

Innovation and Practice of Cyberspace Security Course based on Network Range

Chang Liu

College of Information and Communication, National University of Defense Technology,
Wuhan 430010, China.

Abstract

The network range refers to the simulation of the attack and defense environment of the real Cyberspace by the combination of the virtual environment and the real equipment. This paper discusses the role and position of the network range in the Cyberspace Security Course, introduces the course content and teaching method design based on the "Teaching, Practice, Discussion" 3-segment class. In view of the problems of the teaching resources and the teaching methods of the cyber space security course, this paper puts forward the case resource construction process based on cognitive ability, teaching by encapsulating knowledge points with cases and under the guarantee of the training platform, promote the cultivation of the students' ability of practical innovation, and form case-driven cyberspace security teaching in practice.

Keywords

Network range; Cyberspace Security; Curriculum; Innovation; Practice.

1. Introduction

Network range, also known as the national network range, refers to the simulation of the real cyberspace attack and defense operation environment through the combination of virtual environment and real equipment, which can support the research of cyberspace combat capability and the verification test platform of cyberspace weapon. The network range will provide a simulation environment for the country to build a real network attack and defense operations, and test the electronic warfare means such as hostile electronics and network attacks. The network range will establish a special test platform for the country to verify the information security system, and share research data with relevant departments to improve the national information security level [1]. General Secretary Xi pointed out that "without network security, there will be no national security" and asked us to "strengthen the construction of Cyberspace Security talents and build a team of talents with excellent quality and strong combat effectiveness". In order to implement the national security strategy and speed up the training of high-level talents in Cyberspace Security, the central office of cyberspace, the Ministry of education, the national development and Reform Commission, etc. jointly issued the "opinions on strengthening the construction of network security disciplines and personnel training" in June 2016, and put forward eight opinions on "strengthening the construction of disciplines and personnel training of network security college" [2]. In order to adapt to the development of society and school, the undergraduate teaching oriented by the needs of professional talents must have its own characteristics to adapt to the cultivation of College Students' innovative spirit and innovation and entrepreneurship ability. Therefore, we should actively explore a teaching method of Cyberspace Security Course for network range and apply it to practice [3].

2. Problems in the Teaching of "Cyberspace Security"

2.1. The Conflict between the New and Curriculum Systems

Network security is a complex information system composed of many subsystems, which integrates information science, such as communication and system, computer and application cryptography, software engineering and communication engineering. Teachers engaged in network security research need to have profound professional basic knowledge, keep pace with the times, and timely understand the technical characteristics and latest progress of professional frontier application fields, such as cloud computing, blockchain and artificial intelligence[4]. In the traditional teaching system, the curriculum is relatively conservative, the theory is complex and redundant, the students lack of interest in learning, it is difficult to combine the actual system to learn and apply, resulting in obstacles to the understanding of the knowledge system; part of the curriculum based on the new field is more important than the form, only introducing real-time and real-time engineering cases, bringing too much design principles and ideas, making it difficult for students to form a deep understanding of the subject Thinking in a systematic way.

2.2. The Collision between the New and Old Teaching Systems

On the one hand, the innovation and entrepreneurship resources in cyberspace security field are rich, the practice forms are diverse, and the industry ideas advocate freedom and independence. However, the management and evaluation system of traditional teaching system is solidified, which is based on the curriculum and practical activity settings, and centered on the examination and evaluation system[5]. It can not meet the students' free choice of interests, and teachers can not select excellent innovation and entrepreneurship The backward teaching system of Cyberspace Security Talents with potential and excellent research ability has gradually become an obstacle to the development of students; on the other hand, the integration of the new system is difficult: although emerging teaching measures and systems are emerging gradually, such as science and technology competitions, business incubation platforms and self selected courses, they cannot be reasonably integrated into the system, because of the different quality of practical activities, they cannot be guaranteed Every student has gains in practical activities. The evaluation and quantification of their achievements are difficult to integrate into the existing evaluation indicators, and the actual operation is easy to cause controversy.

2.3. The Disjunction between Basic Teaching and Innovative Research

The existing basic teaching is limited to the knowledge in the textbook. Due to the limitation of class hours and the arrangement of teaching tasks, teachers can only complete the teaching plan step by step, rarely discuss with students, mainly to train students' ability of understanding and memory of knowledge points, and to cultivate students' ability of scientific thinking and independent thinking in innovative research. Try to avoid the inadaptability or self-confidence of undergraduates to scientific research work after entering the postgraduate or doctoral stage, which leads to the teaching effect and the goal of training basic teaching talents in cyberspace security field.

