

# Research on the Strategies of Institutions in Carrying Out Cybersecurity Education Work under the Overall National Security Outlook

Qian Jin, Du Fang, Zhang Kaiyuan

*NonCommissioned Officer Academy of PAP, Hangzhou, Zhejiang, China*

**Abstract:** The overall national security concept is a comprehensive strategic concept covering both traditional and non-traditional security areas, and serves as the basis and guidance for national security strategy. The concept highlights the systemic nature of national security, focuses on preventing multiple risks, and safeguards the core interests of the country from an all-round perspective. As the training and output base of all kinds of talents, the establishment of the overall national security concept is especially important while focusing on skill improvement. Network security work is the important foundation of all online work, and it is the guarantee for the smooth implementation of the work of institutions. This paper mainly discusses the strategy of carrying out network security education work in institutions under the overall national security concept.

**Keywords:** Overall National Security Concept; Cyber Security Education Work; Higher Vocational Colleges and Universities

## 1. Introduction

General Secretary Xi Jinping pointed out that we should take the establishment of the National Security Education Day as an opportunity to take the overall concept of national security as a guide, fully implement the national security law, carry out in-depth national security publicity and education, and effectively enhance the national security awareness of the whole nation. The purpose of network security education work in higher vocational colleges and universities is to cultivate students' awareness of network security and ensure that they can effectively respond to information network security management issues in their future careers. This educational work involves a variety of fields and emphasizes the

establishment of the concept of network security in daily learning. Higher vocational colleges and universities incorporate cybersecurity education into their curricula and encourage students to actively participate in cybersecurity training, learn relevant cyber skills and master the necessary related skills.

## 2. The Necessity of Cybersecurity Education in Institutions under the Overall National Security Outlook

The overall national security concept advocates the protection of national security from multiple levels, and as a talent training base, strengthening cybersecurity education in colleges and universities can effectively safeguard national security. Institutions as a place of knowledge dissemination, the network is more likely to become a source of information leakage, the potential risks can not be ignored, it is necessary to cultivate students' awareness of network security. Institutions to carry out network security education can strengthen the information security management of institutions to prevent security risks and avoid the impact on society. In addition, modern technology and informationization environment puts forward higher requirements for information security, and the wide application of social media in institutions can accelerate the speed of information dissemination. Institutional cybersecurity education responds to this environmental change and helps to improve students' adaptability to informationization. Digital information spreads easily and may trigger chain reactions inside and outside the institution. Cybersecurity education emphasizes the proper handling of sensitive information, cultivates students' awareness of cybersecurity, and helps them master the skills of protecting national information security in the informatization environment. Compliance with professional

ethics is one of the core contents of cybersecurity education in institutions. Students will enter different positions after graduation, and compliance with professional ethics is the foundation of their career, and cybersecurity education in institutions shapes the students' view of professional ethics by teaching relevant laws and regulations. Students acquire knowledge of cybersecurity and develop a sense of compliance in their studies, preparing them to follow regulations in the workplace in the future.

Second, the strategy of network security education in institutions under the overall concept of national security

### **2.1 Integration of Curricula and Practical Training**

Under the overall national security concept, the integration of courses and practical training in institutions can cultivate students' awareness of network security and enhance their ability to respond to information security. The combination of curriculum and practical training ensures that students can master theoretical knowledge and also apply what they have learned in a real environment. The integration of curriculum and practical training promotes the transformation of network security education from the traditional teaching mode to the practical direction, and provides an effective way to cultivate high-quality network security talents.

Institutions can introduce cybersecurity education content into their curricula, combining it with specialized knowledge. Case studies related to cybersecurity are embedded in each professional course to guide students to understand the importance of cybersecurity when learning professional knowledge. At the stage of curriculum design, institutions can introduce cybersecurity experts to participate in the planning of curriculum content to ensure that the curriculum content not only meets the requirements of the overall national security concept, but also fits the professional reality. Institutions set up lectures on cybersecurity, inviting authoritative experts in the field of cybersecurity to share their experience and teach students the latest cybersecurity technology, so as to enhance the realism of the course content. Practical training is an important part of the integrated curriculum, and institutions can create a real environment for

network security practice through laboratories. Virtual network security laboratories are built to simulate various network security scenarios, and students are required to handle network sensitive information in the simulated environment to test their network security skills. Institutions can cooperate with Internet organizations to provide training opportunities, and have the chance to experience the real cybersecurity working environment first-hand during off-campus training. Students participating in the internship are required to sign a network security agreement and undergo rigorous network security training. Students exposed to network security tasks in the real work environment can apply the knowledge learned in the course to practice and consolidate their network security awareness. Network security education can also be combined with institutional cultural activities, institutions can organize network security cultural festivals, institutional cultural activities to provide a platform for students to demonstrate their abilities, encourage students to actively participate in network security-related activities, and cultivate students' awareness of network security.

