Eurasia Journal of Science and Technology
ISSN: 2663-1016
DOI: 10.61784/ejst3006

RESEARCH ON TALENT CULTIVATION IN CYBERSECURITY UNDER THE BACKGROUND OF NEW ENGINEERING DISCIPLINES

Xiong Wei, BangChao Wang*, Hang Luo, YingKai Yuan
School of computer Science and Artificial Intelligence, Wuhan Textile University, Wuhan 432022, Hubei, China.
Corresponding author: BangChao Wang, email: 576728902@qq.com

Abstract: In the current rapid and stable economic operation, network security is an important cornerstone to safeguard national security and the interests of the people. The rapid development of new technologies and applications such as blockchain, virtual reality, smart IoT, and artificial intelligence has spawned a series of new formats and models. In the context of the new engineering disciplines, there exist problems in the cultivation of talents in the field of network security, such as insufficient integration of disciplines, lack of teaching staff, and insufficient cultivation of comprehensive qualities. This paper explores the cultivation methods of talents in the field of network security under the background of the new engineering disciplines from three aspects: strengthening the practical ability of interdisciplinary integration, expanding international perspectives and continuous learning ability, and cultivating teamwork and social responsibility.
Keywords: New engineering disciplines; Interdisciplinary integration; Network security

1 INTRODUCTION

President Xi's speech at the first meeting of the Central Leading Group on Cyber Security and Informatization in February 2014 stated that without cyber security, there would be no national security, no stable economic and social operations, and it would be difficult to protect the interests of the broad masses of the people [1]. President Xi pointed out in the "Speech at the National Symposium on Cyberspace Security and Informatization Work" in April 2018 that "cyberspace security and informatization are strategic issues for national security and development, a new field of military struggle, and an opportunity to win." , New means of winning from the commanding heights "The importance of cyberspace security has become increasingly obvious in today's digital society. With the popularization of the Internet and the rapid development of information technology, the network has become the core infrastructure in various fields such as business, government, education, and social networking. Cultivating and possessing high-quality cyberspace security talents is crucial. These professionals can ensure the security of network systems and prevent and respond to various network threats.

1.1 Cyberspace Security

Cyberspace security is a discipline dedicated to the study and practice of protecting the security of network systems, data and communications. It covers many aspects, including network security, information security, computer security, cryptography, etc. Students majoring in cyberspace security usually need to learn computer science, network technology, information security regulations, risk management and other related knowledge. After graduation, they can work as network administrators, information security analysts, security engineers, risk management experts and other positions in various organizations, providing network security protection services for enterprises and government agencies [1]. There are certain differences between the three majors of cyberspace security, information security and network security. The foothold of cyberspace security lies in space, namely the four major areas of sea, land, air and space. The foothold of information security lies in information, the security of information during transmission, that is, the security of the information itself, uninterrupted, not tampered with, intercepted, and generally refers to various information and data. The foothold of network security lies in the entire network, ensuring the normal operation and security of the network.

1.2 Importance of Cyber Security

The importance of cyberspace security has become increasingly apparent in today's digital society. Especially its importance to individuals, organizations and society is becoming more and more obvious:
First, individuals generate a large number of digital footprints on the Internet, including personal information, social media activities, financial transactions, etc. The importance of cyberspace security lies in ensuring that personal privacy is not illegally accessed and abused. Secondly, cyberspace security ensures the safety of online banking, electronic payment, financial fraud, and e-commerce activities, and prevents the theft and abuse of financial information. Enterprises and organizations store and transmit a large amount of sensitive information on the Internet, including business plans, research and development results, customer data, etc. The maintenance of cyberspace security ensures that these business secrets are not accessed and leaked without authorization [1].

In the digital economy era, enterprises and countries rely on the Internet for business activities. Maintaining cyberspace security helps create a safe, stable and trustworthy network environment, promoting economic development and business activities. In cyberspace, the integrity of information is crucial. Cyberspace security ensures that information is not tampered with during transmission and storage, and maintains the credibility of information[4][5]. The country's critical infrastructure, government agencies and military systems all rely on the Internet. Maintaining cyberspace security is crucial to national security and can prevent threats such as cyber attacks and information warfare. The importance of cyberspace security lies in preventing all kinds of cyber crimes, including online fraud, telecommunications fraud, and malware propagation. This helps protect individuals, businesses and society from criminals.

