Research and Practice of Practice Innovative Ability Cultivation for Cyberspace Security Postgraduates Under the Vision of New Engineering

Shibin Zhang[1,a,*], Yuanyuan Huang[2,b], Shiti She[3,c], Yan Chang[4,d], Yanjun Long[5,e]

{cuitzsb@cuit.edu.cn[a], hy@cuit.edu.cn[b],649249791@qq.com[c], cyttkl@cuit.edu.cn[d], 2446912692@qq.com[e]}

School of Cybersecurity, Chengdu University of Information Technology, Chengdu ,China[1,2,4,5]
Advanced Cryptography and System Security Key Laboratory of Sichuan Province, Chengdu ,China[1,2,4,5]
Information Technology Center, Chengdu Shuangliu International Airport Co., Ltd., Chengdu , China[3]

Abstract. The difference between new engineering and traditional engineering lies in its interdisciplinary and comprehensive. Under the vision of new engineering, technical talents are required to have strong practical and innovative ability. In accordance with the national requirements for the construction of new engineering, guided by the needs of national network security strategic, and focusing on the deep integration of network security industry demand, this paper establishes the "five dimension-double base" training system and the "five level-three stage" training mode for the practice innovation ability of the cyberspace security master with "capability center" as the guidance, which mainly solves the serious disconnection between the theoretical study and engineering practice, and improves the practical innovation ability of the cyberspace security master. The teaching practice shows that the training system of this practice innovative ability is feasible, and has been widely recognized and highly appraised by the society, and has played a good demonstration and leading role in the training of innovative talents of network security for local universities.

Keywords: New Engineering; Cyberspace Security; Postgraduate; Practice Innovative Ability

1 Introduction

To implement China's significant strategies, such as innovation-driven development, Made in China 2025, and Internet power, the national economic construction has put forward new requirements for the professionalism of technical talents and the quality of higher engineering education in various fields[1]. In response to national demand, the Ministry of Education has formulated a trilogy for constructing “New Engineering” since February 2017, which are “Fudan Consensus”, “Tianda Action”, and “Beijing Guidelines”. It has been successively issued the “Notice on Carrying Out Research and Practice of New Engineering,” “Notice on Promoting Research and Practice Projects of New Engineering”, “Notice of the Publication of the First Batch of Researches and Practice Projects by General Office of the Ministry of Education”, “Action Plan for Innovation in Artificial Intelligence in Higher Education Institutions” and decided to develop a batch of colleges of future technology in higher

NMDME 2023, October 13-15, Xi'an, People's Republic of China

DOI 10.4108/eai.13-10-2023.2341347

education institutions, which opened up new ways for reforming engineering education in colleges and universities.

Compared with conventional engineering education, New Engineering focuses on developing new technologies and industries that face the future[2]. It strives to promote the progress of interdiscipline and integration of multiple disciplines, emphasizing practicality, interdiscipline, and comprehensiveness and innovating in aspects of the ideology, the quality, the structure, and the system of educational concept. In order to cultivate talents of cyberspace security that are urgently needed, the Ministry of Education decided to establish a first-level discipline of cyberspace security(code 0839) under the category of engineering in June 2015, granting an engineering degree[3]. Cyberspace security is a comprehensive discipline that integrates computer science, electronic technology, mathematics, physics, biology, law, management, and education and has grown its unique connotation, theory, technology, and application that serves today's digital world[4]. While as a comprehensive discipline integrated with various disciplines, the conventional training mode designed for single-discipline postgraduate students is insufficient to match the fast-paced development of cyberspace security theory and technology[5].

Master's education is at a higher level of the higher education system; it serves as a crucial source of talent for constructing the national innovation system, and it is also a significant part of cultivating high-quality, innovative talents[6]. It had become an urgent task for national development to cultivate a large number of high-quality cyberspace security professionals who possess a strong ability to innovate, practice, and adapt to rapid economic and social advancement since 2014 when cyberspace security was promoted as a national strategy. Since the year of 2005, Chengdu University of Information Technology has been recruiting postgraduate students in cyberspace security(approved as a master's degree authorization institution by the year of 2018). Guided by the demand for a national cyberspace security strategy and considered in the perspective of talent cultivation strategy, Chengdu University of Information Technology has proposed a "capability center" oriented training system that improved the practical innovation ability of cyberspace security masters.

