

From Discipline-Oriented to Competency-Based: Research on a "Broad-Spectrum and In-Depth" Training Model for High-Level Talents in Cyberspace Security

Yan Liu ^{a *}, Xiaoyu Guo and Ruixiang Li

¹ Henan Key Laboratory of Cyberspace Situation Awareness, Zhengzhou, 450000, China.

^a ms.liuyan@foxmail.com, ^b guoxy_ieu@outlook.com, ^c ruixiang_li@yeah.net

Abstract. With the formal establishment of cyberspace as the "fifth domain" following land, sea, air, and space, the training of cybersecurity talents has evolved from a mere focus on technical education to a critical component of national security strategy. However, current graduate education remains constrained by traditional discipline-oriented linear models, facing triple challenges of skill supply-demand mismatch, the paradox of broad employment prospects versus narrow research fields, and a lack of ethical awareness in the era of artificial intelligence. This paper proposes a shift towards a competency-based approach, constructing a "broad-spectrum and in-depth" training model for high-level talents. By establishing a flexible knowledge base, an ecosystem of research-application synergy embedded throughout the entire chain, and a layered cognitive defense system, the aim is to cultivate compound security experts with a solid foundation, practical sharpness, and clear ethical boundaries to address increasingly complex national security challenges.

Keywords: Cyberspace Security, Talent Training, Competency-Based, Broad-Spectrum and In-Depth, Research-Application Synergy.

1. Introduction

As cyberspace has been formally recognized as the "fifth domain," its strategic significance has become increasingly prominent. The competition in cyberspace ultimately boils down to a competition for talents. The training of high-level cybersecurity talents has transitioned from purely technical education to a strategic key link concerning national sovereignty and development. For graduate education, the critical challenge lies in cultivating compound experts who possess both profound theoretical knowledge and practical combat capabilities.

Since the establishment of cyberspace security as a first-level discipline in 2015, the scale of talent training in China has continued to grow, yet the supply-demand contradiction remains acute. According to the 2024 Cybersecurity Industry Talent Development Report released by the Ministry of Industry and Information Technology's Education and Examination Center^[错误! 未定义书签.], there is a significant shortage of compound talents with complex engineering problem-solving abilities, and a clear "scissor gap" exists between educational supply and industrial demand. In terms of theoretical exploration, the transition from knowledge imposition to a competency-based approach has become a trend. Internationally, frameworks such as NIST's NICE framework (Revision 1)^[2] have established a standard base centered on "Tasks, Knowledge, and Skills" (TKS). Domestic scholars like Zhang Huanguo^[3] and Feng Huamin^[4] have proposed numerous reform proposals targeting discipline independence and practical teaching. However, systematic solutions for balancing "broad-based general education" and "specialized research" at the graduate level remain insufficient.

Currently, the graduate training system primarily faces three lagging challenges on the educational supply side: first, knowledge supply lags behind technological iteration, leading students into a "tubular vision"; second, training mechanisms lag behind practical combat evolution, resulting in a disconnect between laboratory environments and real-world confrontations; third, value guidance lags behind technological impacts, leading to a deficiency in AI-era ethical and cognitive defense capabilities.

To address these dilemmas, this paper proposes a shift towards competency-based training, constructing a "broad-spectrum and in-depth" training model for high-level talents. This model aims to achieve a unity of broad-based foundations and specialized expertise in students through three pillars: establishing a flexible knowledge base based on competency diagnosis, embedding an ecosystem of research-application synergy throughout the entire chain, and constructing a layered cognitive defense system. Additionally, this paper designs implementation paths including credit substitution, physical university-enterprise platforms, and diversified evaluation to ensure the system's implementation.

The subsequent sections of this paper are arranged as follows: Section 2 reviews relevant research progress; Section 3 analyzes the training dilemmas; Section 4 elaborates on the construction of the "broad-spectrum and in-depth" system; Section 5 proposes implementation paths; and finally, a conclusion.