Maintaining cyberspace security helps prevent and respond to various types of cyber attacks, including malware, ransomware, distributed denial of service attacks, etc. As a global network, the importance of cyberspace security is related to cooperation and exchanges between countries. Ensuring the security of cyberspace helps promote global connectivity, international cooperation and information sharing.

Cyberspace security is vital to individuals, businesses and society as a whole, and its maintenance involves many aspects of technology, regulations and awareness. With the continuous development of science and technology, the importance of cyberspace security will continue to increase.

1.3 The Importance of Cultivating Cyberspace Security Professionals

Talent is the key to the competition in cybersecurity. The key to a clean and clear cybersecurity space lies in people and relies on people. my country has a huge population of 710 million people on the cyber front, and the construction of a security protection network cannot be separated from professional core talents[3]. During the 2019 National Cybersecurity Publicity Week, General Secretary President Xi made important instructions to adhere to the integrated development of cybersecurity education, technology, and industry, and to form a benign ecology of talent training, technological innovation, and industrial development[4]. In the current global cyberspace competition, cyberspace security technology and talents are the red line of absolute discourse power and sovereign security.

According to the Internet Security Report, my country's major industries currently need about 700,000 cybersecurity talents of all kinds, with a gap of 95%. It is estimated that by 2027, there will be a gap of 3.27 million cybersecurity personnel in my country, while the talent training scale of colleges and universities is 30,000 per year. Many industries are facing a serious shortage of cybersecurity talents[1]. In this sense, instead of calling for "talents in all kinds of ways", it is better to "cultivate talents in all kinds of ways". Although there are some "hackers", this requires systematic professional training under the background of new engineering. There is a serious lack of truly original and systematic high-level talents. "The training of cyberspace security talents in the teaching and scientific research system is a key move to occupy the high ground of cybersecurity[6].

In 2016, my country awarded a large reward to cybersecurity talents for the first time, which shows that the country attaches great importance to professional, leading and compound talents in the field of cybersecurity. Cyberspace is the fifth territory to be explored after land, sea, air and space. If we take the lead in occupying the talent high ground and building a talent echelon, the cyber world will return to rationality and order, and the vast dream will be more smoothly reflected in reality.

2 TRAINING OF CYBERSPACE SECURITY TALENTS AT HOME AND ABROAD

According to the White Paper on the Practical Capabilities of Cybersecurity Talents issued by the Ministry of Education, by the end of 2021, 215 universities in my country have opened cybersecurity majors, more than 60 universities have established cyberspace security colleges, 11 universities have been approved as national first-class cybersecurity colleges, 37 universities have been approved as first-level doctoral programs in cyberspace security, and 16 universities have established cyberspace postdoctoral research stations [8][9][14]. The cyberspace security major of Beijing Institute of Technology cultivates high-quality engineering and technical talents who are oriented towards the field of cyberspace security, can serve national strategies, meet the needs of economic and social development, have lofty ideals and beliefs, excellent professional knowledge, sound physical and mental personality, profound humanistic qualities, broad international vision, can propose, analyze and solve complex engineering problems with a systematic perspective, and are competent for scientific exploration, technical research, product development, education and teaching, and management work in this professional field and related fields. Beihang University has signed strategic cooperation agreements with 18 cybersecurity companies, including 360 Technology, Qi'anxin, Tencent, Venusstar, and Sangfor, to cooperate deeply with cybersecurity companies, jointly educate talents, and jointly tackle key problems. Focusing on the four directions of discipline construction, we have made great progress in talent training goals, curriculum setting, textbook compilation, and practice. Strengthen cooperation in teaching, research and other aspects.