2 Main issues faced in cultivating practical innovation ability of cyberspace security master students

New engineering has its characteristics of interdiscipline and comprehensiveness compared with conventional engineering, which requires technicians to acquire strong practical innovation ability. China is currently building its internet power and thus is urgently in need of cultivating a large group of talents that possess broad theoretical foundations, strong practical innovation ability, high comprehensive quality, and adaptive to global advancement[7]. However, there are several problems that exist in the currently cultivating the practical innovation ability of network security master students.

(1) Insufficient practical innovation ability of cultivated talents fails to meet the needs of the country and society.

Due to the majority of universities adopting imbalanced training systems that emphasize theoretical teaching while neglecting the practical and innovative part, general postgraduates

lack the ability to innovate or apply theoretical knowledge to solve real-world problems, causing employers in today's society dissatisfaction with the postgraduates[8].

(2) Insufficient knowledge breadth of cultivated talents fails to meet the needs of the country and society.

Cyberspace security professionals are supposed to be versatile and possess a broad knowledge base, interdisciplinary skills, self-learning ability, and many other skills. However, the current training system has defects such as insufficient knowledge depth, weak multidisciplinary skills, and inadequate practical abilities[8]. Thus, universities cannot cultivate talents that are qualified enough to match the needs of employers, and employers will have to provide secondary training to the graduates, which causes a waste of educational resources.

(3) Faculty lack of practical innovation ability cannot cultivate talents with practical innovation ability

Most professors in many universities' cyberspace security are transferred from other computer-related disciplines such as computer science and technology, software engineering, and telecommunication engineering[8]. There are relatively few teachers who are entirely in line with the cyberspace security major (due to the relatively low salaries of universities, most graduates with high qualifications tend to work in companies that offer higher salaries). The backbone courses of cyberspace security are usually taught by teachers of other majors, which leads to deviation from the core requirement of cultivating cyberspace security talents. Meanwhile, teachers who are also capable of practical innovation are even scarcer, which directly causes the graduates' practical ability to fail to meet the needs of employers.

(4) The relative lack of infrastructure for practical teaching has seriously hindered the cultivation of innovative talents in cyberspace security practice

Due to the rapid development of cyberspace security technology and the lack of funding for school operations (especially for local universities), the infrastructure for practical teaching cannot keep up with technological advancement. A great many universities are not equipped with virtual environment simulation platforms and authentic practice devices[9]. For students, the lack of a practical application environment in teaching, resulting in a disconnection between theory and social practice, is tantamount to empty talk. At present, the shortage of practical teaching platforms for cyberspace security has become a significant bottleneck hindering the cultivation of cyberspace security talents.

(5) The hasty and utilitarian evaluation method of achievement leads to the lack of innovative ability of cultivated talents.

Currently, most of China's universities regard the number of papers published as the primary standard for evaluating academic achievements and lack sufficient attention to implementing these research results. This standard is highly possible to lead universities into the wrong region of scientific research evaluation, resulting in a waste of massive amounts of resources and forming a hasty academic environment. Many researchers tend to choose projects that are easy to conduct and publish essays and reject projects with long development cycles and strong practicality. This situation directly reduced the opportunity for master's students to participate in practical innovation projects and made it difficult for original and disruptive results to emerge.

Based on these reasons, our university's cyberspace security master's degree program is now oriented by national cyberspace security strategy needs, actively matches our country's new demand for constructing New Engineering, and attaches importance to the deep integration with the need for the cyberspace security industry. Our institute has already established the "five dimension-double base" training system and the "five level-three stage" training mode for the practice innovation ability of the cyberspace security master with "capability center" as the guidance, which mainly solves the serious coming apart between theoretical learning and engineering practice program, and improved the practical innovation ability of cyberspace security master's degree.

3 Research and implementation on the talent cultivation system of practical innovation ability oriented by "capability center"

As the diagram Fig.1 shows, the "five dimensions" refers to the five aspects of cultivating the ability of cyberspace security masters, namely basic professional ability, engineering practice ability, practical innovation ability, organizational communication ability, and professional ethics quality. "Dual basis" is a dual-practice base for cultivating the practical innovation ability of cyberspace security masters: that is, the “on-campus practice teaching base” for cultivating the engineering practice ability of cyberspace security masters (including those independently founded by universities or co-founded by universities, enterprises, and research institutes), and the “off-campus practice innovation base” for cultivating the practical innovation ability (including those co-founded by universities and enterprises or research institute).

