

Practical Integration of Ideological and Political Elements into Information Security Courses

Yabin Yang*, Kai Cheng

School of Computer and Artificial Intelligence, Henan Finance University, Zhengzhou, Henan, China

**Corresponding Author*

Abstract: Information Security is an elective course for students majoring in Data Science and Big Data Technology. It plays a significant role in enhancing students' technical competence in computer information security and fostering their professional ethics, while also serving as an effective vehicle for promoting the educational goal of cultivating virtue and talent and strengthening public awareness of overall national security. By highlighting the necessity of integrating values education into the Information Security curriculum, this paper proposes a feasible teaching approach. Teaching experience has shown that incorporating values education into every stage of Information Security instruction helps improve students' legal awareness and overall quality.

Keywords: Values Education; Information Security; National Security; Network Security; Teaching Practice

1. Introduction

As an important measure for implementing the fundamental task of fostering virtue in higher education in the new era, the fundamental goal of course-based values education is to break down the barriers between professional course teaching and ideological and political teaching, integrate value guidance, knowledge imparting, and ability building, promote the collaborative education of all professional courses and ideological and political theory courses, and thereby comprehensively enhance the quality of talent cultivation in universities[1,2]. Currently, under the background of the implementation of the Digital China strategy and the strong momentum of the development of big data industry, the cyberspace and data space have become new national sovereignty domains after land, sea, sky, and space, and information security and data security have deeply

penetrated into national governance, economic and social development, social operation, and people's lives in all aspects[3-5]. They are strategic supports for ensuring national security and stability, the healthy development of the digital economy, and the protection of citizens' personal information and legitimate rights and interests.

A junior student majoring in Data Science and Big Data Technology has completed the core prerequisite courses such as Computer Network, Operating System, and Database Principles. They possess a solid theoretical foundation in the field, strong logical thinking abilities, and a certain engineering practice background. They can quickly understand and master the course content of Information Security. However, at this stage, students are in an important period of establishing career concepts and values, and there is a phenomenon of emphasizing practical operations while neglecting ideological education[6]. They lack scientific and rigorous guidance and cultivation in terms of the values of cybersecurity, legal and moral red lines, industry norms, and social responsibility. Information security is a core elective course for senior students of this major and is a key course for cultivating professional skills and fostering professional awareness.

At present, there are still many problems in the teaching of information security courses in universities, mainly manifested as overly focusing on technical knowledge while neglecting ideological and moral education[7,8], the integration of values education into the teaching of professional knowledge being too rigid, and to a large extent, separating professional skills education and ideological education[9,10]. This has failed to meet the requirements of professional information security talent cultivation in the context of big data. Therefore, by taking into account the cognitive characteristics of third-year university students and the teaching rules of the courses,

we explore the values education elements inherent in the courses. On the basis of reflecting the professional characteristics of the courses, we establish a suitable ideological and political teaching model for students' learning development that is feasible to implement, achieving the unity of skill cultivation and value guidance, and having strong application value for educational reform.

2. The Necessity of Integrating Ideological and Political Elements into the Information Security Course

Information security is a professional course that combines both theoretical knowledge and practical application. For senior students in their third year of university, this course is not only an important stage for them to enhance their professional skills, but also a crucial period for them to determine their career direction and stabilize their values.

From the perspective of the course content, the information security course covers multiple knowledge modules such as cryptography, network security, system security, data security, application security, security management, and related laws and regulations. The teaching methods include classroom lectures, experimental operations, vulnerability reproduction, offensive and defensive confrontation, case lectures, and project practice. Each part contains rich values education materials. The theoretical teaching enables students to understand the principles of security mechanisms, the process of offensive and defensive confrontation, and the boundaries of technology use, cultivating their scientific and dialectical thinking abilities; the on-machine experiments and offensive training emphasize process norms, bottom-line awareness, and responsibility boundaries; case lectures enhance students' sense of patriotism and legal consciousness by analyzing real security incidents; project practice helps cultivate collaboration spirit, innovation ability, and professional qualities.

