

AI-Empowered Restructuring of the Security Curriculum Cluster for Network Engineering Programs in Private Universities: A Case Study of Guangdong Neusoft University

Zhikai Li, Minjun Dai, Yingying Cai, Jiali Yi, Changfeng Wu

Neusoft Institute Guangdong, Foshan 528000, Guangdong, China

Copyright: © 2026 Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), permitting distribution and reproduction in any medium, provided the original work is cited.

Abstract: Facing challenges of lagging curriculum updates, fragmented articulation, isolated practice teaching, and distorted evaluation, this paper interprets AI-empowered curriculum cluster restructuring from demand-side sensing, capability mapping, and data feedback, constructs a “five-in-one” framework linking AI-based dynamic sensing, capability map modeling, cluster restructuring, smart teaching implementation, and data-driven evaluation, and proposes an implementation path covering demand sensing, a four-module curriculum system, core-course restructuring, three-tier AI usage norms, and closed-loop evaluation, offering a reference for application-oriented cybersecurity talent cultivation in private universities.

Keywords: Artificial intelligence; Private universities; Network engineering; Security curriculum cluster; OBE concept; Data-driven evaluation

Online publication: September 30, 2026

1. Introduction

Cybersecurity has become a critical foundation of national security and the digital economy, and cultivating cyberspace security professionals has been elevated to a national strategic priority^[1]. With the rapid evolution of artificial intelligence (AI) and big data, cybersecurity positions increasingly demand attack-defense practice, secure development, AI-tool collaboration, and engineering ethics rather than isolated knowledge. The *Outline for Building a Leading Country in Education (2024–2035)* proposes a composite “AI + X” training model, and private universities, as major providers of applied talents, must respond proactively in the security courses of network engineering programs.

Existing research covers national-strategic cultivation system design^[1], capability-oriented practice teaching^[2], OBE-based course restructuring^[3], reform under engineering education accreditation^[4], and

industry-integrated models ^[5], with the BOPPPS model applied in cybersecurity courses ^[6,7]. Studies on generative AI in education address AI-empowered higher education reform ^[8], AIGC-empowered course design ^[9], dynamic curriculum updating ^[10], and the normative “teacher–machine–student” collaborative classroom ^[11].

Overall, existing studies exhibit three limitations: they focus mostly on local reform of individual courses rather than cluster-level restructuring; AI is mostly positioned as a classroom aid, with its role in dynamic program adjustment underexplored; and schemes fitting the positioning of private universities and connecting “job demands–curriculum system–teaching implementation–evaluation feedback” remain scarce. Taking Guangdong Neusoft University as a case, this paper analyzes the dilemmas of the security curriculum cluster in private universities and proposes a “five-in-one” restructuring framework and its implementation path.

2. Realistic dilemmas of the security curriculum cluster

2.1. Static training programs and fragmented curriculum articulation

Security technologies and threat patterns evolve rapidly, yet private universities usually revise training programs on a four-year cycle, so course content lags one to three years behind, and adjustments rely mostly on teachers’ experience rather than systematic analysis of recruitment markets, certifications, vulnerability bulletins, and competition topics, widening the gap between static programs and dynamic industrial demands ^[12]. Meanwhile, the “three chains” within the cluster remain disconnected: on the knowledge chain, prerequisites are decoupled from core courses, hindering understanding of vulnerabilities such as SQL injection; on the capability chain, lecturing is separated from attack-defense scenarios; on the practice chain, experiments are disconnected from competitions, and isolated knowledge points can hardly form a joint force.

2.2. Isolated practice teaching and the absence of comprehensive attack-defense capability

Current practice teaching is dominated by single-point verification experiments, where students pass assessment simply by completing prescribed steps in the lab manual. Such training reproduces the exploitation of individual vulnerabilities, but students lack comprehensive capabilities in combined exploitation, lateral movement, defense hardening, and emergency response in real attack-defense scenarios. The attack-chain thinking and systematic defense design required by security positions can hardly be acquired through “follow-the-manual” experiments, so practice teaching needs to move from “single-point verification” to “comprehensive confrontation.”

