

Construction and Practice of Cultivation System for Innovative Talents in Cyberspace Security

Chunwang Wu^{1,*}, Linxia Li² and Luqiao Zhang³

^{1, 3} Chengdu University of Information Technology

² Chengdu University

*Corresponding author. Email: ajexuwu@cuit.edu.cn

ABSTRACT

In June 2015, The Academic Degrees Committee of the State Council of China and the Ministry of Education decided to add the First-Level Discipline of "cyberspace security" under the category of "engineering". The establishment of the first-level discipline is aimed at implementing the national security strategy, which is not only conducive to speeding up the training of high-level talents for cyberspace security, but also puts forward higher requirements for Discipline Construction and personnel training system. Based on the analysis of the concept and connotation of cyberspace security, this paper summarizes more than 10 years experience of Chengdu University of Information Technology in the construction of information security specialty, and gives some suggestions on the construction and practice of Cyberspace Security innovation personnel training system.

Keywords: Cyberspace security, Discipline construction, Talent training system.

1. INTRODUCTION

In 2008, US Presidential Decree No. 54 defined cyberspace: Cyberspace is an overall area in the information environment, which is composed of independent and dependent information infrastructure and networks. Including the Internet, computer systems, embedded processors and controller systems. Cyberspace has gradually developed into the fifth largest strategic space after sea, land, air and sky. Cyberspace Security studies security threats and protection issues in cyberspace. In a confrontation environment, it studies the threats and protective measures faced by information in the production, transmission, storage, and processing links, as well as the network and the system itself Threats and protection mechanisms. Cyberspace security includes not only the integrity, confidentiality, and availability of information studied in traditional information security, but also the security and credibility of the infrastructure of cyberspace.

With the improvement of social informatization and the rapid development of information technology, the network has been deeply integrated with traditional industries. The Internet penetration rate in China is rising rapidly. As of June 2020, the number of Internet

users in China is 940 million, the Internet penetration rate is 67.0%, the number of national and regional top-level domain names ".CN" is 23.04 million; the number of online shopping users is 7.49 Billion; the number of online government service users reached 773 million. Since 2013, China has become the world's largest online retail market for seven consecutive years. In the first half of 2020, online retail sales reached 5,150.1 billion yuan. Network security is not only related to the national economy and people's livelihood, but also closely related to national security. It not only involves the country's political, military, and economic aspects, but also affects national security and sovereignty. To build a national information security system and ensure the security of important departments and infrastructure, a large number of cyberspace security professionals are needed.

In order to fully implement Xi Jinping's Thought on Socialism with Chinese Characteristics in the New Era and follow the spirit of the National Medium and Long-term Education Reform and Development Plan (2010-2020) and the National Medium and Long-term Talent Development Plan (2010-2020), colleges and universities should Reasonably set up professional talent training programs, innovate talent training models, and establish a comprehensive development and

application-oriented talent view. Strengthening the school-running characteristics of cyberspace security and other related majors such as information security and adapting to the needs of the new situation has important practical and social significance.

2. THE CONSTRUCTION OF CULTIVATION SYSTEM FOR INNOVATIVE TALENTS IN CYBERSPACE SECURITY

The talent training system of colleges and universities generally includes subject system, curriculum system, teaching system, and teaching quality monitoring and guarantee system. The professional talent training program is the compass to achieve the goal of talent training, the basic way for colleges and universities to realize the talent training specifications, and an important guarantee for comprehensively improving the quality of talent training.