From the perspective of the training objectives, third-year university students will face important tasks such as in-depth professional study and internship employment. They should possess a correct view of cybersecurity, security technology, and legal concepts. Information security technology is a double-edged sword; while it protects information systems, there is

also the risk of abuse. Therefore, integrating values education into professional teaching, so that students have a safety red line, legal awareness, patriotic sentiment, and craftsmanship spirit, is necessary and urgent.

Therefore, integrating values education into the teaching of information security courses is necessary and urgent, so as to help students establish a comprehensive national security perspective, deeply understand the close connection between cybersecurity and national security; enhance students' legal awareness and ethical bottom lines, and clarify the boundaries between legal and illegal behaviors; cultivate students' rigorous, pragmatic, and meticulous scientific attitude and craftsmanship spirit; improve students' comprehensive abilities in teamwork, offensive and defensive capabilities, and emergency response; strengthen students' belief in taking the path of independent technological development, and enhance their sense of responsibility and mission for maintaining national cyber security.

3. The Integration Path and Teaching Implementation of Ideological and Political Elements for Third-Year University Students

In order to integrate ideological and political theory courses with professional knowledge, based on the learning characteristics of third-year university students and the content characteristics of the information security course, a four-dimensional integrated teaching system of "value guidance - knowledge imparting - practical reinforcement - quality improvement" has been formed. Comprehensive value infiltration is carried out in aspects such as national security outlook, legal and moral concepts, rationality of science and technology, unity and cooperation, and sense of responsibility.

3.1 Deepen Education on Patriotism and Technological Confidence in Alignment with the Strategy of Building a Strong Cyber Nation

Currently, under the wave of digital transformation, cybersecurity has become an indispensable part of the national security system. It is a fundamental prerequisite for ensuring national security, the normal operation of the economy and society, and the protection of massive information resources from being infringed upon. It is also an important

cornerstone for the healthy and orderly development of the digital economy. Therefore, the information security course should take on the responsibility of cultivating talents for ensuring the security of big data. In the teaching process, it should not be limited to the learning of specific knowledge and technologies, but should be closely integrated with national security strategies. The contents such as China's independent innovation capabilities in the field of cryptography, the security guarantee of key information infrastructure, data security system construction, and sovereignty of cyberspace should be incorporated into the teaching system. This will guide students to go beyond the professional scope and understand the importance and special significance of information security from the perspective of national interests and the overall development of society, and establish an overall national security awareness.

In the basic cryptography teaching unit, the course focuses on explaining the commercial cryptography algorithms SM2, SM3, and SM4 developed independently by China, as well as the complete domestic cryptography system they constitute. By comparing the development paths and differences of cryptography technologies at home and abroad, and combining the typical research process of Chinese cryptography researchers who have persisted in independent innovation and achieved a transition from being controlled by others to being independently controllable, students can personally feel the technological achievements made by China in the field of cybersecurity, enhancing their national confidence and independent innovation spirit. For the network attack and network security practical courses module, during the teaching, the requirements for the security guarantee of important information systems such as energy, transportation, finance, and government affairs should be combined. The clear mission and professional responsibility that security workers should shoulder in the new era under the background of big data should be clarified. A comprehensive understanding and recognition of what "cybersecurity is not a trivial matter, every word and sentence is related to emotions" should be achieved. By combining teaching materials such as the National Cybersecurity Week of China, large-scale cybersecurity attack and defense events at home and abroad, and large-scale user data leakage

incidents, students should recognize the severe situation of cyber space security at present. They should actively combine their learning of professional knowledge and employment development with the requirements of national cybersecurity construction, and cultivate an attitude and responsibility of using technology to serve the country and benefit the people.

3.2 Strengthening the Rule of Law and Ethics, and Establishing a Bottom-Line Awareness for the Use of Technology

The third-year students majoring in Data Science and Big Data Technology are in the transitional period before graduation and employment, about to enter the front-line practical teams in the workplace. The professional conduct and compliance with laws and regulations during their on-the-job period directly determine the professional quality and behavioral norms of graduates in this industry in the future. This is also one of the important prerequisite conditions for ensuring their healthy career development. At the same time, due to the dual nature of information security technology - it can be used to ensure network security and protect data resources, or it can be abused to breed cyber criminal activities - legal education, moral education, and bottom-line education must become the main thread of the values education content for this course, running through the entire process of values education.

