Journal of Contemporary Educational Research, 2025, Volume 9, Issue 11
http://ojs.bbwpublisher.com/index.php/JCER
ISSN Online: 2208-8474
ISSN Print: 2208-8466

Exploration and Practice of General Education Courses on Cybersecurity in Higher Education Institutions

Xuejing Zhang, Yueqin Li, Fang Yang, Jingjing Wu*

Smart City College, Beijing Union University, Beijing 100101, China

**Author to whom correspondence should be addressed.*

Abstract: Strengthening cybersecurity education for college students holds significant importance in achieving the strategic goal of building China into a cyber power. This article begins by discussing the significance and necessity of implementing cybersecurity education for university students. Drawing on disciplinary characteristics and student learning analysis, it presents a comprehensive construction process and countermeasures for a general cybersecurity education course, covering aspects such as teaching content development, teaching resource creation, and pedagogical approaches. The aim is to provide reference and guidance for other universities in developing general cybersecurity education courses.

Keywords: Cybersecurity; General education; Security awareness

Online publication: December 10, 2025

1. Introduction

Cyberspace serves as a common domain for human activities, and its secure and orderly development is a global consensus. China places great emphasis on cultivating cybersecurity talent. In 2015, it added “Cyberspace Security” as a first-level discipline, and in 2016, six ministries and commissions jointly issued the *Opinions on Strengthening the Construction of Cybersecurity Disciplines and Talent Cultivation* [1]. In April 2025, the Department of Ideological and Political Work under the Ministry of Education further required the integration of cybersecurity education into daily teaching and promoted the initiative of “Tens of Millions of Teachers and Students Taking the Same National Security Education Class” [2], signifying that cybersecurity has become an important component of the cultivation of all college students.

Although college students possess basic awareness of online security precautions, they lack a systematic knowledge framework. In 2023, our university designated “Cybersecurity” as a general elective course in the natural sciences category. By 2025, it had further incorporated “National Security” into the talent cultivation program as a required general education course. Currently, the “Cybersecurity” elective course has been offered twice, with favorable teaching outcomes. This paper summarizes the necessity, content, resources, and teaching methods of the course construction, providing references for similar courses.

2. The necessity and significance of constructing general education courses on cybersecurity

It is an important pillar for implementing the strategy of building China into a cyber power. Currently, China’s critical information infrastructure frequently faces overseas attacks, prompting multiple departments to regularly organize cybersecurity attack-defense drills to enhance defensive capabilities. As the core base for talent cultivation, universities need to enhance students’ cybersecurity skills and awareness through courses, laying a talent foundation for safeguarding national information security, ensuring the stability of digital infrastructure, and building China into a cyber power [3].

It is an inevitable requirement for higher education to keep pace with the times. The post-2000s generation has become the main body of college students. As “the generation that has grown up alongside the Internet,” their study, scientific research, and daily life are deeply intertwined with the Internet, and potential security risks pose new challenges to higher education. According to the 56th Report of the China Internet Network Information Center [4], China’s internet user base has reached 1.123 billion, with an internet penetration rate of 79.7%. The internet has become the mainstream mode of production and living. While updating their knowledge systems regarding internet technologies, universities must also simultaneously advance the teaching of cybersecurity technologies and the cultivation of awareness to ensure that education keeps pace with the development of the times.

It is a crucial measure to ensure students’ safety and well-being. In recent years, there has been an upward trend in cybersecurity incidents affecting college students, with issues such as internet addiction, cyberbullying, telecom fraud, and data breaches seriously threatening their life, property, and physical and mental health. Against the backdrop of the deep integration of artificial intelligence and the internet, equipping students with cybersecurity knowledge and skills and fostering a correct sense of security have become urgent tasks for universities in nurturing talent.

It is an important opportunity to promote interdisciplinary integration. For comprehensive universities with a high proportion of liberal arts and art majors, offering general education courses in cybersecurity, a field in engineering, can compensate for the lack of scientific literacy among liberal arts students. Simultaneously, it promotes the sharing of resources such as faculty, laboratories, and teaching achievements from science and engineering disciplines across the entire university, breaking down disciplinary barriers. However, currently, cybersecurity education in most universities [5] relies on departments such as the network center and student affairs office, conducted through lectures, class meetings, and competitions. The content is fragmented and lacks a scientific evaluation mechanism, making it difficult to track teaching effectiveness. Therefore, it is imperative to offer systematic general education courses in cybersecurity.