3. Optimization and Innovation of Cyberspace Security Course based on Network Range

3.1. Building a Complete Teaching Resource Environment

Efforts should be made to build an information platform for teaching resources, increase resource investment in software and hardware of the network range, enrich teaching forms, and optimize teaching practice experience; teachers should follow the idea of "student-

centered, teacher led" to teach courses, which are not limited to textbooks, but integrate basic concepts and protocols into the actual open system of the network range, and encourage students to join in traditional programs Self design; in class discussion, teachers use heuristic questions to deepen students' understanding of knowledge, focus on students' abstract thinking, active practice awareness, and the cultivation of independent innovation ability; teachers encourage students' teams to use their spare time to learn, complete the construction of programs, and project development through research-based project design in the context of curriculum With exhibition, teachers find a balance point in the collision of the new and old curriculum system, and realize the innovative practice of learning in research in the curriculum system [7]. Take the information security major as an example, conduct in-depth research on relevant sectors of the society, closely contact and exchange with enterprises and other scientific research institutes, pay attention to the social demand feedback on the knowledge and skills of Cyberspace Security talents, on the one hand, adjust the training plan and teaching plan according to the basis, on the other hand, establish a prediction model for the future demand and development of Cyberspace Security talents Based on the key laboratory and equipment planning projects of related disciplines, we have set up a curriculum system for Cyberspace Security related majors.

3.2. Case-practice Driven Teaching

In view of the practical problems faced by the teaching reform of "Cyberspace Security", the author, through thinking and communication, puts forward to create an independent and diversified research and innovation practice environment for students from the two aspects of curriculum system reform and extracurricular practical activities, combined with the current research hotspot in the field of Cyberspace security. It mainly focuses on the current hot technology fields of network range, including system security, network security, web security, cryptography principle and application, basic course research of network space security, etc. Considering the training plan, teaching objectives, teaching contents, teaching methods, teaching means, development trend and the development and application of curriculum system reform of Cyberspace Security direction courses, the relevant courses are designed carefully.

Based on the relevant case resources, based on many classic and similar business project cases, in the form of practice, to improve the students' interest in the application of professional fields and stimulate the ability of hands-on innovation. In teaching practice, through case encapsulation and explanation of key knowledge points, students can break through the cognitive limitations of traditional theory teaching methods. In students' innovative thinking, only theoretical innovation is not enough. At the same time, practical innovation of finding, thinking and solving problems should be found more widely. Under the requirements of project tasks, objectives, guidelines and other supporting documents and team cooperation, establish project development milestones, and have multi process control and checkpoints, so as to systematize development process control, and use real test tools to evaluate the effect of project development or practice in the real test environment.

3.3. Promoting the Cultivation of Students' Innovation Ability through Practical Training

The courses of Cyberspace Security related majors are closely related to the network range. Therefore, we should strengthen cooperation with the information industry department, focus on the construction of a training base integrating production, learning and research, and open up channels for students to connect with the society, so that students can understand the real project needs and receive standardized training. It mainly includes three levels: professional course implementation, practical training course implementation and completion and practice implementation. Different implementation levels are completed under the environment guarantee of online learning platform and offline training platform. Under the training of

different projects in the network range platform, students can achieve qualified professional ability of network security technology when they finish their studies, for example, in the aspect of basic discipline theory, The courses of "Introduction to information system security", "algorithm design and analysis", "formal language and automaton theory" are added to help students establish a forward-looking professional cognition of network range and consolidate the theoretical basis of the specialty; in terms of professional theory, the comprehensive courses of "software security design", "large information system analysis and design", "network space security situation awareness" are added Combined courses advocate thinking from the perspective of network range system security, and provide more opportunities for theory and practice; for cutting-edge technologies in the field, elective courses such as "block chain principle and technology", "Internet of things security" are added for students to study and explore.

4. Practice of Cyberspace Security Course Construction based on Network Range

4.1. Course Content Design

At home and abroad, the training objectives of Cyberspace Security Major in the undergraduate stage are all focused on the basic knowledge and skills of Cyberspace Security, emphasizing the technical practice ability of students. Therefore, the course can be designed in two parts: Theory and experiment. Taking the Internet and the world wide web as the main research objects, focusing on the network security issues around the structure and behavior characteristics of the network, and according to the idea of "structure behavior" to design the network science curriculum content system.

Based on the basic concepts and models, the theoretical content focuses on the analysis of network range and network security issues, such as network attack and defense game, network robustness analysis under attack, etc., emphasizes the specific application of network range in network security issues, and cultivates the ability of students to apply network science theory to the analysis of network security issues. In the experiment part, students are asked to explore the specific application of network science theory by creating specific application scenarios of network security problems, and use computer technology to complete the problem-solving process.