2.3. Unregulated AI use and distorted teaching evaluation

Generative AI tools are entering classrooms rapidly, but most courses lack scientific usage norms: students over-rely on AI-generated results while neglecting principle comprehension and manual verification, weakening independent problem-solving. Traditional evaluation over-relies on attendance, lab reports, and final examinations, and can hardly capture attack penetration, defense hardening, teamwork, and engineering ethics. The interweaving of “how to use AI” and “how to evaluate” is a problem that curriculum cluster reform must confront.

3. Theoretical logic and overall framework of AI-empowered curriculum cluster restructuring

3.1. Triple theoretical logic

- (1) Demand side: the logic of AI-driven dynamic sensing. Traditional curriculum decisions rely on teachers' experience and scattered employment feedback, with dispersed and untimely demand signals. AI makes large-scale parsing of unstructured job data possible: text mining of recruitment information, certification syllabi, vulnerability bulletins, competition topics, and enterprise cases transforms dispersed demand signals into structured capability requirements, enabling the curriculum system to respond to industrial changes on a semester basis.
- (2) Supply side: the logic of capability mapping. The key lies in a stable mapping between job competencies and curriculum elements. The capability map takes "job competency–graduation requirements–course objectives–knowledge modules–experiment projects–evaluation indicators" as its skeleton, organizes fragmented knowledge points into an integrated network oriented toward learning outcomes, and provides a common baseline for content selection, experiment design, and resource gap identification, structurally resolving knowledge isolation and curriculum fragmentation.
- (3) Evaluation side: the logic of data profile feedback. The OBE philosophy requires learning outcomes to drive continuous improvement. Smart teaching platforms and virtual ranges enable full-sample collection of process data: AI transforms students' range operations, project development, and competition performance into multi-dimensional capability profiles, shifting evaluation from "result scoring" to "process diagnosis," and diagnostic results feed back into the adjustment of course objectives and teaching strategies, forming a closed loop of continuous improvement.

3.2. The "five-in-one" framework and basic principles

Based on the above logic, this study constructs a "five-in-one" framework of "AI-based dynamic sensing–capability map modeling–security curriculum cluster restructuring–smart teaching implementation–data-driven evaluation and feedback," forming a closed loop connected by data flow from industrial demands to learning outcomes. Four principles are followed: outcome orientation and reverse design, capability-driven cluster collaboration, human-AI collaboration with clear boundaries, and data-driven continuous improvement.

4. Implementation path of security curriculum cluster restructuring

4.1. Building an AI-driven mechanism for dynamic sensing of job demands

Focusing on typical positions such as penetration testing, security services, and security operations, multi-source data including recruitment information, certification requirements (CISP, NISP, OSCP), vulnerability bulletins, CTF topics, and graduate feedback are collected. An AI analysis engine performs keyword extraction, capability classification, and trend analysis to generate a "job competency change list" and "curriculum cluster adjustment suggestions" (see **Figure 1**), transforming lagging manual research into normalized data sensing that feeds into program optimization and content updating.