2. Literature Review

2.1 International Research Progress: Model Construction for Competency-Based Education

In the international context, cybersecurity education is undergoing a profound transformation from knowledge imposition to competency-based training. The Cybersecurity Workforce Framework (NICE Framework) released by the National Institute of Standards and Technology (NIST) in the United States represents a landmark achievement in this field. The framework, particularly its Revision 1, reconstructs traditional job description methods by standardizing the core elements of cybersecurity work into the "Tasks, Knowledge, and Skills" (TKS) system, providing a universal language and standard base for global cybersecurity talent training and evaluation^[2].

Based on the NICE framework, foreign scholars have actively explored its implementation paths in higher education. Multiple empirical studies have pointed out that traditional higher education courses often focus on theoretical knowledge transmission while neglecting skill training required for practical tasks. Scholars have proposed methods to map TKS indicators in the NICE framework to university course syllabi^[5] to clarify the competency outputs corresponding to each course, thereby significantly enhancing the match between graduates and job requirements. This provides crucial methodological support for the transition from a discipline-oriented to a competency-based teaching paradigm.

2.2 Domestic Research Progress: Local Exploration of Discipline Independence and Practical Paths

Research on cyberspace security talent training in China focuses on addressing the positioning issues during the initial stages of discipline construction and the practical ability training urgently needed by the industry.

In terms of discipline positioning and supply-demand contradiction analysis, since the establishment of cyberspace security as a first-level discipline in 2015, Zhang Huanguo, a pioneer in the field, has keenly pointed out that the discipline construction must guard against an "academicization" tendency. He emphasizes that cyberspace security possesses strong adversarial and engineering characteristics, and talent training cannot simply follow the path of traditional computer science, which emphasizes theoretical derivation. Instead, it should establish an independent knowledge system that integrates theory and practice^[3]. However, the existing training models still fail to fully adapt to industrial development. The 2024 Cybersecurity Industry Talent Development Report released by the Ministry of Industry and Information Technology's Education and Examination Center indicates that despite the continuous growth in the scale of cybersecurity talents in China, the supply-demand structural contradiction remains severe, particularly with a significant shortage of compound talents possessing practical combat capabilities and complex

engineering problem-solving abilities. The existing educational supply and industrial demand exhibit a clear "scissor gap"^[1].

In terms of practical teaching model reforms, addressing the chronic issue of emphasizing theory over practice, domestic scholars have proposed clear reform proposals. Feng Huamin, Secretary-General of the Cyberspace Security Teaching Steering Committee under the Ministry of Education (2021), conducted an in-depth analysis of the current state of national cybersecurity talent training, pointing out that universities generally suffer from static experimental environments and practical training scenarios detached from real-world combat. He advocates for the establishment of a practical teaching system based on real attack-defense scenarios^[4].

In terms of specific implementation paths, based on teaching practices at Beihang University, Liu Jianwei and Li Junxiong (2020) proposed a "full-cycle practical" teaching model. They advocate for the introduction of real enterprise cases and attack-defense simulation platforms to construct an integrated practice platform for "teaching, learning, practicing, testing, and evaluating" and implement a dual-mentor system involving both universities and enterprises to address the lack of practical experience among university faculty^[6]. Furthermore, to standardize the evaluation of practical abilities, the latest white paper released by the Cyberspace

Security Professional Teaching Steering Committee under the Ministry of Education (2024) further clarifies quantitative evaluation standards for cybersecurity talents' practical abilities, proposing that scientific measurements of students' security testing and evaluation capabilities should be conducted through simulation exercises, competition confrontations, and other means^[7].

2.3 Evaluation of Existing Research

In summary, existing research has laid a solid foundation for cybersecurity talent training: NIST has established international standards for competency models^[1], Zhang Huanguo has clarified the independent logic of discipline construction^[3], and Feng Huamin and Liu Jianwei have pointed out specific paths for practical reforms^[5-6].