3. Exploration of course construction

The course team focused on the objectives of “precise content and diversified resources,” carrying out practical efforts in both course content and resource development, while also innovating teaching methods to ensure effective teaching outcomes.

3.1. Course content construction

Taking into account the multidisciplinary and comprehensive characteristics of our university, the course content centers on four key directions: "application, innovation, development, and cutting-edge," while integrating a hidden ideological and political thread, forming a system of "four content blocks with one hidden thread" that balances knowledge transmission with value guidance.

Incorporate core content sourced from mainstream applications. Focusing on next-generation cybersecurity technologies as the core, the course concentrates on mainstream application areas such as Web security, cryptography, malicious code, system security, networks and firewalls, and laws and regulations within limited class hours. Instructors can flexibly adjust the content based on students' majors and interests to ensure the practicality of the knowledge.

Offer competition and practice content that serves the cultivation of innovative talents. The field of cybersecurity combines technicality with interest orientation. The course introduces the CTF (Capture The Flag) competition model, registration channels, and post-competition analysis to tap the potential of non-specialized students. It also explains cybersecurity emergency response centers, vulnerability mining, and practical network defense operations, inviting members of the university's attack team to share their experiences on-site. Guided by the philosophy of "interest first, competition-driven practice," the course encourages students to become "white hats" defending cybersecurity and fosters their innovative spirit.

Integrate industry convergence content oriented towards future development. Based on students' majors and career plans, the course presents application cases of cybersecurity in various industries (such as security services and graded protection). This not only boosts students' motivation to learn but also plants the seeds of "cybersecurity protection" awareness, helping them proactively practice safety concepts in their future careers.

Keep up with dynamic content tracking and cutting-edge technologies. In response to the rapid development of the cybersecurity field, the course explains cutting-edge technologies such as AI security and big data security. By combining theoretical instruction with practical operations, students are exposed to the latest industry advancements, ensuring that the course content remains "fresh and updated."

Weave implicit ideological and political education threads throughout the entire course. With "cultivating talent through moral education" as the foundation, ideological and political elements are integrated throughout the teaching process: first, by emphasizing the connection between cybersecurity and national security, guiding students to align their personal actions with the national agenda; second, by incorporating content from laws and regulations such as the Cybersecurity Law to cultivate students' online ethics; and third, by advocating the concept of "collaborative construction, governance, and sharing," encouraging students to participate in campus cybersecurity promotion and enhancing their sense of responsibility.

3.2. Curriculum resource construction

To achieve the integration of knowledge in the humanities and sciences, the course team has expanded resources across multiple dimensions and constructed a diversified resource repository:

We possess interdisciplinary knowledge reserves. Teachers have read over 30 books in history, philosophy, biography (such as *Tao Te Ching*, *Sapiens: A Brief History of Humankind*, and *Steve Jobs*), as well as popular science works (such as *The Beauty of Mathematics*). They have also watched over 50 hours of documentaries (such as *The Fifth Dimension* and *Zero Day*), visited more than 10 museums, and explored connections between binary systems and ancient Yin-Yang and Eight Trigrams, as well as musical notes and rhythms, enhancing the fun of the course content.

We utilize diverse forms of teaching resources. The course employs a blended approach combining MOOC/SPOC models with flipped classrooms, incorporating third-party resources such as CCTV documentaries, outstanding external MOOCs, and public account videos. Additionally, it has recorded school-specific resources, including classic cybersecurity experiments and short case study videos. The 30-minute promotional video titled "The City and Gates of Cybersecurity," produced by the course team, was shortlisted among the top 40 entries in the 2024 National College Teachers' National Security Education Teaching Excellence Showcase and received an Excellence Award.

3.3. Teaching methods and means

Given the significant differences in students' majors and their relatively low level of emphasis on general education courses, the course team has innovated teaching methods to balance both engagement and effectiveness.