The 2023 Corporate Cybersecurity Compliance Survey Report released by the UK Department of Science and Technology shows that 32% of small and medium-sized enterprises have suffered data leaks and security attacks in the past 12 months. The average cost of corporate network application violations is £1,100, and the average cost for large and medium-sized enterprises is £4,960. In order to deal with cyberspace security, the British government has taken a series of measures to establish a certification training program to improve the professional level of professionals engaged in cybersecurity and information assurance; strengthen postgraduate education and expand the pool of experts

with cyberspace security expertise; and establish a cybersecurity research institute to conduct research to confirm the model, nature and extension of cybersecurity skills [10][11]. The demand for cybersecurity talents in the government, public sectors and industry is still growing [4]. The United States has a very mature management and talent training system and has established a high-level cybersecurity talent training system. For example, it has classified and formulated a standardized framework for the training of cyberspace security professionals in accordance with various knowledge and ability spectrums in the field of cybersecurity, and focused on practical ability training. In addition, in order to meet the needs of the government and society for urgently needed cybersecurity talents, the United States has broken through the obstacles in the management mechanisms of powerful departments and some public sectors. For example, the U.S. Department of Defense's Cyber Special Operations (CES) and the Department of Homeland Security, which is responsible for civilian critical infrastructure, have begun to play a role in setting up similar personnel sequences.

3 DEFICIENCIES IN THE TRAINING OF CYBERSPACE SECURITY TALENTS

Although both China and foreign countries have increased their efforts in the training of cyberspace security professionals, due to some reasons, the training of cyberspace security talents faces a series of defects, which may affect students' actual abilities and their ability to adapt to industry needs.

(1) Outdated curriculum. The cybersecurity curriculum of some colleges and universities lags behind industry demand and cannot reflect emerging technologies and threats in a timely manner, resulting in students lacking the latest practical application knowledge after graduation[7][8].

(2) Insufficient practical experience. Some training institutions and universities lack sufficient practical operation and experience in the process of cybersecurity professional training, which makes students feel uncomfortable when facing practical problems [8].

(3) Lack of comprehensive quality training. In the process of cybersecurity talent training, sometimes too much emphasis is placed on the technical level, while the cultivation of students' comprehensive qualities, such as communication skills and teamwork skills, is neglected [9].

(4) Insufficient teaching staff. The teaching staff of cybersecurity majors in some schools is relatively weak, resulting in the inability of teaching level and teaching resources to meet students' needs.

(5) Insufficient cross-disciplinary integration. There is a lack of cross-disciplinary integration with journalism, law, intelligence and communications [7][8][9].

(6) Lack of industry-recognized certificate training: Some schools and training institutions have failed to fully integrate industry needs and lack relevant certification courses. Students face competitive pressure in the job market after graduation [14].

4 DESIGN AND IMPLEMENTATION OF TRAINING MODEL

In the context of New Engineering, we should strengthen interdisciplinary and cross-border integration, and focus on cultivating engineering talents with innovative ability, practical ability and teamwork spirit. Cybersecurity talent training should also have a series of new characteristics and comprehensive abilities. Cyberspace security talent training under the background of New Engineering should be strengthened in the following aspects:

(1) Strengthening the improvement of interdisciplinary integration and practical ability. New Engineering emphasizes the interdisciplinary training model. Cybersecurity talents should have multi-field knowledge. They should not only understand computer science and network technology, but also have knowledge of related fields, such as law, psychology, management, etc. Cybersecurity talents should improve their ability to solve practical problems through actual projects, experiments and drills. Practical training can include activities such as simulated network attack and defense, vulnerability mining, and emergency response. New Engineering focuses on cultivating innovative ability. Cybersecurity talents should have innovative thinking to discover new vulnerabilities and propose new security defense mechanisms. Students are encouraged to participate in scientific research projects in the field of security to cultivate independent thinking and problem-solving abilities.