However, existing research still has limitations: first, the deep application of competency models at the graduate level remains to be explored, with current reforms primarily focused on undergraduate skill training; second, although the Ministry of Industry and Information Technology's report points out the talent shortage, systematic solutions for balancing broad-based general education and specialized research are still insufficient. This paper aims to further construct a "broad-spectrum and in-depth" talent training system based on previous research to address these pain points.

3. Dilemma Analysis of Graduate Training in Cyberspace Security at Universities

3.1 Knowledge Supply Lags Behind Technological Iteration

The core characteristic of graduate education determines that it must delve deeply into specific sub-fields, such as having students focus on optimizing a particular type of encryption algorithm or deeply exploring a specific technical path in vulnerability mining. This narrow-field deep diving is a necessary prerequisite for cultivating research capabilities. However, real-world network attacks are never contests of a single technology but systemic confrontations involving multiple links and cross-domains. The adversarial nature of cybersecurity requires practitioners to possess a broad-spectrum vision and capabilities.

This contradiction leads to a direct phenomenon where many graduate students can achieve high levels in their specific research directions, publish high-quality academic papers, yet possess limited knowledge of general foundational technologies such as network resource mapping, network active defense, and software reverse analysis.

Some students even exhibit a state of fragmentation, where they "understand cryptography but not attack-defense, understand attack-defense but not operation and maintenance." More alarmingly, some students, due to long-term focus on a single domain, develop mental fixedness, hindering their ability to think from a cross-domain perspective.

The consequences are evident. This "tubular vision" leaves graduates, despite their high academic qualifications, facing numerous challenges in the workplace. When confronted with complex Advanced Persistent Threat (APT) attack chains, which often involve multiple stages such as multi-point breaches, lateral movement, and data exfiltration, requiring the integrated application of various technologies for judgment and defense, they often struggle to identify features beyond their specific expertise. This lack of holistic control and coordinated response capabilities traps them in a dilemma of "seeing the trees but not the forest," failing to meet the core needs of enterprises and national operational departments.

3.2 Training Mechanisms Lag Behind Operational Evolution

The essence of cybersecurity lies in high-intensity, dynamic confrontations between individuals. The iteration speed of attack-defense technologies is measured in days, and real-world confrontations are filled with uncertainties and noise. However, existing training mechanisms often isolate students in pristine laboratory environments, creating a false sense of prosperity detached from operational realities.

The most prominent issue is the disconnection between research topics and data sources from actual threats and pain points. Many graduate students' research topics originate from gaps identified through literature reviews rather than real-world threats. Experimental data often rely on publicly available datasets, which, after screening and standardization, have been stripped of the complexity and uncertainty present in real network environments, far removed from the actual traffic and attack scenarios encountered in enterprise intranets. Consequently, students trained in laboratory settings often lack training in emergency response and strategic gaming under high-pressure conditions.

The repercussions of this mechanism are that enterprises and national operational departments must bear the high cost of "secondary training." Many employers report that newly hired graduates, while theoretically sound, possess weak practical skills and operational awareness, requiring three to six months of specialized training before they can independently undertake tasks. Some even fail to adapt to real confrontational environments and are eliminated. More critically, models that perform well in laboratory settings often fail when deployed in real red-blue confrontation environments, unable to cope with variables such as complex noise and sudden changes in opponent strategies, becoming a core bottleneck restricting talent quality.

3.3 Value Leadership Lags Behind Technological Disruption

The rapid proliferation of AI technologies, such as large language models and deep fakes, is reshaping the landscape of cybersecurity attack-defense. On one hand, these technologies lower the barriers to generating malicious code and launching network attacks, significantly expanding the coverage and destructive power of cyber threats. On the other hand, new types of threats, such as cognitive warfare and public opinion manipulation, are emerging, posing higher demands on talents' value judgment and cognitive defense capabilities. However, the value leadership of traditional training systems has clearly failed to keep pace with this technological disruption.

For a long time, graduate training in cyberspace security has emphasized technical instruction, focusing core efforts on hard skill training such as algorithm optimization and attack-defense technology breakthroughs, while severely neglecting systematic training in technological ethics and cognitive security. Even when some universities offer related courses, they are often electives or lectures with fragmented content and outdated information, failing to form effective capability training.