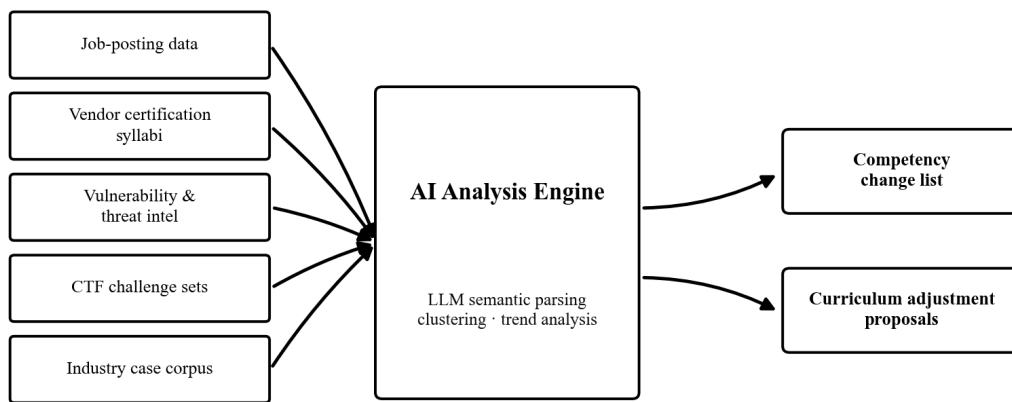


Figure 1. AI-driven dynamic sensing mechanism of job demands

4.2. Integrating the security curriculum cluster via capability mapping

On the basis of demand sensing, a vertical mapping of “job competency–graduation requirements–course objectives–knowledge modules–experiment projects–evaluation indicators” is established, and the curriculum cluster is restructured into four modules (see **Figure 2**). The foundational support module consolidates underlying knowledge for security practice; the core attack-defense module, centered on Web Security Technology and Network Attack and Defense, cultivates vulnerability analysis, attack-chain construction, and defense hardening; the AI security extension module introduces AI-assisted vulnerability mining and large model security; the comprehensive practice module carries integrated projects, competitions, and innovation training.

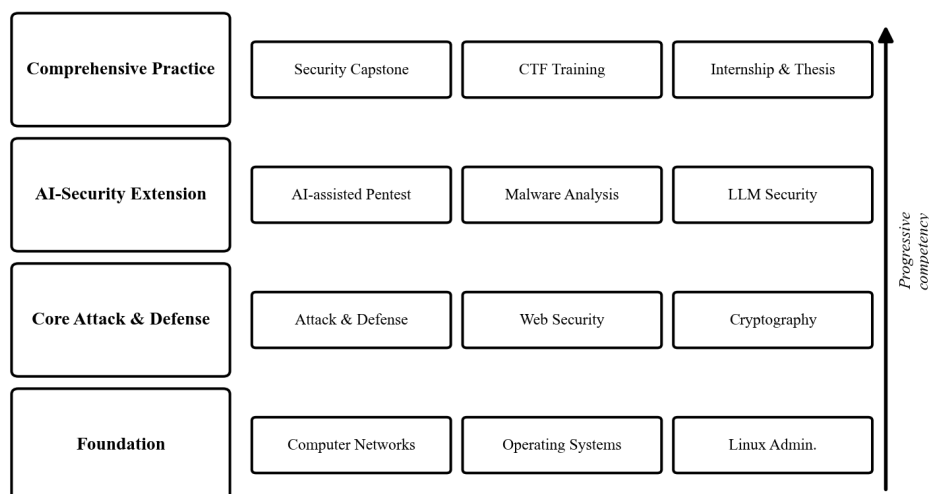


Figure 2. Four-module structure of the security curriculum cluster

4.3. Exemplary restructuring of core courses

Web Security Technology adopts a four-level progressive structure of “technology–tools–scenarios–design” (see **Figure 3**): from the principle analysis of core vulnerabilities such as SQL injection and XSS, to practical tools such as Burp Suite, Docker ranges, and AI code auditing, then embedding vulnerability knowledge into real business scenarios, and finally landing on security solution design tasks, achieving the capability leap from “being able to attack” to “being able to design.”

Network Attack and Defense constructs an “AI + BOPPPS + OBE” teaching model, integrating generative AI into the six BOPPPS phases and forming a teaching chain of “intelligent introduction–precise objectives–data-based pre-assessment–immersive participation–intelligent assessment–smart summary,” in which AI undertakes learning diagnosis, resource recommendation, and assessment feedback, while teachers focus on teaching design and value guidance.