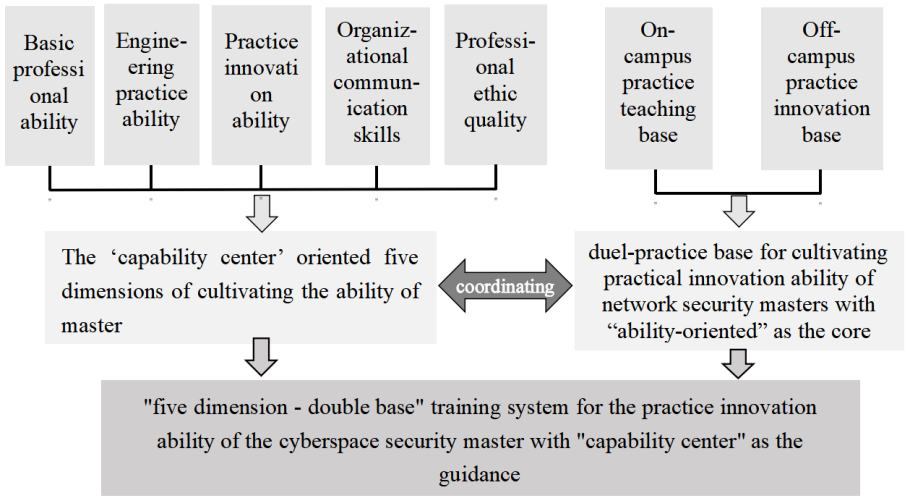

Fig.1 "five dimension-double base" training system for the practice innovation ability of the cyberspace security master with "capability center" as the guidance

3.1 Proposing a level to assess cultivation to a cyberspace security master in five dimension

Today's cyberspace security master ought to be guided by national strategy, aimed at fulfilling social needs, oriented towards practical applications, and focused on improving professional ethics, engineering practice, and innovation ability. Analyzing the requirements of the cyberspace security industry and professional fields for the knowledge and ability structure, paying attention to the deep integration of talent training with national and industrial needs, establishing a scientific and reasonable curriculum system, attaching great importance to cooperative learning, case analysis, on-site practice, simulation training, practical innovation, and other methods, emphasizing the cultivation of engineering practice and practical innovation ability[10], we proposed five dimensions of cultivating the five abilities of cyberspace security masters centered on "ability orientation".

3.2 Established a dual-practice base centered on "capability orientation" to cultivate the practical innovation ability of cyberspace security masters

(1) Built a "five-in-one" school-based practice teaching base for cyberspace security masters

In order to enhance the practice innovation ability of postgraduate students, since 2011, our school has built a practice teaching base that integrates the following five platforms: teaching experiments, engineering practices, scientific research training, scientific and technology competition, and practice innovation[11], which solves the problem of the lack of coordination between the practical innovation ability cultivation inside and outside the university. Based on the school-based practice teaching base, we established a series of practice teaching curricula and frameworks for cyberspace security masters. Ten practical teaching courses that converge basic knowledge, scientific and technological competition, technology, industry, and innovation ability have been set up. Six authentic engineering practice projects, eight scientific research training projects, and one network attack and defense platform are now open and accessible for the cyberspace security master of our school. A platform for the research and development of new technology is established, which implemented an open laboratory management system, and an open experimental teaching mode has been created in which students can choose experimental content and conduct experiments under the guidance of mentors.

(2) Created a technology competition platform that integrates learning, competition, and research.

To enhance the engineering practice and innovation ability of cyberspace security masters, we established a competition. The competition converges open, diverse, practical, and innovative education. It builds a multi-dimensional, all-round, and whole-process technology competition education platform composed of "skill competition-academic forum-knowledge competition" participated by enterprises[12]. The competition is based on the basic knowledge of the technical application of cyberspace security, covering network attack and defense technology, cloud server security, big data security, Internet of Things security, and other directions, emphasizing examining the practical and application innovation ability of contestants. Currently, the competition questions have been included as cases in the practical teaching for cyberspace security masters, which has improved the significance of holding competitions and expanded the benefits of graduate students, greatly enhancing students' engineering practice and innovation ability.

(3)Built distinct off-school practice innovation base in types of research and practice

In recent years, in accordance with the overall goal of “cultivating high-quality, specialized talents with healthy mind and body, good humanistic quality, systematic theoretical knowledge, and solid practical ability”, our university has established off-campus production and education, science and education integration practice innovation bases inside IT field enterprises or scientific research institutions that conducting national and provincial key research projects or possess decent conditions in talent cultivation. These bases have fully utilized their advantages of professionalism, strong engineering ability, and strong innovation ability. They have created a platform for cyberspace security master’s engineering practice, application innovation, and degree thesis research. At present, ten distinctive bases for the integration of industry, technology, and education have been established, which are in two types of technology research and technology application, forming a dual mentor guidance mechanism consisting of both on-campus and off-campus mentors. The technology research base mainly trains postgraduate students’ engineering technology research and innovation capability to tackle problems in the industry's research, promotion, and application of key techniques. The technology application base mainly cultivates students’ abilities in engineering application, solving technical problems in the actual production of enterprises.