Use blended learning to stimulate interest. By combining MOOC/SPOC models with flipped classrooms, the course leverages collected new media resources and school-specific short videos for supplementary instruction. Classroom activities incorporate group discussions, live polling, raffles, and attendance/question-and-answer awards sponsored by security enterprises. These strategies not only boost student motivation but also reinforce cybersecurity awareness.

Employ experiential learning to broaden horizons. Utilizing school-enterprise collaboration resources, the course designs three types of site visits: (1) touring the Institute of Computing Technology, Chinese Academy of Sciences, to understand foundational security technologies; (2) exploring the university's Information Network Center to familiarize students with campus network defense mechanisms; and (3) visiting Qi An Xin Technology Group's Security Center to gain insights into industry trends and corporate culture. These off-campus resources are transformed into a "second classroom."

Implement practical learning to strengthen comprehension. Leveraging a virtual cyber range in the Information Security Laboratory, the course simulates high-risk scenarios such as phishing attacks, data breaches, and ransomware. Experiments are based on real-world incidents, such as the 2022 phishing attack on Northwestern Polytechnical University by the U.S. NSA. Using a "teacher demonstration + student debrief" approach, the course ensures students from diverse majors can complete operations, enabling them to directly experience hacker techniques and stimulating their curiosity.

Case-driven learning connects with daily life. The course selects real-life cases relevant to students, such as telecom fraud on campuses, hotel data breaches, and excessive data collection by e-commerce platforms [6]. By analyzing vulnerability mechanisms from a technical perspective, it not only reminds students to protect their personal information but also inspires them to proactively identify security risks and safeguard national information security in their future careers.

4. Conclusion

The Internet is a vital tool for college students' learning and daily life, and possessing sound cybersecurity literacy is a prerequisite for safely enjoying the conveniences it offers. Helping college students develop a systematic understanding of cybersecurity and fostering a strong sense of security awareness constitutes an important responsibility for universities in talent cultivation. This article summarizes the construction experience of our university's general cybersecurity education course from the perspectives of course necessity, content, resources, and teaching methods, aiming to provide references for other institutions. Only by enhancing the cybersecurity awareness and knowledge levels of all college students can we provide solid support for building China into a cyber power.

Funding

This work was supported in part by the 2024 Core General Education Course Construction Project of Beijing Union University, titled "Cybersecurity: Exploring the World of White Hat Hackers"; the 2025 Educational Science Research Project of Beijing Union University (JK202514); the General Project of Science and Technology Program of Beijing Municipal Education Commission under Grant KM201911417011; and the Academic Research Projects of Beijing Union University (ZK30202407).

Disclosure statement

The authors declare no conflict of interest.

References

[1] Office of the Central Leading Group for Cybersecurity and Informatization, National Development and Reform Commission, Ministry of Education, Ministry of Science and Technology, Ministry of Industry and Information Technology, Ministry of Human Resources and Social Security, 2016, Opinions on Strengthening the Construction of Cybersecurity Disciplines and Talent Cultivation, viewed June 6, 2016, http://www.cac.gov.cn/2016-07/08/c_1119184879.htm

[2] Notification from the Department of Ideological and Political Work, Ministry of Education, 2025, on Organizing Activities for the National Security Education Day in 2025 (Document No. 4 [2025]from the Department of Ideological and Political Work), viewed October 25, 2025, http://www.moe.gov.cn/s78/A12/tongzhi/202504/t20250403_1185987.html

[3] Zhang L, 2024, Research on Cybersecurity Education in Universities during the Mobile Internet Era. Journal of University Logistics, (5): 82–84.

[4] China Internet Network Information Center, 2025, The 56th Statistical Report on Internet Development in China, viewed July 21, 2025, https://www.cnnic.cn/n4/2025/0721/c326-11327.html

[5] Lin J, 2020, Research on General Information Security Education for College Students in the "Internet+" Era. Digital Technology and Application, (38): 209–210 + 212.

[6] Guo S, 2021, Reflections and Curriculum Design on General Education Courses in Cyberspace Security. Network Security Technology and Application, (02): 97–100.