The consequences of this cognitive deficiency are multifaceted. From a legal perspective, some students, lacking a clear understanding of red lines, inadvertently violate laws in their research or practice, such as unauthorized testing of website vulnerabilities or dissemination of vulnerability exploitation tools, facing legal liability. From a security standpoint, when faced with new threats like deep fake videos and automated public opinion manipulation, they lack basic identification and defense capabilities, easily becoming victims or even unwitting participants in cognitive warfare. More severely, a small number of students may exploit their technical skills for illegal purposes due to a lack of ethical principles, becoming sources of risk for technological abuse and betraying the fundamental purpose of cybersecurity talent training.

4. Constructing a "Broad-Spectrum and In-Depth" Three Dimensional Training System for Cyberspace Security Talents

4.1 Flexible Knowledge Base Based on Competency Diagnosis

The key to addressing the issue of knowledge supply lagging behind technological iteration lies not in increasing class hours or expanding course coverage, which would only exacerbate student burdens and potentially dilute the cultivation of core research capabilities. The truly effective path is to precisely identify each student's competency gaps and construct a flexible, adaptive knowledge base to achieve a harmonious integration of broad-spectrum foundations and in-depth expertise.

The primary task is to establish a competency baseline diagnosis mechanism. Breaking away from the traditional model of "enrollment determines courses," a pre-enrollment competency diagnosis is conducted for new students, covering core general modules such as network mapping, reverse analysis, active defense, content security, and cryptographic foundations to comprehensively assess students' technical foundations and competency gaps. The diagnosis is not a simple pass-fail test but forms a personalized competency profile, clearly identifying the gaps each student needs to address and the advantages they can leverage. This diagnosis is not a one-time event but is conducted annually to dynamically track changes in student competencies.

Based on the diagnosis results, a "diagnosis-exemption-remediation" dynamic training path is established. For students who pass the baseline diagnosis and demonstrate general competency, exemptions from foundational course credits are granted, encouraging them to enroll in advanced specialized topics such as quantum cryptography, large model security, and cloud-native security at an earlier stage, focusing on in-depth research in their specialized fields. For students who fail the diagnosis and have competency gaps, flexible remediation methods such as MOOCs, short-term intensive training camps, and one-on-one tutoring are employed to ensure they possess a qualified general technical foundation before entering the core research stage. This model avoids having students with strong general competencies "accompany" others in learning while ensuring a competency baseline for students with weaker foundations, achieving personalized training.

Simultaneously, cross-domain thinking seminar mechanisms are promoted to facilitate knowledge integration. Breaking down barriers between laboratories and research directions, regular cross-domain seminar systems are established, bringing together students studying cryptography, system attack-defense, and content security to engage in in-depth discussions on topics such as "viewing cryptographic implementation from an attack-defense perspective" and "vulnerability mining strategies in content security." These seminars are not simple technical sharing sessions but guide students to examine issues from different perspectives, breaking mental fixedness and achieving cross-domain knowledge fusion and broad-minded thinking expansion. Additionally, students are encouraged to participate in cross-directional research projects to strengthen cross-domain capabilities in practice, ensuring that a broad-spectrum foundation truly serves in-depth research.

4.2 Fully Integrated Research-Application Synergy Ecosystem

The core to addressing the disconnection between training mechanisms and operational realities is to inject operational genes into the entire lifecycle of talent training rather than treating it as a supplementary or ornamental element before graduation. This requires constructing a fully integrated research-application synergy ecosystem to achieve deep fusion of teaching, research, and operations, allowing students to hone their capabilities and accomplish research innovations in real-world scenarios.

At the curriculum level, joint teaching and training are implemented. Technical experts from national key cybersecurity units and industry-leading enterprises are actively engaged in the entire process of curriculum design, teaching implementation, and assessment evaluation. Rather than simply inviting experts for lectures, the latest threat intelligence and real attack-defense cases from enterprises and operational departments, after declassification, are transformed into teaching materials, and practical teaching materials and case libraries are compiled. Simultaneously, industry certification standards are aligned with course content, allowing students to accumulate professional capabilities during their coursework and shorten the adaptation period for their future positions.