In the teaching process, deeply explore real cases in the actual development of big data industry, integrate the relevant legal provisions in the "Cybersecurity Law", "Data Security Law", "Personal Information Protection Law", and "Criminal Law" regarding illegal network attacks, system illegal intrusion, data illegal acquisition and dissemination, and illegal interference and sabotage into it, and use the learned professional knowledge to interpret the legal connotations, guiding students to correctly understand the boundaries of technology application. In addition, let students deeply understand the difference between "legitimate and reasonable white hat research" and "illegal and unlawful internet gray industry", avoiding students from going astray.

In the teaching implementation stage, representative judicial cases are selected to carry out contextualized warning education activities. By analyzing real cases such as the responsibility of major data leakage incidents,

illegal intrusion into civilian and government computer systems, and unauthorized penetration testing, deeply interpret the root causes of the cases, the consequences of the illegal acts, and the damage they cause to the industry, enabling students to personally understand the legal responsibilities faced when technology behavior exceeds the legal allowable range, firmly establishing the fundamental concept that "technology application must strictly follow legal provisions". In addition, the course focuses on the professional ethics norms of network security, emphasizing the strengthening of students' confidentiality awareness, integrity quality, and maintaining an objective and neutral professional stance, guiding students to uphold the professional mission of maintaining network public security and protecting user data rights, and striving to become high-level professionals in the field of big data security with legal knowledge, understanding of legal spirit, compliance with legal provisions, adherence to professional bottom lines, professional conduct, and the courage to take responsibility.

3.3 Emphasize Science and the Spirit of Craftsmanship, and Enhance Rigorous and Pragmatic Professional Capabilities

Since information security is a practical science that emphasizes operational accuracy, process rigor, and detail management, there must be no slightest error in activities such as network attack and defense, encryption and decryption, patch repair, etc. A minor operational mistake or carelessness in handling details can lead to the paralysis of the entire information security protection mechanism, resulting in serious consequences such as information leakage, system paralysis, and network attacks. Students majoring in Data Science and Big Data Technology have already developed good practical skills and problem-solving abilities after two years of study. However, during experiments or completing project tasks, they often show carelessness, lack of standardized procedures, and sloppy experimental records, lacking the meticulous professional attitude. Therefore, this course, focusing on important practical sections such as experimental teaching, vulnerability reproduction, security settings, and system reinforcement, introduces scientific spirit and craftsmanship spirit education in the design, to achieve a balance between skill training and quality cultivation.

Strictly following the student's practical operation rules, in the experimental process, ensure standardized operation, standardized procedures, standardized records, and reproducible conclusions, guarantee the authenticity of experimental data and the rigor of experimental reports, and eliminate sloppy operation, false records, and perfunctory learning attitudes. For example, in operations such as system security reinforcement, firewall strategies, data encryption, etc., repeatedly emphasize the working concept of "small details reveal danger, standards determine success/failure", so that students can adhere to the rules and respect the skills; in vulnerability discovery and analysis, security verification testing, and attack-defense simulation exercises, focus on cultivating students' spirit of tracing the root cause of problems, rigorous thinking logic, and rigorous and realistic attitudes, overcoming impetuous and perfunctory learning tendencies.

At the same time, through multiple steps such as having students solve the same problem with different solutions, build different levels of prevention systems, and conduct attack-defense effect comparisons in the course, to broaden students' horizons, inspire them to think about new security mechanisms and prevention methods, and continuously cultivate students' "serious, patient, focused, responsible" working attitude, correct bad habits in practical operations, guide students to develop standardized and standardized professional thinking habits, and lay a solid professional skills foundation and good professional qualities for further taking on positions such as security operation engineers, penetration engineers, security architects, and security compliance assessment engineers.

