Evaluation and Enhancement Strategies for University Students' Cybersecurity Literacy and Competency in the Context of Platform Society: Postprint

Authors: Chen Qi, Xiong Huixiang, Dai Qinquan, Gu Jiayun

Date: 2023-04-01T00:00:00+00:00

Abstract

[Purpose/Significance] This study constructs an evaluation index system for college students' network information security literacy capabilities and conducts empirical analysis by integrating domestic and international literature research with the characterization of college students' network information security literacy within the platform society perspective, thereby providing a reference for the scientific assessment of network information security literacy. [Method/Process] Based on preliminary research, an evaluation index system for college students' network information security literacy oriented toward the new environment was initially constructed, and online questionnaire surveys were implemented. Utilizing exploratory factor analysis methods, eight first-level indicators were extracted from the data samples, including "Network Information Security Knowledge"and "Basic Skills for Platform Security Usage."Concurrently, the coefficient of variation method was employed to assign weight coefficients to indicators at all levels, followed by empirical analysis. [Results/Conclusions] Empirical results demonstrate that college students perform relatively well on indicators related to basic awareness of network information security, while considerable room for improvement exists in deep-level multi-dimensional cognition, specific knowledge, and practical skills. Furthermore, the study reveals that indicator scores did not exhibit significant differences among college students across different grades, majors, and university types. Based on these findings, countermeasures and suggestions for enhancing college students' network information security literacy from the platform society perspective are proposed, focusing on three relevant stakeholders: "state-university-individual student."

Full Text

Research on the Evaluation and Promotion Strategy of College Students' Network Information Security Literacy Ability from the Perspective of Platform Society

Chen Qi[1],[2], **Xiong Huixiang**[1], **Dai Qinquan**[1], **Gu Jiayun**[1] [1]School of Information Management, Central China Normal University, Wuhan 430079 [2]China Library Innovation and Development Research Center, Central China Normal University, Wuhan 430079

Abstract

[**Purpose/Significance**] This study constructs an evaluation index system for college students' network information security literacy ability through literature review both domestically and internationally, combined with the characterization of college students' network information security literacy under the platform society perspective, and conducts empirical analysis to provide references for scientific measurement of network information security literacy. [**Method/Process**] Based on preliminary research, this paper initially constructed an evaluation index system for college students' network information security literacy oriented toward the new environment and conducted an online questionnaire survey. Using exploratory factor analysis, eight first-level indicators such as "network information security knowledge" and "basic skills for platform security use" were extracted from the data samples. Meanwhile, the coefficient of variation method was employed to assign weight coefficients to indicators at all levels for empirical analysis. [**Result/Conclusion**] Empirical results indicate that college students perform relatively well in indicators involving basic awareness of network information security, while there remains considerable room for improvement in deep-level multi-cognition, specific knowledge, and practical skills. Additionally, the study finds no significant differences in indicator scores among students of different grades, majors, or university types. Based on these findings, this paper proposes countermeasures and suggestions for improving college students' network information security literacy from the perspective of platform society, focusing on three related subjects: "state-university-individual student."

Keywords: platform society; network information security literacy; exploratory factor analysis; evaluation index system

1. Introduction

The upgrading and iteration of computer and information technology have spawned a large number of platform-based applications, while the optimization of network environments, particularly the development of ubiquitous networks, has enabled these applications to penetrate deeply into various aspects of people' s lives. According to relevant statistics, in the January 2022 China App

Store iPhone popular app download rankings, the monthly download volume of the top 10 applications all exceeded 3,300,000, with WeChat ranking first with a staggering 10,515,227 monthly downloads [**?**]. These applications cover application scenarios closely related to public life, including instant messaging, finance, mobile shopping, information, and social networking, and are playing an increasingly significant role. Some scholars have noted that if software was previously embedded in objects, now objects revolve around platforms [**?**]. As public life continues to migrate toward digital and commercial platforms, society as a whole may have entered what Dutch scholar J. Van Dijck calls "The Platform Society" [**?**].

Platform society represents a more precise distillation and summary of the social environment under the current new technological background, with personal information (data) serving as an important production element [**?**]. The types of network information in platform society include not only traditional internet-based text, images, audio, and video information, but also personal privacy information stored on various internet platforms (such as account credentials, fingerprints, facial information) and personal dynamic behavioral trace information (such as likes, comments, location data, and permission information). While platform society brings convenience to public life, it also generates numerous problems, such as excessive collection of personal information and unnecessary device permissions by some platforms, increased risks of individual user identification through multi-source data integration and mining, and illegal use of personal privacy information by others. Facing the public value and public interest hazards concerning citizen privacy and information security involved in internet commercial platforms requires not only effective government regulation and self-discipline of market entities, but also citizens themselves constitute an important dimension [**?**].