4 "Five level-three stage" training mode for the practice innovation ability of the cyberspace security master with "capability center" as the guidance

To enhance the practical innovation ability of masters in cyberspace security and ensure the sustainable and continuous growth of the practical innovation education for the masters, by the requirements in the “Several Opinions on Doing a Good Job in the Training of Full-time Masters” issued by the Ministry of Education, our school has deeply cooperated with relevant departments, governments, enterprise, and institutions to explore a reasonable and feasible new mode of "school-government-enterprise-institution" collaborative education that adapts the national strategy and social demands[12]. Thus, a “five level-three stage” training mode for the practice innovation ability of the cyberspace security master with “capability center” as the guidance is established. (shown in fig.2)

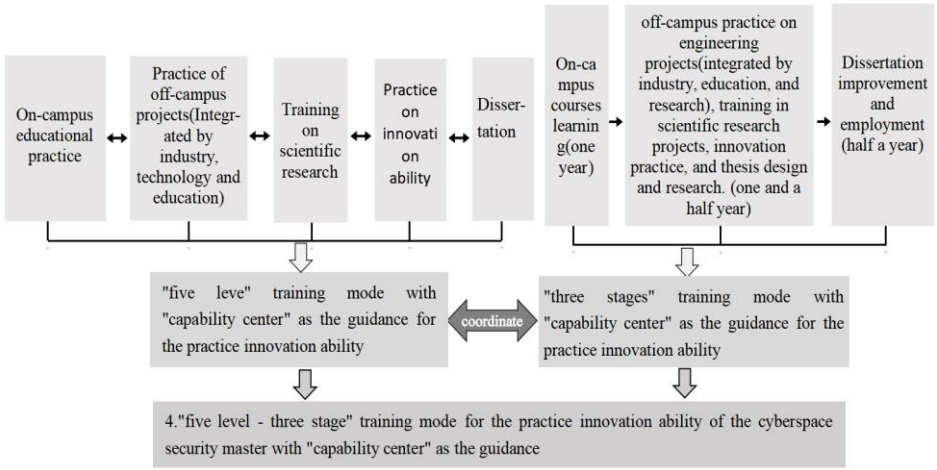

Fig.2 "five dimension-double base" training system for the practice innovation ability of the cyberspace security master with "capability center" as the guidance

4.1 The "five-level" progressive practical innovation ability training mode oriented towards "competency centers"

As shown in fig.2, the "five-level" refers to the "five-level" progressive practical innovation ability training mode of "On-school educational practice, Practice of off-campus projects(Integrated by industry, technology and education), Training on scientific research, Practice on innovation ability, and dissertation". The teaching practice of on-campus courses is mainly completed in the first academic year under the guidance of the course mentors (including the employment of off-campus part-time teachers). off-campus (industry-education and science-education integration) engineering project practice is generally completed on the basis of deep cooperation between our institute and relevant national departments, government agencies, enterprises and institutions, and scientific research institutions to establish industry-education and science-education integration practice bases (which can be established on campus or off campus). Scientific research project training is conducted under the guidance of mentors (including off-campus part-time mentors). Under the guidance of the mentors, students independently choose topics, complete project design, prepare research conditions, implement projects, write research reports, and engage in academic communication. The practice of innovation ability is carried out under the guidance of mentors (including part-time mentors outside the school) and on the premise of respecting students' interests and hobbies. Students choose their own topics for innovation ability practice (including openness, exploration, and research-based practice). The degree thesis is written under the guidance of the supervisor (including part-time instructors outside the university), with the student selecting a topic from the practice of engineering projects, scientific research projects, and innovative practice, and completing it according to certain requirements. It is also the final answer sheet to test the student's final learning outcomes.

4.2 The "three stages" practical innovation ability training mode oriented towards "competency centers"

As shown in Figure 2, the "three-stage" model refers to a "competency-centered" three-stage practical innovation ability cultivation model, which includes "in-school course learning (1 year) and off-campus (industry-education and science-education integration) engineering project practice, scientific research project training, innovation ability practice, degree thesis design and research (1.5 years), and degree thesis improvement and employment (0.5 years)".