3.4 Strengthen Teamwork and Project Implementation, and Enhance the Overall Educational Effectiveness

Compared with the teaching methods in lower grades that focus on memory and individual basic experiments, third-year university students have a more complete and systematic knowledge framework. They have strong independent thinking and self-exploration abilities, making them suitable for higher-level teaching methods such as project-driven, task-led, and team collaboration. Moreover, this method also aligns with the working characteristics of the big data industry and the cybersecurity industry. At the

same time, it can effectively solve the problem of fragmented and unsystematic knowledge in traditional classroom teaching. Therefore, the information security course, in accordance with the requirements of the talent cultivation plan and based on the application background of big data security, sets a series of comprehensive, innovative, and practical tasks. It breaks away from the single-point knowledge teaching model and promotes students' understanding of professional knowledge in the process of team cooperation. Students can master certain practical skills through hands-on practice and improve their comprehensive quality in the process of communication and coordination.

This course starts from practical work and arranges multiple practical tasks such as enterprise internal network security reinforcement plan design and planning, Web penetration and defense implementation, data security classification protection design scheme for big data platforms, and cybersecurity emergency drills. Each task is completed by students in groups. The project is decomposed into several task units, and each group completes the work processes such as requirement research, design planning, platform construction, hands-on practice, security assessment, effect verification, summary report, and demonstration explanation, which restore the actual network information security project construction process in the enterprise.

During the project implementation, students need to actively communicate and coordinate with each other, jointly tackle technical problems, reasonably allocate workloads, and learn communication and coordination, division of labor and collaboration, and taking responsibility in helping each other. Thus, they can truly exercise their communication and coordination abilities and teamwork skills. In addition, the comprehensive and complex projects also pose certain challenges to students' comprehensive application of technologies, problem-solving abilities, and stress resistance, which is conducive to cultivating students' execution ability and adaptability. Through systematic team project training, it can effectively change the scattered and isolated state of students' knowledge learning, promote the synchronous improvement of their knowledge system, technical ability, and comprehensive quality, and achieve an important leap from mastering scattered

professional knowledge to possessing comprehensive and compound practical cybersecurity capabilities.

3.5 Integrate with the Sense of Mission and Responsibility, Cultivate the New Era's Cybersecurity Guardians

The third year of university is an important period for students to clarify their career paths, set career visions, and form career values. It is also a crucial transitional stage from professional knowledge learning to practical work application and from adapting to the campus environment to adapting to the development of society. Oriented towards the career planning of third-year students majoring in Data Science and Big Data Technology, the current and future trends of the industry, the national security network development plan, as well as their own career development are integrated into the teaching process. This aims to guide students to focus on employment, establish a career vision that is correct, long-term, and serves the national strategic development, overcome one-sided understandings such as excessive utilitarianism and overemphasizing skills while neglecting ideology, and help students establish correct professional thoughts and career ideals.

Firstly, in the classroom, the deeds of outstanding experts and scientists in China's cybersecurity are constantly introduced, showcasing the important achievements and technological breakthroughs in areas such as cryptographic algorithms research, information confidentiality management, and information security defense, as well as the independent intellectual property rights. The contributions of cybersecurity professionals in various competitions, government services, and national basic infrastructure construction activities in China are also introduced. Through vivid and specific industry education examples, students can personally feel the significance and social responsibility of the cybersecurity field, enhance their professional sense of belonging, industry honor, and enterprising spirit, and inspire students to consciously integrate their personal career aspirations and development plans into the historical journey of building a digital power and achieving national rejuvenation.

Secondly, clarify the role positioning and responsibilities of cybersecurity personnel in the new era, and let students understand that

cybersecurity personnel are not just technicians; at the national level, they are defenders of China's Internet space sovereignty security; at the social level, they are guardians of digital social governance order; at the individual level, they are defenders of personal information rights and legitimate interests. At the same time, continuously strengthen the positive role of career guidance, guide students to abide by professional ethics, adhere to technical bottom lines, resist the black and gray industries on the internet and the abuse of technology. Advocate that students adhere to the concept of technology for good, be courageous in taking on industry missions and social responsibilities, and strive to grow into high-quality new era cybersecurity talents with all-round development and moral, intellectual, physical, aesthetic, and labor skills.