2. Literature Review

2.1 Platform Society Research The concept of "platform society" was proposed by Dutch scholar J. Van Dijck et al. in *The Platform Society: Public Values in a Connective World*, with the core argument that platforms have become an infrastructure in people' s production and life practices and have deeply penetrated social institutions and their operations [**?**]. Around this work, a number of insightful and inspiring book reviews have emerged [**?**]. Existing foreign research can be roughly divided into two categories: First, research discussing the motivations for the rise and development of platform society itself and the data governance issues it triggers, such as how platforms become social focus [**?**], interdisciplinary research agendas for platform governance [**?**], and four data governance models emerging in platform society: DSPs (Data Sharing Pools), DCs (Data Cooperatives), PDTs (Public Data Trusts), and PDS (Personal Data Sovereignty) [**?**]. Second, research analyzing the impact, reshaping, or implications of platform society on other research objects, including social media [**?**] and work/employment [**?**].

Domestic research on platform society is mostly concentrated in journalism and communication disciplines, with themes roughly divided into two aspects: First, theoretical research on the origin of platform society and talent cultivation and technological reflection under this background. For instance, Ren Tianhao et al. explored three questions including "how network media evolution contributed to the rise of digital platforms" [**?**], while Hu Yong also analyzed the reasons for platform rise [**?**]. Facing the popularity of short videos in platform society, Liu Xinchuan et al. analyzed development concerns and approaches for innovation [**?**]. Zhang Zhian et al. discussed the cultivation of public communication talents oriented toward society and public culture in the context of platform society [**?**]. Second, empirical research on specific issues from the platform society perspective. For example, Ji Deqiang et al. proposed conceptual innovation suggestions for stakeholders in public opinion in the platform era based on interview data [**?**]. Jia Ruixue conducted participatory observation on 80 frequently used apps by domestic users to examine the current situation of personal data openness in platform society [**?**].

2.2 Network Information Literacy, Network Information Security, and Network Information Security Literacy Since the concept of information literacy was formally proposed by P. G. Zurkowski in 1974 [**?**], it has continuously attracted attention from scholars worldwide. With internet development, especially the emergence of Web 2.0, new requirements have been imposed on traditional information literacy capabilities in terms of information sensitivity, knowledge, skills, and ethics [**?**]. Therefore, analyzing and researching network information literacy within the internet environment represents an important direction for adapting to contemporary developments.

Meanwhile, internet development has also brought information security and network security hazards. Zhang Jing et al. argue that the boundaries between information security and network security definitions are increasingly blurred, and the term "network information security" is increasingly used in academia, which to some extent equates to information security [**?**]. Experts and scholars have not yet reached a unified view on the connotation of network information security (or information security). ISO defines information security as "the technical and managerial security protection established and adopted for data processing systems to protect computer hardware, software, and data from destruction, alteration, and disclosure due to accidental and malicious reasons" [**?**]. Yin Jianguo believes network information security includes two aspects: First, cyberspace security, mainly referring to the security maintenance of network infrastructure, focusing on preventing technical attacks such as viruses and network cracking; second, network information content security, mainly concerning network fraud, pornography, terrorism, and other information content security issues [**?**]. He Yue et al. argue that network information security includes not only physical equipment security, information system operation security, and information resource security, but also the security consequences of network information dissemination [**?**]. These definitions show that experts

generally agree network information security includes hardware, software, and information content security. With rapid network development, many relatively mature network information security standards have emerged domestically and internationally to more normatively ensure network information security, such as ISO/IEC 15408 (CC) [?], ISO 27000 series [?], and UK' s BS7799 standard [?] internationally, and China' s authoritative standards like *Information Technology—Security Techniques—Guidelines for Information Security Management Systems Audit* (GB/T 28450-2020) [?] and the national standard for personal information protection *Information Security Technology—Personal Information Security Specification* (GB/T 35273-2020) [?].

In the platform society environment, information production, release, and transmission become increasingly convenient, while information security hazards such as information leakage and fraud become more concealed and complex, posing new challenges to both network information literacy and network information security. This study argues that platform society, network information literacy, and network information security should form a ternary relationship of "environment-means-vision," where platform society represents the latest summary of the entire network and real social environment, network information security is the eternal goal pursued by human society, and network information literacy adapted to the platform society perspective serves as a necessary means to promote network information security. Against this background, network information security literacy, as one of the core capabilities of network information literacy, has gradually become an independent research object for analysis and exploration by experts and scholars.

2.3 Network Information Security Literacy Evaluation Research

Given that existing research on "information security literacy evaluation" is mostly conducted within the internet context, this study also incorporates such research for reference. Through literature review and organization, existing research can be roughly divided into three categories: First, design and empirical research on information security literacy evaluation index systems for multiple subjects, such as J. R. A. Ndiego et al. who developed a questionnaire scale including general security awareness and physical security to survey information security awareness levels among undergraduates at a higher education institution in Kenya [?], and other scholars focusing on tax personnel [?], ethnic minority college students in Xinjiang [?], Shanghai citizens [?], and military academy students [?]. Second, education and talent cultivation-oriented analysis of information security literacy education, such as Sun Liutao' s analysis of deficiencies in current college student network information security literacy cultivation from the perspective of campus network culture [?], and Luo Li' s review of network information security talent cultivation strategies and practices in Europe and America to propose reference suggestions for China [?]. Third, practical application-oriented design of information security literacy evaluation systems and software, such as the design and implementation of personal information security literacy evaluation

APPs [?] and online information security literacy evaluation systems [?].

