ShengQuan Yu, and Qi Wang. "Connected Construction: A New Direction in Knowledge Construction Research. (in Chinese)" *E-education Research* 42.10(2021):12-18,24.
- [15] Levi, Daniel, and David A. Askey. *Group dynamics for teams*. SAGE publications, 2020.
- [16] Sweet, Michael, and Larry K. Michaelsen. "How group dynamics research can inform the theory and practice of postsecondary small group learning." *Educational Psychology Review* 19 (2007): 31-47.
- [17] HongJian Liao, and Qi Zhuang. "Preliminary exploration of the application of group dynamics in online collaborative learning. (in Chinese)" *Modern Distance Education* 000.004(2005):30-32.
- [18] ATT&CK v14. <https://attack.mitre.org/>. October 2023.