4. Conclusion

Integrating the content of ideological and political theory courses into information security-related courses and conducting integrated teaching that combines value guidance and professional knowledge transmission for students in the third year of university has achieved good results. Students' national consciousness has been strengthened, their legal awareness and security awareness have become more solid, their experimental attitude has become more rigorous, and their practical collaboration and engineering implementation abilities have significantly improved. At the same time, students have strengthened their professional ethics concepts and sense of responsibility in terms of ideological understanding.

Practice has proved that course values education is not a mechanical superimposition of ideological and political content and professional courses, but an effective internal unity. Only by naturally integrating ideological and political elements into the course objectives, teaching content, classroom explanations, experimental operations, assessment and evaluation, etc. in accordance with the characteristics of the courses, the current situation of students, and the principles of education, can the effective implementation of the educational goals be truly achieved.

In the future, we will continue to strengthen values education in information security courses, make efforts in enriching case resource libraries, increasing practical teaching links, and

improving the assessment and evaluation system, and closely combine professional knowledge teaching and values education to improve teaching quality and educational effectiveness. We will strive to cultivate more new-era professional talents with firm ideals and beliefs, good ideological styles, excellent professional skills, and excellent professional ethics to serve the country.

References

- [1] Wang J, Li Z. Exploration of the Integration Path of Course Ideological and Political Education in Professional Course Teaching Process - Taking the Engineering Surveying Course as an Example. *Higher Education Journal*, 2024, 10(17):176-179.
- [2] Gan S D, Liu G Q, Wei J J et al. Research on the Ideological and Political Education in the Intelligent Management Accounting Course. *Accounting and Finance Communication*, 2024, (8):150-157.
- [3] Peng C X. Digital Technology and Legal Transformation. *Journal of East China University of Political Science and Law*, 2024, 27(4):5.
- [4] Ren H Y, Sun Z, Liao S et al. A Review on the Application of Large Language Models in Network Threat Analysis Computer Application, 1-26 [2026-05-31]. <https://link.cnki.net/urlid/51.1307.TP.20260517.1711.002>.
- [5] Bao X L, Xu X F, Liu T et al. Teaching Innovation Practice of Information Security Course in the Context of New Engineering Education// National Association for Computer Education Research. 33rd National Conference on New Technologies and Education in Computer Science. Proceedings. [Publisher unknown], 2025:83-87.DOI:10.26914/c.cnkihy.2025.119060.
- [6] Zhang L, Xia B, Xing Y et al. Research on the Practical Pathway of Professional Ideological and Political Education in Cybersecurity within the Threshold of Value Guidance// China Computer Federation, National Association for Computer Education Research. 2025 China University Computer Graduate Education Conference (CCGEC2025) Proceedings. [Publisher Unknown], 2025:25-29.
- [7] Yang J Q, Zhang Q L, Zheng Y et al. "Innovative Teaching of Internet of Things

- Information Security Course from the Perspective of 'Technology - Ethics - Ideological and Political Education'. Computer Education, 2026, (2):232-235.DOI:10.16512/j.cnki.jsjyy.2026.02.031.
- [8]Wang G. Exploration of Improving Students' Practical Skills and Innovative Teaching Models in the Context of Network Information Security Professional Education//Jiangxi Art and Culture Development Promotion Association, Nanchang Institute of Technology. The Proceedings of the First Symposium on Artificial Intelligence Empowering New Liberal Arts Construction and Innovation Development (Volume 2) [Publisher Unknown], 2026:223-226.
- [9]Pan S H, Li J X. Exploration and Practice of the Paradigm for Ideological and Political Education in Higher Vocational IT Professional Groups: A Case Study of Computer Network Technology Professional Group. Modern Vocational Education, 2023, (6):61-64.
- [10]Yang J G, Lu W, Wang S Z. Practice Exploration of Undergraduate Course Ideological and Political Education Teaching Paradigm in the Digital Era - Taking Civil Engineering Major as an Example// China Construction Education Association, Fujian University of Technology. Proceedings of the Symposium on First-Class Courses in Civil Engineering and Ideological and Political Education in Courses. [Publisher Unknown], 2024:124-127.