In summary, although experts and scholars have conducted many innovative and practically significant studies on network information security literacy under diverse subjects and objectives, this study argues that as human society gradually enters platform society, citizens' , especially college students' , network information security literacy should be given new characteristic interpretation and scientific measurement. However, few scholars have currently focused on constructing an evaluation index system for college students' network information security literacy from the platform society perspective.

3. Construction of College Students' Network Information Security Literacy Evaluation Index System from the Platform Society Perspective

3.1 Characterization of College Students' Network Information Security Literacy from the Platform Society Perspective The fundamental difference between platform society and previous information society or network society forms lies in the continuous platform-based migration of people' s various practical activities [?]. Platformization obviously brings great convenience, including improved infrastructure and network environments that enhance practical efficiency, while also better satisfying public demands. However, internet platform companies are ultimately profit-oriented commercial organizations that bear extremely strong public attributes [?], making states, societies, citizens, and other practice subjects inevitably dependent on resources and services provided by platforms. When massive amounts of data and information are collected, mined, analyzed, and reused by platform enterprises, the network information security issues of various subjects, especially college students as important forces for future social development, must be considered.

The trend of platform society is irreversible. Under this new perspective, college students' network information security literacy should have new connotations and extensions, specifically manifested in four aspects: First, in network information security awareness, college students should fully recognize that the transformation of life practices brought by platform society often comes at the cost of ceding personal information privacy and should continuously enhance their information security prevention awareness. Second, in network information security knowledge, they should understand relevant theoretical knowledge about information security, device security, and usage behavior security under the premise of having certain cognition of the new environment. Third, in network information security skills, as the platformization trend becomes increasingly evident and college students encounter more platforms in daily life, they need to master diversified security skills within single platforms and across multiple platforms to address various information security threats and hidden dangers. Fourth, in network information security law and ethics, internet platform companies facilitate efficient interaction among users. In platforms with almost zero entry thresholds and relative freedom, college students should ac-

tively pay attention to and understand relevant information security laws and continuously improve their ethical awareness.

3.2 Initial Evaluation Indicator Design Referencing and drawing upon first-level indicators with high usage frequency in existing research results [**?**, **?**], this study adopts "network information security awareness," "network information security knowledge," "network information security skills," and "network information security law and ethics" as the first-level indicators of the evaluation model. Combined with the characteristics of platform society and following the principle of concise yet key indicator-focused evaluation index system design, this study sets a total of 32 second-level indicators under the four first-level indicators (see Table 1).

3.2.1 Network Information Security Awareness

This indicator refers to college students' psychological manifestations such as judgment, cognition, and attitude toward network information security phenomena and events, which can influence their behavior in participating in network information activities. Specifically, it includes cognition of the importance of information security and the role individuals play therein, sensitivity to information security privacy when exchanging information on network platforms, and reflection on the ownership of personal information privacy under platform society. Based on the above analysis, this study designed 12 second-level indicators X1-X12 under "network information security awareness."

3.2.2 Network Information Security Knowledge

This indicator refers to college students' mastery of theoretical knowledge related to network information security, including basic knowledge of information leakage hazards, information security protection tools, and security prevention skills. Under the platform society perspective, network information security knowledge includes not only understanding and mastery of theoretical foundations such as information leakage hazards and information security protection skills, but also knowledge of emerging terms such as "information fog," "information cocoon," "information cage," "data divide," "right to data deletion," "right to be forgotten," and "big data price discrimination." Based on the above analysis, this study designed six second-level indicators X13-X18 under "network information security knowledge."

3.2.3 Network Information Security Skills

This indicator emphasizes the ability to flexibly apply information security awareness and knowledge to daily practice. Under the platform society perspective, network information security skills emphasize capabilities demonstrated in information security protection before, during, and after platform use, such as paying attention to user service agreements and privacy terms, password setting, permission settings, spam information filtering, and utilization of security tools. Meanwhile, college students in platform society are characterized by their

learning and life practices being platformized to varying degrees, with their information distributed across various platforms. Therefore, network information security skills under this perspective should also include diversified information security risk assessment and avoidance capabilities, as well as reflection abilities for different platforms. Consequently, this study designed eight second-level indicators X19-X26 under "network information security skills."

3.2.4 Network Information Security Law and Ethics

This indicator emphasizes that college students can understand and comply with relevant external constraints at the legal level and internal constraints at the moral level in information security activities. To obtain platform convenience, users usually have to cede part of their information and data privacy to platforms. Once this information (and data) is out of users' control, what algorithms platforms use to process it and what conclusions are drawn remain a "black box" to users. Once users' rights and interests are infringed upon, they should know how to respond using legal means. This study argues this is also an important aspect of network information security literacy. In addition to legal aspects, users' specific behaviors in interacting with platforms and other users should also follow certain ethical norms. Based on the above analysis, this study designed six second-level indicators X27-X32 under "network information security law and ethics."