### **2.2 Establishment of a Multi-Level Network Security Training System**

The establishment of a multi-level cybersecurity training system in institutions helps to develop students' professional skills and ensure that students at different levels receive targeted training. The design of a multi-level cybersecurity training system allows cybersecurity education to be matched to the students' stage of study and promotes the long-term effects of cybersecurity education. Multi-level cybersecurity training by institutions can provide customized cybersecurity education content to meet the needs of different learning stages, ensuring that every student can receive appropriate training. Through the relevant training sessions as an opportunity to promote students to strengthen the bottom line thinking, enhance the awareness of prevention, and build a strong network security defense line. At the same time, we adhere to the problem-oriented approach, focus on the weaknesses and risks of network security, and continuously strengthen the construction of human, technical and institutional defenses to build a "brick wall" of network security.

At the basic level, institutions can carry out basic cybersecurity training at the stage of new student enrollment, invite cybersecurity experts to give lectures, popularize general knowledge of cybersecurity and relevant laws and regulations, and help students understand the basic requirements of cybersecurity. Organize network security knowledge tests for new students to ensure that all students have basic network security knowledge reserves. Incorporate cybersecurity education into freshmen's entrance education to give students a preliminary understanding of cybersecurity principles. At the intermediate level, institutions can set up specialized cybersecurity training for the cybersecurity requirements in professional courses. Teachers of each professional course will cooperate with cybersecurity experts in designing the course content, so that cybersecurity education can be integrated into professional learning. Regular seminars on cybersecurity knowledge will be held, and cybersecurity experts in specialized fields will be invited to interact with students and answer cybersecurity questions encountered by students in the course of their studies. Institutions can provide a cybersecurity skills assessment mechanism to ensure that students meet the basic standards of cybersecurity skills through practical operational tests. At a high level, for students who are about to graduate, institutions can set up high-level cybersecurity training programs and invite senior cybersecurity experts in the industry to share their practical work experience and cybersecurity cases, so as to help students understand the cybersecurity requirements in the workplace. Institutions can also set up a cybersecurity training certification system and issue cybersecurity skills certificates to encourage students to actively participate in training and improve their cybersecurity skills. In addition, institutions can establish a mentor system for cybersecurity education, inviting industry experts to serve as mentors for students, providing personalized cybersecurity guidance, and helping students equip themselves with cybersecurity skills in the early stages of their careers. Through the multi-level cybersecurity training system, institutions can ensure that every student can obtain appropriate cybersecurity training at all stages of their learning career, and promote the comprehensive development of cybersecurity education in institutions.

### **2.3 Strengthening the Information Security Infrastructure of Institutions**

Under the overall national security concept, the information security infrastructure of institutions has become a key element in safeguarding network security education in institutions. Nowadays, with the rapid flow of information and the wide application of technology in institutions, strengthening the information security infrastructure can help prevent information leakage and network attacks and ensure the security of internal data in institutions.

Strengthening an institution's information security infrastructure requires both physical and cyber dimensions. In the physical dimension, institutions can strengthen their surveillance systems by installing high-definition cameras in key areas to ensure that cybersecurity areas within the institution are monitored. Network centers establish access control systems and use biometrics to ensure that only authorized personnel have access to sensitive areas. Set up warning signs for cybersecurity areas to remind students and faculty of the importance of cybersecurity. Enhance management of key areas such as computer rooms and laboratories with professional security personnel to prevent unauthorized personnel from entering. At the network level, institutions can deploy advanced network security equipment to ensure the security of the institutional network, install firewalls and intrusion monitoring systems, real-time monitoring of the institutional network, timely detection of abnormal behavior, and the establishment of data encryption mechanisms to ensure that data is protected. Institutional networks need to set up multi-level permissions, strictly control the access rights of different users to prevent unauthorized access, regular network security audits, check network security vulnerabilities, to ensure the stability of the information security infrastructure. Strengthening the information security infrastructure of the institution also needs to pay attention to the information security education within the institution, and carry out information security publicity activities throughout the university to popularize the knowledge of network security to teachers and students. Set up network security training courses to help teachers and students understand network