In the practical training segment, systematic advancement through drills replaces traditional training. National-level "Cyber Defense Operations," industry-level red-blue confrontation exercises, and critical infrastructure security drills are incorporated as core practical components of graduate training, with clear credit requirements and assessment standards. Students are encouraged to participate as main forces in these high-pressure, highly realistic confrontation tasks, validating their algorithmic models, optimizing defense strategies, and enhancing emergency response capabilities in real-world operations. Simultaneously, a drill review mechanism is established, where operational experts and university supervisors jointly provide feedback, analyzing not only technical gains and losses but also reviewing cognitive shortcomings to achieve a closed loop of "drills-reviews-improvements."

In the research segment, deep project integration is promoted. Leveraging major projects such as the National Key Research and Development Program and the National Natural Science Foundation, combined with graduate workstations and university-enterprise joint research bases, a "dual-supervisor" system is fully implemented—where university supervisors are responsible for guiding research methods and theoretical foundations, and enterprise or operational department supervisors are responsible for cultivating project practice and operational capabilities. Students are encouraged to enter the research process with real "bottleneck" problems, conducting research and completing their dissertations around solving national and industry-level practical challenges, fundamentally changing the research mode of "creating in a vacuum." In this model, students' research outcomes can meet both academic requirements and directly serve operational needs, achieving unity in research and application value.

4.3 Layered Governance of Ethical and Cognitive Defense Lines

To address the technological disruption brought by the AI era and establish a solid value foundation for talents, a layered governance system of ethical and cognitive defense lines must be constructed, integrating value leadership throughout the entire training process to achieve simultaneous enhancement of technical capabilities and ethical literacy and cognitive abilities. This defense line is not a single curriculum system but a multi-level training system encompassing bottom-line constraints, general education, and cognitive training.

The first layer is the cultivation of legal and ethical bottom-line thinking. A compulsory course on Cybersecurity Law and Engineering Ethics is offered, covering not only legal and regulatory provisions but also incorporating real judicial precedents and industry ethical controversy cases. Through case analyses, mock trials, and other forms, students deeply understand the principle that "technological neutrality does not imply exemption from responsibility" and clarify the legal boundaries and ethical bottom lines of technological applications. Simultaneously, specialized lectures are invited from law enforcement agencies and enterprise compliance experts to share

practical compliance risks and response experiences, guiding students to establish a "compliance-first" mindset and prevent unintentional crimes.

The second layer is general education in cognitive security literacy. While not requiring all students to master advanced cognitive confrontation techniques, they must possess basic cognitive security awareness and defense capabilities, namely "technological political sensitivity." Through general education courses, specialized seminars, and other forms, students are trained to identify new threats such as deep fake content, automated public opinion manipulation, and online rumors, understanding the societal impacts and national security significance behind these threats. Simultaneously, interactive and scenario-based teaching methods are introduced to make cognitive security education more engaging and effective, helping students establish a comprehensive cognitive defense system.

Building upon this, specialized ethical training is conducted for students whose research directions involve high-risk technologies. For those studying malicious code analysis, vulnerability exploitation, AI-generated content security, and other fields, advanced ethical seminar courses are added, conducting in-depth discussions on the boundaries of technological applications and risk prevention measures. A "research ethics review" mechanism is established to ensure that research processes and outcome applications comply with legal and ethical standards. Through this layered training, a comprehensive ethical and cognitive protection system is constructed, solidifying the value bottom line for all students while meeting the specialized needs of students in specific fields.

5. Trinity Implementation Path for Cyberspace Security Talents

5.1 System Restructuring: Establishing a "Credit Substitution and Flexible Academic System"

Systems are the core guarantee for the implementation of the training model. The primary task is to break down the institutional barriers that constrain talent training and establish a flexible system tailored to the "broad-spectrum and in-depth" model, with the core being the implementation of credit substitution and a flexible academic system.