5 Conclusions

Since 2011, our university has been profoundly cooperating with relevant national departments, government agencies, enterprises and institutions, and scientific research institutions in the cultivation of master's degree students in cyberspace security and explored a reasonable and feasible new model of multi-party collaborative education for "university-government-enterprise-institution" that meets the national development strategy and social needs. We have established a "five-dimensional (professional basic ability, engineering practical ability, practical innovation ability, organizational communication ability, professional ethics quality)-double-base (on-campus practical teaching base, off-campus

practical innovation base)" cyberspace security master's practical innovation ability cultivation system, oriented by the "capability center". The "five-level (on-campus curriculum teaching practice, off-campus (industry-education and science-education integration) engineering project practice, scientific research project training, innovation ability practice, dissertation)-three-stage (on-campus curriculum learning (1 year) and off-campus (industry-education and science-education integration) engineering project practice, scientific research project training, innovation ability practice, dissertation design and research (1.5 years) and dissertation improvement or employment (0.5 years))" network security master's practice innovation ability training mode has achieved good results in the practice innovation ability training of cyberspace security master's in our university. The cyberspace security master's practice innovation ability, professional ethics, and quality have been significantly enhanced and have been widely recognized and highly praised by society, playing a good demonstration and leading role for local universities in cultivating innovative talents in cyberspace security.

Acknowledgments: This work is supported by The Higher Education Talent Training Quality and Teaching Reform Project of Sichuan Province (No. JG2021-997, No. JG2021-980, No. JG2021-981), the Teaching Reform Project of Chengdu University of Information Technology (No. JYJG2023056, No. CUITGOMP202101).

References

[1] Ruinian Hu, Pu liu. Research on the Construction and Development Path of "New Engineering" in Colleges and Universities in the New Era. Decision & Information, pp. 111-122(2019). (in Chinese)

[2] Zhong Wei, Li Chong, Fang Jiwen, Wang Xiaorong. Approaches to Improve Innovative Ability of Postgraduates of Mechanical Engineering under the Background of New Engineering Disciplines. The Guide of Science & Education. pp. 70-71,73(2019). (in Chinese)

[3] Cui Jixin,Chu Rongzhen, Zhang Jiangbo. Reflections on the Training Mode of Information Security Talents in Institutions of Higher Learning. Education and Teaching Forum. pp. 223-224 (2018). (in Chinese)

[4] Zhang Shibin, Wu Chunwang. Training Standards for Excellent Engineers in Information Security. Xidian University Press. 2016. (in Chinese)

[5] Feng Wen, Chen Jinsong, Lei Xiao. Exploration of interdisciplinary training mode for graduate students in new engineering disciplines. Journal of Cultural and Educational Materials. pp. 196-197 (2020). (in Chinese)

[6] Uprising "Maintaining Cybersecurity" to National Strategy [EB/OL]. [2014-03-08] http://www.gov.cn/xinwen/2014-03/08/content_2633153.htm. (in Chinese)

[7] Peng Jialiang, Wu Yi, Gao Bin. Exploration of the Innovative Ability Training Model for Master's Students in Cyberspace Security. Industrial Technology Innovation. Vol. 1, pp: 113-114(2019). (in Chinese)

[8] Pisareva, O. M., Alexeev V. A. Organizational Aspects of Ensuring Information Security in the Framework of Creating an Intelligent Transport System in the Russian Fed eration. IOP Conference Series: Earth and Environmental Science. Vol. 666, pp. 62077(2021).

[9] Cai Weiquan, Li Xudong, Zeng Qingzhu, Liu Rongying. Cultivation of Engineering Innovation Ability of Master of Engineering Postgraduates of Emerging Engineering Education. Higher Education in Chemical Engineering. pp: 69-72(2020). (in Chinese)

[10] Baan N. V. D., Gast I., Gijselaers W. Coaching to prepare students for their school-to-work transition: conceptualizing core coaching competences. Education and Training. Vol. 64, pp. 398-415 (2022).
[11] Zhang Shibin, Liang Shanyan, Ning Wenguan, Chang Yan, Yan Lili, Sheng Zhiwei, Song Haiquan. Research on the Training System of Network Security Engineer's Innovation Ability. Journal of Information Security Research. Vol. 6, pp: 898-905(2020). (in Chinese)
[12] Zhang Shibin,Chang Yan, Yan Lili. Exploration of the Training Model for Network Security Applied Talents Based on Multi party Collaboration. Confidential work. pp: 57-58(2021). (in Chinese)