(2) Broadening international vision and continuous learning ability: Cross-internationalization is one of the goals of New Engineering training. Cybersecurity talents need to understand the latest international security threats, technologies and standards. Students are encouraged to participate in international security competitions and cooperation projects to enhance their international competitiveness. The field of cybersecurity is changing rapidly. New engineering disciplines should cultivate students' awareness and ability of continuous learning, encourage them to participate in industry certification, seminars, training and other activities, and continuously improve their professional level.

(3) Cultivate teamwork and social responsibility. Cybersecurity issues usually require teamwork to solve. The training of cyberspace security talents in new engineering disciplines should emphasize teamwork and communication skills. Cultivate students to play different roles in the team, The ability to solve complex problems. New engineering advocates that engineering talents have a sense of social responsibility. Cybersecurity talents should understand the importance of their work to society, pay attention to the impact of information security on society, and their social responsibility in ensuring cybersecurity.

Through the characteristics of these new engineering disciplines, we can strengthen the integration of knowledge with fields such as journalism, law, and psychology, enhance the improvement of interdisciplinary practical capabilities,

broaden international perspectives and continuous learning capabilities, and cultivate teamwork and social responsibility. In the context of new engineering disciplines, we can cultivate more comprehensive talents with strong innovation capabilities and better adaptability to future cyberspace security.

COMPETING INTERESTS

The authors have no relevant financial or non-financial interests to disclose.

FUNDING

This article is supported by a grant of National Natural Sci-ence Foundation of China (Major Program) (program 92367201).

REFERENCES

[1] Li Qiang. Review meeting of "Planning Scheme for Urban Internet of Things Key Management System Based on Domestic Cryptographic Algorithms" was held in Beijing. China Construction Informatization, 2019(3): 2. DOI: CNKI:SUN:ZGJS.0.2019-03-022.
[2] Yuan Sheng. Training of network security talents for practical combat. China Information Security, 2023(3): 47-48.
[3] Wu Jianping. Cyberspace security is actually a competition for high-level talents. China Education Network, 2016(10): 1.
[4] Wang Xing. Research on the construction system of network security talent team in the UK. China Information Security, 2015(11): 101103. DOI: 10.3969/j.issn.1674-7844.2015.11.038.
[5] Yin Libo. Pay attention to Cybersecurity talent training. China Information Security, 2014(12): 1. DOI: 10.3969/j.issn.16747844.2014.12.038.
[6] Li Xueying. Optimizing cybersecurity budget management mechanism and promoting cybersecurity talent training. China Information Security, 2023(4): 52-54.
[7] Wang Xing. Prospects of Biden administration's cybersecurity talent strategy. China Information Security, 2023(3): 43-46.
[8] An Shuzhao, Wan Xiaoyan. Research on cybersecurity talent training mechanism in the new era. Internet Weekly, 2023(7): 36-38.
[9] Wang Lei, Xu Zijing, Zhu Ge, et al. Exploration of generative artificial intelligence empowering cybersecurity talent training. China Audio-visual Education, 2023(9): 101-108.
[10] Yin X. Research on Training Strategies of High-level Practical Skills of Network Security Talents. ICEMBE 2023. DOI: 10.23977/ICEMBE2023.069.
[11] Buttyán L, Félegyházi M, Pék G. Mentoring Talent in {IT}{Security–A} Case Study//2016 USENIX Workshop on Advances in Security Education (ASE 16). 2016.
[12] Liu Z, Wang N. A New Experiment Teaching Mode for Network Security & Law Enforcement Major to Meet the Need of New Engineering Talent Training//2019 3rd International Conference on Education, Economics and Management Research (ICEEMR 2019). Atlantis Press, 2020: 214-217.
[13] Yamin M M, Erdodi L, Torseth E, et al. Selecting and Training Young Cyber Talent: A Recurrent European Cyber Security Challenge Case Study//International Conference on Human-Computer Interaction. Cham: Springer International Publishing, 2022: 304-321.
[14] Xiang Jizhi. Strengthening industry-university cooperation to improve the quality of cybersecurity talent training: An interview with Feng Huamin, Secretary General of the Ministry of Education's Higher Education Cyberspace Security Professional Teaching Committee. China Information Security, 2023, (03): 27-30.