On one hand, the "sole curriculum focus" is abandoned, and a "skill-credit" conversion standard is established. The graduate training program is revised to clearly stipulate that situations such as students passing the pre-enrollment competency diagnosis, obtaining high-level industry certifications, and achieving outstanding results in operational drills can all be used to substitute corresponding foundational course credits. This system not only recognizes students' existing capabilities and operational achievements but also guides them to focus their efforts on cultivating advanced capabilities and specialized expertise, avoiding resource waste from repetitive learning. Simultaneously, a dynamic assessment mechanism for credit conversion is established, where conversion standards are adjusted in a timely manner based on industry technological development and certification system updates to ensure system adaptability.

On the other hand, a flexible research-operation cycle is implemented to address the "conflict between academic studies and operations." Students are allowed to apply for flexible adjustments to their study duration, course learning time, or thesis submission time due to participation in national major attack-defense drills, on-site research, or enterprise practice. A specialized approval and coordination mechanism is established, where university supervisors, enterprise supervisors, and the college jointly assess the value of students' operational tasks and academic progress to develop personalized academic plans, ensuring that students can deeply participate in operations without affecting their research progress and degree acquisition. This system design provides guarantees for students to actively participate in operations, enabling true integration of research and application.

5.2 Platform Construction: Establishing a Physical "University-Enterprise Community of Shared Fate"

Platforms are the carriers for research-application synergy, necessitating the transformation of university-enterprise cooperation from a loose internship base model to a deeply integrated university-enterprise community of shared fate, achieving resource sharing, shared responsibilities, and mutual benefits to provide solid support for talent training.

Firstly, physical joint research and operation centers are co-established. Universities and enterprises jointly invest in venues, equipment, faculty, and funding to establish integrated platforms for teaching, research, and operations. These centers are equipped with real network environments, attack-defense equipment, and threat intelligence resources, serving as both practical classrooms for students and research and development bases for enterprises and research platforms for universities, achieving efficient resource utilization.

Secondly, a comprehensive resource-sharing mechanism is constructed. In terms of teaching resources, universities and enterprises jointly develop practical case libraries, teaching materials, and online courses, achieving dynamic updates of teaching content. In terms of faculty resources, a "mutual appointment and dispatch" system is implemented, where university faculty go to enterprises for on-the-job training to update their operational knowledge, and enterprise experts are full-time instructors at universities, participating in training program design. In terms of research resources, enterprises open up real datasets and technological platforms, while universities open up research outcomes and laboratory resources to jointly conduct major research projects, forming a resource for "teaching-research-operations."

Finally, the scope of "order-based training" is expanded. From a few pilot enterprises to key infrastructure industries such as power, finance, and transportation, order-based training is jointly conducted with industry associations and multiple enterprises. Customized training programs are developed based on industry common needs and enterprise individual needs. This model not only forms an industry-level talent reservoir to meet the talent needs of key fields but also enhances the targeting and employment rate of talent training, achieving a triple win for universities, enterprises, and industries.

5.3 Assessment Reform: Implementing a "Representative Work + Ethical One-Vote Veto" System

The assessment system is the guiding baton for talent training, necessitating the abandonment of a single paper-oriented approach and the establishment of a diversified assessment system tailored to competency-based training, while strengthening ethical constraints to ensure the correct direction of talent training. The core is to implement a "representative work + ethical one-vote veto" system, achieving unity in capability and value assessments.

Build a diversified achievement evaluation system encompassing "theses + code + tools + contributions." Move away from the practice of relying solely on academic theses as the core criterion for degree awarding. Instead, incorporate students' core code, developed security tools, key contributions in practical exercises, applied invention patents, and formulated industry standards into the scope of achievement evaluation, and clearly define the evaluation weights and recognition criteria for different types of achievements. For example, if a security tool developed by a student is practically applied by enterprises or if the student makes outstanding contributions in national-level cybersecurity protection campaigns, these can serve as important bases for degree awarding. This evaluation system guides students to shift from "researching for the sake of papers" to "researching for the sake of solving problems," balancing the cultivation of both academic and practical capabilities.