Information security and other cyberspace security-related majors of Chengdu University of Information Technology pay attention to the improvement of education and teaching quality, and continuously strengthen professional construction and teaching reform. After more than ten years of hard construction and reform and innovation, a distinctive information security major has been formed. It has played a certain demonstrative and leading role in the training of information security talents in local colleges and universities, and is a provincial-level "first-class discipline construction" discipline in Sichuan. The training goal of this major is to train to meet the actual needs of my country's socialist economic construction, and to develop in an all-round way of morality, intelligence, physical beauty; with information security technical knowledge and reasoning ability, information security detection, system design and maintenance, security assurance, and information security application Development ability; possess professional ability and correct attitude, independent learning ability, organization and collaborative work ability, engineering management ability and comprehensive competitiveness; information security application engineering technical talent with innovative spirit and international consciousness. By 2020, Chengdu University of Information Technology has trained 14 undergraduates and 13 postgraduates in information security, with more than 3,000 undergraduates and about 200 graduates.

3. EXPLORATION AND PRACTICE OF CULTIVATION SYSTEM FOR INNOVATIVE TALENTS IN CYBERSPACE SECURITY

The cyberspace security major is developed based on multidisciplinary development such as mathematics, computer, cryptography, etc. It has a strong application. In the practice of the innovative talent training system, the construction of relevant teachers in universities should be strengthened, and the multidisciplinary knowledge should be strengthened. Cross-penetrate, adopt a diversified teaching model, attach importance to the construction of relevant curriculum groups, emphasize the cultivation of students' practical ability, strengthen teaching supervision, summarize and optimize existing experience, further improve the quality of talent training, and reform the innovative talent training system.

3.1. Faculty Building

The construction of the faculty is a prerequisite for ensuring the quality of talent training and improving academic standards, and has a decisive influence on the development of higher education. In recent years, Chengdu University of Information Technology has issued relevant supporting policies to encourage teachers to continue their studies; actively introduce talents with high academic qualifications and high professional titles, adopt the "one person, one discussion" approach, and provide talent introduction fees and scientific research start-up funds; hiring enterprises and institutions is rich in Front-line engineers with engineering experience serve as "dual-qualified" tutors and come to the school regularly or irregularly to teach students and exchange experiences. Through the above measures, we have built a team of high-quality teachers with a reasonable age, knowledge structure, rich engineering experience, and continuous innovation capabilities.

3.2. Diversified Teaching Mode

The information security major is very practical. On the basis of strengthening the study of theoretical knowledge, we carry out different forms of practical activities according to the direction of training. In the implementation of specific practical teaching, we change the traditional teaching method of Teaching, problem-oriented learning, project learning, experiential learning, games and simulation learning, flipped classrooms, online or blended learning, group debate or discussion, peer-based teaching, group learning, team presentation, role-playing and other teaching modes, etc. Combine them, highlight actual combat, enhance students' actual combat ability, and improve practical teaching effects.

Chengdu University of Information Technology holds four competitions every year, including the Campus Information Security Technology Competition, Sichuan University Student Information Security Technology Competition, Geek Challenge, and Class Competition. At the same time, actively organize and support students to participate in nationwide information security professional-related competitions, so that students can be immersed in the atmosphere of the competition throughout the year, and can be exposed to the latest information security technology with practical application value. Taking 2017 as an example, students majoring in information security won 8 provincial and above awards, with 38 winners, and gained a certain degree of popularity across the country.

3.3. Course Group and Characteristic Course Construction

Course group construction is the basic way to cultivate students' professional ability, and it plays a decisive role in the cultivation of students' professional quality. Chengdu University of Information Technology, based on basic computer professional courses such as "C Language Programming", "Computer Network", and "Database Principles and Applications", has built a course group with reasonable structure, clear levels, and mutual connection between courses. At present, an information security technology course group has been established, including two professional directions of security detection and vulnerability research. Professional courses in the direction of security detection include "PHP Programming", "Network Attack and Defense", "Advanced Attack and Defense Technology", "Code Security Audit", and other courses, vulnerability research directions include "assembly language programming", "virus principles and prevention", "reverse engineering technology", "vulnerability principle and mining" and other courses. These courses are forward-looking and practical, and have cooperated with many domestic companies and are ready to promote them to other universities. In addition, the "Applied Cryptography" course has been established as an excellent course in Sichuan Province and an excellent course in Sichuan Province for resource sharing.