4. Empirical Analysis

4.1 Questionnaire Distribution and Data Collection To obtain real data for weight assignment to indicators at all levels and understand the current status of Chinese college students' network information security literacy, this study conducted empirical research using the online questionnaire method based on the evaluation index system constructed in Table 1. The empirical questionnaire consisted of two parts: The first part collected basic information about respondents, including gender, grade, discipline category, and university type; the second part used a five-point Likert scale to understand respondents'self-assessment scores based on 32 indicators, with options of "strongly disagree,""disagree,""neutral," "agree," and "strongly agree" assigned scores of 1-5. The questionnaire survey was launched on February 4, 2021, lasting for more than ten days, with 271 questionnaires distributed. After eliminating invalid questionnaires, 211 valid data points were obtained. Among the valid data, males accounted for 45.5% and females for 54.5%. There were 112 undergraduates and 99 graduate students. The sample covered first-class university construction universities, first-class discipline construction universities, and other domestic universities, including 12 discipline categories such as economics, education, science, engineering, and management (excluding military science), with 100 from natural sciences and 111 from humanities and social sciences. Partial sample data is shown in Table 2 .

4.2 Descriptive Analysis and Reliability Analysis Using SPSS 22.0 software for descriptive analysis of the data samples in Table 2, the results are shown in Table 3 . The analysis shows that the average values of the four component scales divided by first-level dimensions are all above 3.3, while the average value of the total evaluation scale is above 3.8, indicating that the respondent group has generally possessed certain network information security literacy.

Data dispersion can be evaluated through standard deviation. Generally, the smaller the standard deviation, the smaller the deviation between data values and the mean. In Table 3, the standard deviation of the data samples ranges between (0.43, 0.74), indicating not much dispersion between items and relatively stable survey results.

Reliability reflects the reliability of data samples. Using SPSS 22.0 software to calculate the Cronbach' s α coefficient of the total evaluation scale, the result is 0.899. Generally, when Cronbach' s α coefficient is greater than 0.7, it indicates high questionnaire reliability. Therefore, the scale constructed in this study has high reliability.

Similarly, using SPSS 22.0 to measure the correlation between component scales and between component scales and the total evaluation scale, the results are shown in Table 4 . The correlation among the four first-level indicator sample data ranges between [0.339, 0.567], while the correlation between component scales and the total evaluation scale ranges between [0.737, 0.795], indicating strong independence among component scales and high correlation with the overall evaluation index system. Therefore, the evaluation index system constructed in this study has good internal consistency.

4.3 Extraction of First-Level Indicators Based on Exploratory Factor Analysis To reduce the subjectivity of artificially dividing first-level indicators and let the "data" speak, this study used SPSS 22.0 to conduct exploratory factor analysis on data samples. Before exploratory factor analysis, it is necessary to calculate the validity of data samples. Using SPSS 22.0 to calculate the KMO and Bartlett values of this data sample, the results are shown in Table 5 . The results show that the KMO value of the total scale is 0.852, and the significance level of Bartlett' s test of sphericity is $0.000 < 0.05$, indicating that this scale is suitable for exploratory factor analysis.

Importing the raw data from Table 2 into SPSS 22.0 software and calling the "factor analysis" tool, all items X1-X32 were imported for exploratory factor analysis. The criterion of eigenvalues greater than 1 was applied, and the "maximum variance method" was chosen to rotate the original loading matrix. After calling the above commands, the software sequentially output "total variance explained" (see Table 6) and "rotated component matrix" (see Table 7), which will be explained in turn.

First, in Table 6, "total variance explained"refers to the degree to which extracted common factors contain information from original variables, with "initial eigen-

values" showing preliminary factor extraction results. "Total" represents each factor' s eigenvalue, where larger eigenvalues indicate greater importance of the factor in explaining original variable variation. "Extraction sums of squared loadings" and "rotation sums of squared loadings" represent eigenvalues, explained variance, and cumulative explained variance before and after rotation, respectively. Rotation can make the classification of common factors clearer, and their eigenvalues will change accordingly, but the total sum of eigenvalues remains unchanged. From the "rotation sums of squared loadings" results, exploratory factor analysis extracted eight factors with eigenvalues greater than 1, which together explain 62.588% of the information in the original 32 indicators (generally considered acceptable when variance explanation rate reaches 55%). Therefore, the newly extracted eight common factors can replace the original four first-level indicators.

Second, the meaning of the eight extracted common factors must be analyzed through the "rotated component matrix." Table 7 shows that X13-X18 belong to common factor 1, X19-X23 belong to common factor 2, X30-X32 belong to common factor 3, X4-X6 and X11-X12 jointly belong to common factor 4, X7 and X24-X26 jointly belong to common factor 5, X1-X3 belong to common factor 6, X27-X28 belong to common factor 7, and X8-X10 belong to common factor 8. Among them, the six second-level indicators X13-X18 all come from "network information security knowledge" among the original four first-level indicators, so common factor 1 can be directly named "network information security knowledge." The five second-level indicators X19-X23 mainly focus on college students' basic operational skills regarding service terms, account security, permission settings, and information filtering when using a platform (or APP), so common factor 2 is named "basic skills for platform security use." X30-X32 mainly involve personal behavioral orientation in information activities on network platforms, so common factor 3 is named "network information security behavior norms." Following the same procedure and analyzing the connotation of second-level indicators, the remaining five newly extracted first-level indicators are sequentially named "network information security individual sensitivity," "diversified guarantee skills for platform security use," "network information security global value perception," "network information security law and ethics," and "individual perception of network information security from the platform perspective."