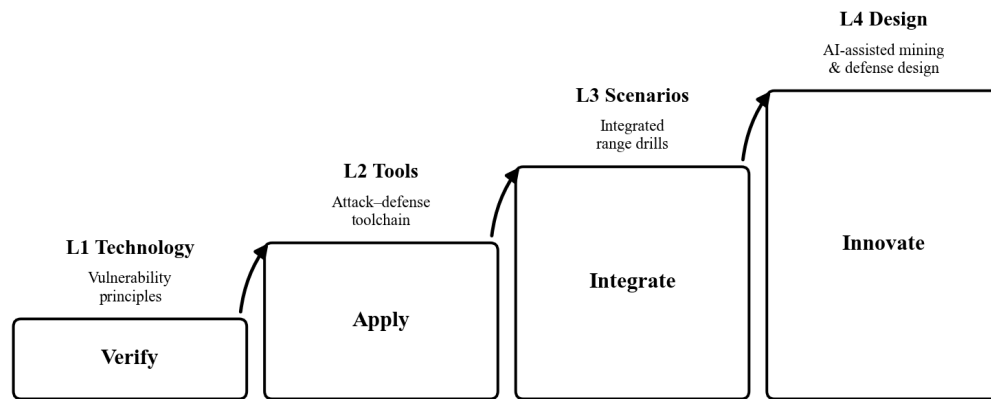


Figure 3. Four-level progressive structure of Web Security Technology

4.4. Establishing three-tier AI usage norms

AI use is divided into three tiers according to task nature, establishing a norm of “tiered constraints + process traceability” (see **Table 1**). The prohibited tier bans AI in basic tasks such as principle comprehension and attack-chain mapping to ensure independent thinking; the assisted tier covers command lookup and information retrieval to improve efficiency; the collaborative tier allows human-AI collaboration in comprehensive tasks such as script generation and vulnerability analysis, provided that prompts, AI outputs, and verification records are retained. This norm avoids “one-size-fits-all” prohibition, prevents students from bypassing the thinking process, and cultivates human-AI collaboration literacy through traceability.

Table 1. Three-tier AI usage norms for the security curriculum cluster

Tier	Applicable learning tasks	Role of AI	Constraints
Prohibited	Principle comprehension, attack-chain mapping, core concept discrimination	Prohibited	Independent completion, with key checks by teachers
Assisted	Command lookup, information retrieval, error explanation	Auxiliary tool	Scope of use must be specified
Collaborative	Script generation, vulnerability analysis, complex troubleshooting	Human-AI collaboration	Prompts, AI outputs, and manual verification and correction records must be retained

4.5. Constructing a dual-track practice system of “range attack-defense + project development”

The range attack-defense track advances through six stages of “basic cognition–single vulnerability–combined exploitation–attack-chain construction–defense hardening–comprehensive confrontation,” matching the capability objectives of core courses. The project development track takes real projects such as security tool development and hardening scripts as carriers to train secure development and engineering thinking. The two tracks support each other, connecting experiments, competitions, innovation projects, and graduation design, forming a practice ecosystem of “promoting learning through competitions and application through innovation.”

4.6. Establishing data-driven evaluation and continuous improvement mechanism

Relying on smart teaching platforms, virtual ranges, and project management tools, process data of ranges, projects, classroom interaction, and competitions are collected to build capability profiles covering attack penetration, defense hardening, script writing, teamwork, and ethical norms, supporting teaching diagnosis, personalized recommendation, and curriculum optimization (see **Figure 4**). Evaluation results serve not only for grading but also for reverse diagnosis of objective achievement, weak knowledge nodes, and resource gaps, forming a continuous improvement mechanism of “evaluation–feedback–adjustment–re-implementation.”

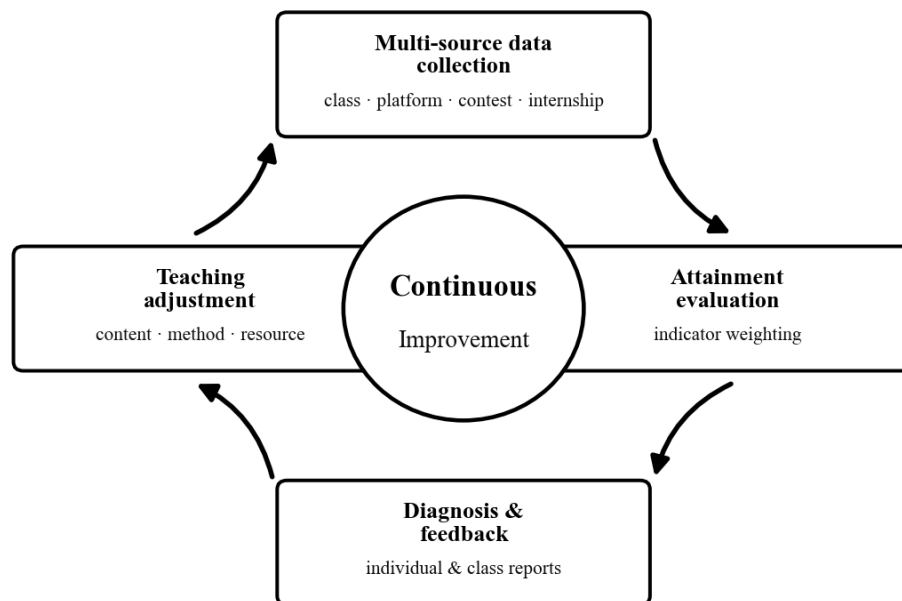


Figure 4. Closed loop of data-driven evaluation and continuous improvement

5. Conclusion and prospects

Aiming at the dilemmas of the security curriculum cluster in private universities, this paper interprets