With the rapid development of the field of network science, there are more and more textbooks of network science course in recent years, but at present, there is no textbook that is fully suitable for the content of this course. There are still some problems in the application of network range and network security. Therefore, in the specific implementation of teaching, the paper and other supplementary materials are distributed to supplement the relevant teaching content.

4.2. Teaching Method Design

In view of the strong theoretical nature of the network science course, focusing on the problem that the model is difficult to understand and apply, the principle of "appropriate mathematical derivation, strengthening scientific thinking, and focusing on safe application" should be followed in teaching. In the teaching implementation, it is based on the three-stage classroom model of "teaching, practice and discussion" [8].

4.2.1. Teaching

The teaching link takes up the time in class. The teaching objective is not all theoretical content, but essential basic concepts, theorems and methods. It is mainly to help students build the "skeleton" of network range knowledge. In terms of teaching methods, it mainly integrates case-based teaching method and scaffolding teaching method. Through actual network security

cases, it can stimulate students' interest, understand the application environment of theory, induce students to further analyze problems, and provide students with scaffolding in the process of solving problems, so as to help students form an overall understanding of problems and cultivate scientific thinking.

4.2.2. Practice

According to different topics, the implementation of the practice link is different. The practice link takes up the time in class, and the content is the experimental content. The practice link takes up the time after class, and the content is written homework. Experiments and written assignments are both the practice of important theories and methods in the teaching content, but the scale and practice mode of the practice objects are different.

4.2.3. Discussion

The discussion will take up all the time in class. In terms of teaching methods, the whole process of situational teaching method is practiced by practice and discussion. In practice, students can explore and practice independently by setting up a situation close to students. In discussion, students can further deepen their understanding of the content through classroom display, collaborative discussion of problems and teacher evaluation, and finally achieve the fullness of knowledge "flesh and blood". For example, taking the best attack and defense strategy calculation experiment subject in a given scenario as an example, the teaching design of practice and discussion is given. Under the guarantee of the training platform, promote the cultivation of the students' ability of practical innovation in the project, and form the characteristic and project driven cyberspace safety teaching in practice.

5. Conclusion

Although the construction of Cyberspace Security Specialty started late, its development is relatively fast by learning from the rich experience of network engineering, information security and artificial intelligence specialty construction. For the construction of Cyberspace Security Specialty, on the one hand, we should fully understand its professional characteristics, form a unique talent training mechanism, and achieve the goal of talent training; on the other hand, we should pay full attention to the role of network range in the construction of Cyberspace Security Specialty, encourage the construction of interdisciplinary science, and train all-round Cyberspace Security technical talents. In view of all kinds of problems that need to be solved in the connection of curriculum system, teaching system and teaching research in teaching practice, we should build a heuristic, discussion and research-based teaching environment, guide students to start from innovative projects in the curriculum, and cultivate their interest in academic research and engineering practice. In view of the current hot technologies of Cyberspace Security, the courses related to cyberspace security are carefully designed. Facing the construction of network range teaching resources, based on the project case encapsulation and cognitive ability, to create real engineering project case development teaching resources, under the guarantee of practical training platform, to promote the cultivation of students' project practice and innovation ability, to help students standardize training, technical qualification and quickly realize the transformation of future engineering role, and to form a distinctive, network-based in practice The teaching method of Cyberspace Security in the range.

References

- [1] B.X. Fang, Y. Jia, A.P. Li, W.Z. Zhang. Research on cyberspace range technology [J]. Journal of information security, 2016,1 (03): 1-9.

- [2] J. Wang, G.S. Zhao, Z.G. Zhao, et al. Construction and optimization of Cyberspace Security Curriculum System [J]. Teaching and Education (Higher Education Forum), 2019 (21): 72-73.
- [3] H. Qiu, Q.X. Wang, J.h. Zhu, Y.F. Li. Exploration of network science curriculum construction of Cyberspace Security Major [J]. Computer education, 2019 (07): 89-92.
- [4] L.F Xuan. Design and implementation of Cyberspace Security range in Colleges and universities [J]. Science and technology horizon, 2019 (11): 87-8.
- [5] Z.G Liu, Z.M Yu, J. Wang, L. Zhang, K.S Li, H. Shen. Research on future oriented network range Architecture [J]. Information technology and network security, 2018,37 (06): 41-46.
- [6] J. Xu. Design and implementation of virtual operating environment for training platform of network range [D]. Southeast University, 2018.
- [7] Y. Wu, Y.J. Wang, Z. Xue. Design of attack and defense range for cyberspace [J]. Communication technology, 2017,50 (10): 2349-2356.
- [8] G.S. Zhao, J. Wang, S.M. Li, X.H. Chen, Wang Meng. Practical teaching design of Cyberspace Security Course [J]. Computer education, 2017 (08): 178-182.