Strengthen ethical pre-review and the one-vote veto mechanism. At critical stages such as graduate thesis proposals, mid-term assessments, and thesis defenses, add a dedicated chapter on "technological ethics review." Establish a review panel consisting of ethics experts, industry compliance experts, and supervisors to rigorously assess the potential ethical and legal risks

associated with students' research content, technological applications, and achievement transformations. For projects involving high-risk research such as malicious code generation, unauthorized vulnerability exploitation, and privacy infringement, and where effective risk prevention and control measures cannot be proposed, implement a one-vote veto to prohibit further research. For projects with minor ethical concerns, require students to revise their research plans and supplement ethical prevention and control measures. This mechanism places ethical constraints throughout the entire cultivation process, establishing a firm value bottom line for talent development.

6. Conclusion

The competition in cyberspace ultimately boils down to competition among talents. Against the backdrop of increasingly complex cyber threats, accelerating technological iterations, and growing national security demands, the cultivation of cyberspace security talents has become a strategic task concerning national sovereignty, security, and development interests. Constructing a "broad-spectrum yet in-depth" graduate cultivation system is by no means a simple adjustment of the curriculum or a partial improvement of the cultivation model; rather, it is a systemic transformation involving educational philosophies, research models, evaluation criteria, and institutional frameworks.

The core of this transformation lies in a paradigm shift from a discipline-centric to a competency-centric approach. Instead of defining the scope of cultivation based on disciplinary boundaries, it focuses on practical needs and competency requirements to construct a cultivation logic of "broad-spectrum foundation, in-depth expertise, and value-led development." Through the construction of a flexible knowledge foundation, it resolves the contradiction between narrow-field in-depth cultivation and the demand for broad-spectrum capabilities among graduate students, achieving unity between foundation and expertise. By creating a collaborative ecosystem of research and application, it breaks down barriers between education and practical combat, achieving integration between research and application. By strengthening ethical and cognitive defenses, it upholds the bottom line of technological application, achieving simultaneous enhancement of capabilities and values.

Only by thoroughly breaking down the walls between universities and industries, theory and practice, and technology and ethics, and allowing education to truly return to practical combat and serve the resolution of real-world problems, can we truly eliminate the scissors gap between talent supply and demand and cultivate compound cybersecurity experts who possess both theoretical acumen and practical prowess, as well as political fortitude. These talents will become the national treasures defending our country's cyberspace security and provide solid talent support for China to take the initiative and safeguard national security in the increasingly fierce competition in cyberspace. Going forward, it is essential to continuously track technological advancements and industry demands, continuously optimize the cultivation system, and propel the cultivation of cyberspace security talents to new heights.

References

- [1] Ministry of Industry and Information Technology Education and Examination Center, China Cybersecurity Industry Alliance. Report on the Development of Cybersecurity Industry Talent (2024)
- [2] NIST. Workforce Framework for Cybersecurity (NICE Framework) (NIST Special Publication 800-181 Rev. 1). Gaithersburg: National Institute of Standards and Technology (2020)
- [3] Zhang, Huanguo. Thoughts on the construction of cyberspace security discipline. Journal of Wuhan University, 62(01): 1-8 (2016)
- [4] Feng, Huamin. Current situation, problems, and countermeasures of national cybersecurity talent cultivation. China Information Security, (09): 38-41 (2021).

- [5] V. L. L. Thing, Adapting the NICE Cybersecurity Workforce Framework for a University Curriculum, in IEEE TALE (2019).
- [6] Liu, Jianwei, Li, Junxiong. Exploration and practice of the “practical combat” teaching mode in cyberspace security. Computer Education, (08): 3-7 (2020).
- [7] Cyberspace Security Professional Teaching Steering Committee of the Ministry of Education. White paper on the practical capabilities of cybersecurity talent (Security Testing and Assessment) (2024)