the triple logic of AI-empowered restructuring, constructs a “five-in-one” framework, and proposes an implementation path, promoting the transformation of security curriculum construction from experience-based judgment to data-driven decision-making, from single-course reform to cluster collaboration, and from outcome evaluation to process diagnosis. The framework still faces challenges in maintaining capability maps and teaching resources, quantifying implicit capabilities such as attack-chain thinking, and dynamically adjusting the boundary of AI use. Future research will focus on automatic capability-map updating, profile validity verification, and empirical examination of reform effectiveness.

Funding

This work was supported by the 2026 annual projects of the Professional Committee for Teaching Quality Management of Private Higher Education Institutions, Guangdong Higher Education Teaching Management Association (GDZLGL26015, GDZLGL26019), and the 2026 Education and Teaching Research and Reform Project of the Guangdong-Hong Kong-Macao Greater Bay Area Universities Online Open Course Alliance (WGKM2026137).

Disclosure statement

The authors declare no conflict of interest.

References

- [1] Weng J, Wei LF, Zhang Y, 2019, Discussion on the Cultivation of Cyberspace Security Talents. *Chinese Journal of Network and Information Security*, 5(3): 44–53.
- [2] Yang H, Jiang LW, Xiong YT, et al., 2020, Construction of Practice Teaching System for Information Security Major Oriented to Capability Cultivation. *Computer Education*, (7): 87–93.
- [3] Zhang JL, Weng JS, Zhang YY, 2025, Research on Teaching Reform of the Operating System Principles Course Based on OBE Concept: Taking Cyberspace Security Major as an Example. *Journal of Higher Education*, 11(10): 81–84.
- [4] Chen ZP, Li H, Jia HM, et al., 2025, Teaching Reform of the Network Security Technology Course under the Background of Engineering Education Accreditation. *Computer Education*, (1): 60–65.
- [5] Su YP, Xiang YJ, Hua M, 2026, Research on Teaching Reform of the “Network Security Service and Management” Course in Civil Aviation Colleges Based on OBE Concept. *Wireless Internet Technology*, (6): 121–124.
- [6] Yuan J, 2024, Research on the Application and Practice of BOPPPS Model in the Network Security Technology Course. *Network Security Technology & Application*, (12): 106–108.
- [7] Pang YM, Li DD, Zhang JY, 2023, BOPPPS Whole-Process Teaching Design and Practice Empowered by Curriculum Resources: A Case Study of the Introduction to Information Security Course. *Journal of Beijing Electronic Science and Technology Institute*, 31(3): 99–107.
- [8] Gong X, Yang Z, Jing LB, 2026, AI Development Empowering Higher Education Reform: Theoretical Logic, Practical Dilemmas and Practical Paths. *Research on Higher Education in Heilongjiang*, (5): 17–22.
- [9] Liu C, Chen YH, Wang HF, 2026, AIGC Empowering Engineering Course Design: Opportunities, Challenges and

Countermeasures. *Science and Technology of Chinese Universities*, (6): 34–40.

- [10] Ma Y, Su Y, Li M, et al., 2025, Preparing Students for an AI-Driven World: Generative AI and Curriculum Reform in Higher Education. *Frontiers of Digital Education*, 2(4): 30.
- [11] Dai JT, 2025, Normative Value and Application Path of Generative Artificial Intelligence in Smart Teaching: A Case Study of the “National Security Rule of Law” Course. *Intelligent Higher Education*, (2): 81–94.
- [12] Han JY, Zhang MG, 2020, Research on the Project-Based Teaching Mode of Innovation and Entrepreneurship Based on OBE Concept. *Experimental Technology and Management*, 37(2): 209–211.

Publisher's note

Bio-Byword Scientific Publishing remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.