3.4. Optimize Course Assessment Methods

In the assessment process, Chengdu University of Information Technology divides the assessment of most courses into regular assessment/process assessment and final assessment. The assessment link can refer to but not limited to the following methods: class discussion, attendance, oral report, homework, mid-term assessment, individual defense, group defense, course essay, design report, design plan, internship report, experimental report, operation skills, works Presentation, oral

examination, closed-book written examination, open-book written examination, etc. In principle, the higher the proportion of usual grades, the more abundant the content of the usual assessment links, and the output of results closely related to the course teaching content (such as displayed works, experimental reports, course papers, etc.). At present, 7 courses such as "C Language Programming", "Database Principles" and "Data Structures" are subject to procedural assessments. After each chapter is completed, students are periodically assessed online, which has changed the tradition. The assessment method of "one exam for life" in the final exam has formed a perfect assessment mechanism.

3.5. Engineering Practice Reform

Under the traditional two-semester model, students' practical exercise time is very limited, and they can only train in engineering practice through computer, internship, and experimentation. On the other hand, the employer has "relevant work experience". The requirements are higher. Therefore, Chengdu University of Information Technology regards engineering practice as a professional compulsory course, divided into engineering practice 1-5, corresponding to the 2-5 semesters, and arranges related engineering practice topics around the 12th week of each semester. Arrange code inspection, demonstration and defense every week. Taking the direction of penetration testing of information engineering as an example, the engineering practice is based on the principle of "combat-oriented, moderately advanced", and the content is C language programming practice; master the basic concepts of security, familiar with the principles of common WEB vulnerabilities; master the common tools of penetration testing; Concepts of user permissions, port forwarding, intranet (domain environment, peer-to-peer network), familiar with common intranet attack methods, privilege escalation, forwarding gateway or routed traffic; master the method of writing python scripts, master penetration attacks, and maintain permissions , Trace removal and defense methods. After several years of practice, students' engineering practice ability has been improved, professional practice level and employment quality have been significantly improved.

4. CONCLUDING REMARKS

Since the "Prism Gate" incident in 2013, cyberspace security has become a hot spot of concern worldwide, and cyberspace security has become an important part of the national security strategy. Following the approval of the Ministry of Education in 2001 to establish an information security major, in June 2015, "cyberspace security" was added as a national first-level discipline. The establishment of the first-level discipline is aimed at implementing national security strategies and not only

helps to accelerate the high-level cyberspace security. Talent training also puts forward higher requirements for discipline construction and talent training system. Based on the analysis of the concept and connotation of cyberspace security, this article summarizes the experience of more than 10 years of information security professional construction in Chengdu University of Information Technology, and gives suggestions on the construction and practice of the cyberspace security innovation talent training system.

ACKNOWLEDGMENTS

This paper is supported by Sichuan Science and Technology Program 2019YFG0408 and 2018GZDZX0011.

REFERENCES

- [1] China Internet Network Information Center. The 46th "Statistical Report on Internet Development in China"[J], 2020.
- [2] Research and Argumentation Working Group of the Ministry of Education for the First-level Discipline of Cybersecurity[R]. The Argumentation Report on the First-level Discipline of Cyber (space) Security. Beijing: Ministry of Education, 2014
- [3] Zhou Guomin etc. A preliminary study on the training of information network security supervision talents based on school bureau cooperation[J].Journal of Guizhou Police Vocational College,2010.
- [4] Zhang Shabin.The reform and practice of the training model of innovative engineering talents in information security [J].Contemporary Educational Theory and Practice, 2012
- [5] Li Jianhua.Thinking about the connotation construction and talent training of cyberspace security first-level discipline [J].Information Security Research, 2015,
- [6] Zhang Shabin.The reform and practice of the training model of innovative talents for postgraduates majoring in information security [J].2015