4.4 Indicator Weight Assignment The evaluation index system for college students' network information security literacy constructed in this study is a two-layer comprehensive evaluation model, where different indicators measure college students'literacy ability from different angles, and thus each indicator has different relative importance to the entire evaluation model. Assigning weights to indicators at all levels, compared with not assigning weights, considers the differences in each indicator' s influence on the evaluation object, making survey results more realistic. Drawing upon Guan Dandan' s research results on weight establishment methods [**?**], this study used the coefficient of variation method to assign weights to first-level and second-level indicators. The core idea of

the coefficient of variation method is that in comprehensive evaluation, if an indicator' s values can significantly distinguish evaluated objects, that indicator should be assigned greater weight, and vice versa.

Based on the data samples in Table 2, this study sequentially calculated the standard deviation and mean of the eight first-level indicators and 32 second-level indicators, then calculated the ratio of standard deviation to mean to obtain the coefficient of variation for each indicator. As shown in Table 8 , for each first-level indicator, its standardized weight equals the ratio of that indicator' s coefficient of variation to the sum of all first-level indicators' coefficients of variation. For example, the sum of F1-F8 coefficients of variation is approximately 1.3613, so F1' s standardized weight is 0.1596 (0.2173/1.3613). Similarly, the remaining seven first-level indicators' standardized weights can be calculated. For each second-level indicator, its standardized weight equals the ratio of its coefficient of variation to the sum of coefficients of variation for all second-level indicators under the same first-level indicator, while its combined weight equals the product of this standardized weight and its belonging first-level indicator' s standardized weight. For example, the sum of six second-level indicators' coefficients of variation under F1 is 1.7495, so indicator X14' s standardized weight is 0.1335 (0.2336/1.7495), and X14' s combined weight is 0.0213 (0.1335×0.1596). Similarly, the combined weights of the remaining 31 second-level indicators can be calculated, with the final sum of all 32 second-level indicators' combined weights equaling 1.

4.5 Empirical Scoring Results After calculating the combined weights of each second-level indicator, these weights were multiplied by college students'self-assessment scores in Table 2. The products under the same first-level indicator were summed to obtain each first-level indicator's final score. The sum of all first-level indicators'final scores constitutes an individual respondent's comprehensive score. Partial calculation results are shown in Table 9 .

4.6 Analysis of Empirical Results

4.6.1 Analysis of Full Sample Empirical Scoring Results To more intuitively display empirical scoring results, visualization images were drawn based on the data in Table 9. The full sample empirical scoring results are shown in Figure 1 [Figure 1: see original paper]. Drawing upon existing research where experts and scholars typically use below 60, 60-79, and 80 and above as important score level divisions [**?**], this study categorizes ratios of sample mean to individual full score not less than 0.8 as "good," ratios between 0.6-0.79 as "fair," and ratios below 0.6 as "poor."

Overall, the ratio of sample mean to individual full score for each first-level indicator is above $0.65 > 0.6$, and the ratio of college students' comprehensive actual score to total full score is 0.76, indicating that college students have a certain foundation of network information security literacy, which aligns with

the preliminary analysis results in Section 4.2. Specifically, college students' ratios of sample mean to individual full score in the three dimensions of "network information security behavior norms," "network information security individual sensitivity," and "network information security global value perception" are all not less than $0.85 > 0.8$. The ratios in the five dimensions of "network information security knowledge," "basic skills for platform security use," "diversified guarantee skills for platform security use," "network information security law and ethics," and "individual perception of network information security from the platform perspective" are all below 0.8, with relatively large differences between scores. This indicates that although college students generally possess certain network information security literacy foundations, their local capability scores are uneven, manifesting as relatively good performance in awareness and personal cognition indicators, but overall fair performance in knowledge and skill indicators, with significant room for improvement.

In today' s increasingly complex network environment with exponential growth of multi-source heterogeneous information in platforms, network information security hazards continue to increase. The real environment requires college students to possess not only certain network information security risk awareness and prevention consciousness but also continuously strengthen their mastery of relevant knowledge and skills.

4.6.2 Analysis of Empirical Scoring Results Based on Multiple Dimensions To understand the network information security literacy levels of college students with different attributes, the data in Table 9 were grouped by grade, major, and university type, and the average scores of each group on the eight first-level indicators were calculated and visualized, with results shown in Figure 2 [Figure 2: see original paper].