security risks and master countermeasures. Organize information security drills to simulate cyber-attack scenarios and test the institution's information security emergency response capabilities. Set up a cybersecurity incident reporting mechanism to encourage faculty and students to report security issues in a timely manner and ensure that information security issues can be handled quickly. Institutions can cooperate with network security companies to jointly build their information security infrastructure, and invite network security experts to conduct regular inspections to ensure that their information security infrastructure meets national security standards. In addition, institutions can also establish institutional information security alliances to share information security resources with other institutions and promote cooperation in information security technology. Through multifaceted efforts, institutions can create a secure and stable institutional environment by strengthening their information security infrastructure, and provide a solid foundation for cybersecurity education.

In short, under the overall national security concept, institutional education always needs to adhere to six dimensional measures. First, the combination of party building leadership. Set up a leading group for network security work, take the lead in studying network security, conduct research on the subject, and come up with important results for vigorous promotion. Second, combine with school management. Take network security publicity and education as a key research content, formulate network security publicity measures, form a long-term mechanism, promote network security knowledge into the brain and heart, improve the network security awareness of the institution's people, and create a pattern of the overall national security view of the nurturing environment. Third, combine with teacher development. Organize teachers to learn network security knowledge, carry out teaching and research activities in disciplines integrated with network security education, so that network security propaganda penetrates into daily education and teaching, enhance the awareness of network security among faculty and staff, and comply with the network security code of conduct. Fourth, combining with the growth of students. Carry out thematic team meetings, so that students understand network

security knowledge; use of network security lectures and other activities to further enhance the awareness of network security and preventive capacity of teachers and students. Fifth, combining home and school co-education. Carry out home-school co-education, using school-family learning methods, students and parents watch and learn relevant videos about network security knowledge, forming a good closed loop. Sixth, combining with campus culture. Network security is to "protect national security, social development, family happiness, personal future," the core essence of the school's school culture and connotation of school discipline and school motto, in-depth excavation, the use of publicity, slogans, slogans, handbills, telling stories about network security in a variety of forms, to create a good educational atmosphere.

### 3. Conclusion

Since ancient times, network security is a matter of national security and national survival. As an important training talent base of the country, institutions must attach great importance to the education of network security concept, constantly improve the network security awareness and protection ability of officers and soldiers, build a solid network security defense line, and provide a solid guarantee for the construction and development of the society.

Under the overall concept of national security, we should always adhere to the fundamental principle of the Party's control of network security, closely focus on the overall development of the Party and the national cause, and strengthen the construction of network security regulations and systems in the light of the situation, tasks and realities faced by network security work. The overall national security concept is a guide to action for maintaining and shaping national security with Chinese characteristics under the new situation, and has great theoretical, contemporary and practical significance for network security education in the new era. Network security education under the overall national security concept has become an important part of institutional culture, and technological innovation in multiple fields has made the work of network security education more diversified and promoted the overall quality of education in institutions. In the future, with the deepening of cybersecurity education, institutions can

cultivate talents with a greater sense of responsibility, who can assume key roles in all walks of life and ensure the stability of the national security system.

### References

- [1] Wang Danyang. Research on the Optimization Path of Overall National Security Concept Education for College Students in the New Media Era [J]. *Communication and Copyright*, 2024, (08): 91-93+97.
- [2] FANG Wei, FANG Ke. Reflections on Strengthening National Security Education for College Students under the Perspective of Overall National Security Concept [J]. *School Party Building and Ideological Education*, 2024, (08): 94-96.
- [3] Xiao Yao, Zhong Charter. Analysis of the cyberculture security governance under the perspective of the overall national security concept [J]. *Administration and Law*, 2024, (04): 43-55.
- [4] Liang Ying, Wang Ying. Research on the Effective Path of Network Security Publicity and Education in Colleges and Universities under the Perspective of National Security [J]. *China Light Industry Education*, 2024, 27 (01): 25-33.