From the comparison between individual indicators and full scores, regardless of grouping dimension, empirical scoring results show that F3, F4, and F6 are relatively close to full scores, while other indicators have relatively larger gaps from full scores. That is, students of different grades, majors, and universities all demonstrate relatively good performance in network information security literacy awareness and basic cognition, but there is significant room for improvement in deep understanding of platform society, network information security knowledge, and skill levels, which aligns with conclusions from full sample empirical scoring results. From the perspective of multiple-dimensional grouping, no significant differences in scores across the eight first-level dimensions are evident between different grades, majors, or university levels.

In summary, this empirical study yields two findings: First, college students generally possess certain network information security literacy, but their internal structure shows capability imbalances, manifesting as relatively good performance in basic awareness but needing improvement in deep multi-cognition, specific knowledge, and skill levels. This imbalance is confirmed in both full sample and grouped sample results based on grade, major, and university di-

mensions. Second, differences in grade, major, and university type do not lead to significant differences in scores across first-level dimensions. This indicates that while information literacy is gradually gaining public attention and widespread discussion, network information security literacy as an important component has not received differentiated attention and cultivation from relevant subjects within different grades, majors, and universities.

5. Promotion Strategies for College Students' Network Information Security Literacy from the Platform Society Perspective

While large internet platforms bring great convenience to citizens' lives, they also pose many information security hazards. Emphasizing citizens' , especially college students' , self-assessment of network information security literacy and continuous cultivation and improvement does not mean resisting platform society development, but rather better protecting citizens' personal interests while keeping pace with the times, thereby promoting society toward a safer and healthier direction. Based on empirical results, this study proposes several countermeasures and suggestions for improving college students' network information security literacy from the platform society perspective at three levels: state, university, and individual student.

5.1 National-Level Strategy of Standardized Literacy Assessment and Personalized Education Support As one of the main behavioral subjects in platform society, the government should, based on deeply grasping the "newness" of the era, comprehensively consider national informatization construction and digital-driven strategic needs for talent, and design and improve a set of scientifically unified and collaboratively connected network information security literacy evaluation systems for students at different stages. This standard should incorporate grasp of the current era, reflection on real society, and dynamic response to future social changes, thereby promoting unified literacy assessment standards while enhancing societal awareness and importance attached to network information security literacy to advance the goal of "promoting construction through evaluation." The state can also support stage-based and collaborative improvement of college students' network information security literacy through favorable policy guidance and environment building. On the other hand, the state can provide personalized, targeted talent cultivation support for different types of universities at the financial level, while also recognizing that college students' network information security literacy capabilities can only be tested and valued through returning to specific practices of the era. Therefore, the state can fully integrate advantageous resources to build bridges for cooperation between universities and other social parties, create beneficial exchange opportunities to connect talent supply and demand ends, and better promote universities to cultivate and output high-literacy talent.

5.2 University-Level Establishment of a "Trinity" Progressive Network Information Security Literacy Education System Network information

security literacy education under the new perspective should have corresponding new development systems. Universities should build a "trinity"progressive, stage-based network information security literacy education system comprising talent cultivation construction, teacher team construction, and information security education environment construction. Specifically, in talent cultivation construction, universities should combine the new era background of platform society to design targeted, hierarchical talent cultivation programs and curriculum teaching systems for different grades and majors. For example, when freshmen first enter school, thematic seminars on network information security education and preliminary literacy assessment can be conducted, while continuous attention and follow-up can be given to senior students' network information security literacy. Additionally, universal quality development collective teaching and small-group thematic discussions can be carried out separately for universal problems exposed by college students and individual students' personalized confusions. In teacher team construction, universities can select a group of teachers to conduct training and scientific assessment on network information security knowledge and skills. Teachers who pass the assessment can serve as instructors for on-campus network information security literacy education. Instructors can come from high-quality campus faculty with relevant disciplinary backgrounds or excellent alumni employed at internet platform companies who can return for exchange and guidance. In information security education environment construction, universities can not only create a good cultivation atmosphere for network information security literacy on campus but also regularly conduct inter-university exchanges and cooperation, such as organizing knowledge competitions, thematic salons, and academic seminars within regional scope to integrate advantageous resources of different university types and jointly contribute to students' network information security literacy improvement.

5.3 Individual Student-Level Network Information Security Literacy Improvement Strategy Following the "Attention-Learning-Experience-Improvement" Pattern College students should enhance their attention to network information security literacy, understand their capability strengths and weaknesses through scientific assessment, and continuously experience, internalize, and comprehend the challenges and new requirements that platform society environments pose to individual literacy capabilities through ongoing learning and practice, thereby ultimately improving network information security literacy as an important component of comprehensive core literacy capabilities. Specifically, on one hand, college students should maintain their current level of network information security awareness and perception, continuously deepen their reflection on personal network information ownership and security under platform society through daily interactions with platforms, and further enhance their understanding of reasonable and legal information behavior norms, multi-value perception, etc., integrating these throughout the entire process of network information security literacy optimization. On the other hand, college students should strengthen their learning of network

information security knowledge and understanding and mastery of diversified security guarantee skills, internalizing them as components of their capabilities through continuous experience and practice. Meanwhile, the increasing complexity of platform society under the information era also requires college students to incorporate the improvement and perfection of their network information security literacy into their personal comprehensive development plans, thereby achieving personal value realization oriented toward social development on the basis of perfecting their literacy capabilities.

References

[1] Diandian Data. January 2022 China App Store iPhone popular app download rankings [EB/OL]. [2022-02-23]. https://app.diandian.com/rank/hotapp-0-4-0-1. [2] KENNEY M, ZYSMAN J. The rise of the platform economy [J]. Issues in science and technology, 2016, 32(3): 61-69. [3] VAN DIJCK J, POELL T, DE WAAL M. The platform society: public values in a connective world [M]. New York: Oxford University Press, 2018. [4] JIA Ruixue. Research on the open relationship of personal data in platform society —based on participatory observation of 80 domestic application platforms (Apps) [J]. Information Studies: Theory & Application, 2021, 44(5): 66-77, 121. [5] LIU Xinchuan, CUI Xiaoxing. Technical reflection and ecological reconstruction of short video communication in platform society [J]. News Front, 2019(11): 44-46. [6] China Internet Network Information Center. The 47th Statistical Report on China' s Internet Development (full text) [EB/OL]. [2021-04-08]. http://www.cac.gov.cn/2021-02/03/c_{1613923423079314}.htm. [7] MCGOWAN A. The platform society: public values in a connected world [J]. Cultural sociology, 2021, 15(1): 160-161. [8] ANDOK M. The platform society. public values in a connective world [J]. Kome-an international journal of pure communication inquiry, 2020, 8(1): 97-105. [9] MICCONI A. The platform society: public values in a connective world [J]. International journal of communication, 2020, 14: 781-789. [10] BALABAN D. The platform society. public values in a connective world [J]. Romanian journal of communication and public relations, 2019, 21(1): 71-74. [11] PLANTIN J C. The platform society: public values in a connective world [J]. Media culture & society, 2019, 41(2): 252-257. [12] GELDERBLOM C. The platform society: public values in a connective world [J]. Partecipazione e conflitto, 2019, 12(3): 980-992. [13] BARNS S. Negotiating the platform pivot: from participatory digital ecosystems to infrastructures of everyday life [J]. Geography compass, 2019, 13(9): 1-13. [14] GORWA R. What is platform governance? [J]. Information, communication & society, 2019, 22(6): 854-871. [15] MICHELI M, PONTI M, CRAGLIA M, et al. Emerging models of data governance in the age of datafication [J]. Big data & society, 2020, 7(2): 2053951720948087. [16] SZULC L. Profiles, identities, data: making abundant and anchored selves in platform society [J]. Communication theory, 2019, 29(3): 257-276. [17] PULIGNANO V. Work and employment under the GIG economy [J]. Partecipazione e conflitto, 2019, 12(3): 629-639. [18] REN Tianhao, CAO Xiaojie. From technology to

architecture: how network media evolution drives social platformization [J]. Journal of Xi' an Jiaotong University (Social Sciences), 2020, 40(5): 144-152. [19] HU Yong. Why have we entered a world controlled by platforms? [J]. Internet Economics, 2019(5): 78-83. [20] ZHANG Zhian, RAN Zhen. Cultivation of public communication talents under platform society context [J]. Youth Journalist, 2020(19): 19-20. [21] JI Deqiang, YING Zhihui. Rethinking "public opinion" : public opinion in the platform era [J]. Modern Communication (Journal of Communication University of China), 2020, 42(2): 49-54. [22] ZURKOWSKI P G. The information service environment relationships and priorities [R/OL]. [2021-04-08]. https://files.eric.ed.gov/fulltext/ED100391.pdf. [23] WU Xiaowei, NA Ri, LI Dan. Research on the design of college students' network information literacy capability scale [J]. Information Studies: Theory & Application, 2009, 32(12): 84-88. [24] ZHANG Jing. Network information security technology [M]. Beijing: Beijing Institute of Technology Press, 2020. [25] PENG Shaoping, NING Rui. Thoughts on China' s network information security [J]. Library Work and Study, 2007(4): 84-86. [26] YIN Jianguo. US network information security governance mechanism and its implications for China [J]. Law and Social Development, 2013, 30(2): 138-146. [27] HE Yue, ZHENG Wenjuan. Research on China's network information security legislation [J]. Science Technology and Law, 2011, 89(1): 70-74. [28] DING Keyun, SONG Gesheng. Interpretation of the revision of "Guidelines for Digital Library Security Management" [J]. Library and Information Service, 2016, 60(S2): 1-3, 8. [29] GU Sui-shan, LIU Shanshan. Research on information security management system construction and countermeasures [J]. Information Science, 2019, 37(8): 108-113, 151. [30] LIU Guocheng. BS7799 standard and its application in meso-level information system auditing [J]. Auditing and Economic Research, 2012, 27(3): 50-56. [31] National Standard Full Text Public System. Information technology—Security techniques—Guidelines for information security management systems audit (GB/T 28450-2020) [EB/OL]. [2021-12-10]. http://openstd.samr.gov.cn/bzgk/gb/newGbInfo?hcno=6307D4C35D688CF4DAD21B6C819D7874. [32] National Standard Full Text Public System. Information security technology—Personal information security specification (GB/T 35273-2020) [EB/OL]. [2021-12-10]. http://openstd.samr.gov.cn/bzgk/gb/newGbInfo?hcno=4568F276E0F8346EB0FBA097AA0CE0 [33] SUN Liutao. Three-dimensional cultivation path of college students' network information security literacy from campus network culture perspective [J]. China Adult Education, 2015(1): 51-53. [34] CAI Wenzheng. Research on dimensions, current status, and improvement strategies of college students' network information security literacy—taking Nanjing University of Posts and Telecommunications as an example [J]. China Collective Economy, 2020(16): 163-166. [35] MA Rui, LIN Hongzhen, JIANG Yunjun, et al. Strategies for improving college students' information security literacy [J]. Science and Technology Entrepreneurship Monthly, 2019, 32(9): 146-149. [36] NDIEGE J R A, OKELLO G O. Information security awareness amongst students joining higher academic institutions in developing countries: evidence from Kenya [J]. African journal of information systems (AJIS), 2018, 10(3): 204-221. [37] ZHANG Chaoying. Research on information security literacy of tax personnel in District

D, City H, Shandong Province [D]. Beijing: China University of Geosciences (Beijing), 2020. [38] HAN Chunyan, WANG Sheng. Network information security literacy of ethnic minority college students in Xinjiang—against the background of the Belt and Road Initiative [J]. Journal of Xinjiang Radio and TV University, 2017, 21(3): 63-66. [39] LUO Li. Research on Shanghai citizens' personal information security literacy evaluation [J]. Journal of Chongqing University (Social Science Edition), 2013, 19(3): 95-99. [40] GAO Donghuai, CAI Hua, DONG Lipeng, et al. Design of student network information security literacy evaluation scale [J]. China Medical Education Technology, 2013, 27(2): 173-177. [41] CAI Hua, GAO Donghuai, DONG Lipeng. Research on cadets' information security literacy evaluation based on AHP [J]. Information Technology, 2013, 37(1): 188-192. [42] LUO Li. Progress in network information security talent cultivation in Europe and America and its implications for China [J]. Computer Knowledge and Technology, 2016, 12(6): 114-116. [43] CHEN Bo, ZHU Han, LIU Yashang. Development of personal information security literacy evaluation mobile software [J]. Information Security and Technology, 2014, 5(10): 50-55. [44] SHEN Xiajuan, GAO Donghuai, GUO Jia, et al. Design and implementation of information security literacy online evaluation system [J]. Computer Technology and Development, 2016, 26(4): 90-95. [45] GONG Cheng, LI Chenggang. Analysis of college students' network information security literacy—from the perspective of object, elements, and subject responsibility [J]. Education Exploration, 2013(6): 134-135. [46] LUO Li. Research on the construction of national information security literacy evaluation index system [J]. Journal of Chongqing University (Social Science Edition), 2012, 18(3): 81-86. [47] WANG Yiqun, ZHANG Li. Framework for discovering and correcting human errors in network information security [J]. Library and Information Service, 2009, 53(16): 40-42, 56. [48] GUAN Dandan. Research on usability evaluation of archival websites based on user experience [D]. Changchun: Jilin University, 2019. [49] LI Zhihe, LIU Zhixiu, NIE Jianwen. Construction of evaluation index system for online teaching academic ability of university teachers [J]. Journal of Distance Education, 2020, 38(5): 81-89. [50] ZOU Jun, CHEN Han, HUANG Wenrong, et al. Research on quantitative evaluation of traditional village vitality [J]. Scientia Geographica Sinica, 2020, 40(6): 908-917.

Author Contributions

Chen Qi: Data processing, paper writing and revision; **Xiong Huixiang**: Research content guidance; **Dai Qinquan**: Data collection and paper revision; **Gu Jiayun**: Paper revision.

Academic Integrity Statement for Authors Submitting to *Library and Information Service*

Library and Information Service has always upheld the mission of publishing

excellent academic paper achievements and promoting industry academic exchanges, and is committed to purifying the academic publishing environment and creating a good academic ecology. In 2013, the journal took the lead in formulating, releasing, and implementing the "Joint Statement of Library Science Journals on Abiding by Academic Ethics and Purifying the Academic Environment" (hereinafter referred to as the "Statement") (see: http://www.lis.ac.cn/CN/column/item202.shtml), and subsequently took the lead in formulating and releasing the "Joint Action Plan of Chinese Library and Information Science Journals to Resist Academic Misconduct" (hereinafter referred to as the "Joint Action Plan") (see: http://www.lis.ac.cn/CN/column/item247.shtml). To implement and realize this philosophy, this journal hereby solemnly declares that from now on, all submitting authors must commit that papers submitted to this journal must comply with the above "Statement" and "Joint Action Plan," consciously adhere to academic ethics, and resolutely resist academic misconduct. *Library and Information Service* adopts a zero-tolerance policy toward all papers suspected of plagiarism, piracy, and other forms of academic misconduct, and implements corresponding punitive measures.

Library and Information Service Magazine Press

Note: Figure translations are in progress. See original paper for figures.