Cybersecurity Awareness and Digital Hygiene among Pre-service Primary School Teachers: A Case Study of Kazakhstan

Aruna Amzeyeva[1], Aziya Zhumabayeva[2], Askarbek Kussainov[2], Aziza Zhunusbekova[2,*], Aiym Tynyskhanova[2], and Karashash Zhanadilova[3]

[1]Department of Pedagogy, Psychology, and Primary Education Methodology, Korkyt Ata Kyzylorda University, Kyzylorda, Kazakhstan
[2]Department of Primary Education, Abai Kazakh National Pedagogical University, Almaty, Kazakhstan
[3]Department of Social and Age Pedagogy, Sh.Ualikhanov Kokshetau University, Kokshetau, Kazakhstan
Email: aruna_amzeeva@mail.ru (A.A.); aziya_e@mail.ru (A.Z.); kusainov_apnk@mail.ru (A.K.); a.zhunusbekova@abaiuniversity.edu.kz (A.Z.); aiym.tynyskhan@gmail.com (A.T.); janadilova_karashash@mail.ru (K.Z.)
*Corresponding author
Manuscript received July 1, 2025; revised July 21, 2025; accepted August 29, 2025; published January 16, 2026

***Abstract*—Given the rapid growth of digital technologies and the rise in digital threats, preparing future elementary school teachers in cybersecurity and digital hygiene is essential. This study aims to evaluate the awareness, digital competence, and motivation of future teachers regarding digital security, while identifying gaps in their training amid the ongoing digitalization of education. A quantitative descriptive design was employed to assess 120 third-year students from Korkyt Ata Kyzylorda University in Kazakhstan. The questionnaire included sections on digital hygiene, cybersecurity knowledge, motivation, and self-assessed digital competence. Participants scored an average of 2.7 out of 5 in overall cybersecurity awareness, indicating moderate knowledge. Key weaknesses were found in understanding the risks of sharing personal data online (*M*=2.5) and teaching digital safety to children (*M*=2.6). While 60% regularly used antivirus software and 76.7% stored passwords securely, only 41.7% always updated software, and 37.5% had not received any digital safety training. In contrast, motivational readiness was high (*M*=4.5 for willingness to learn). While the study is descriptive in nature, it provides an important initial diagnostic of digital security competence. Future research is recommended to apply more advanced statistical analysis to explore causative and correlative relationships. These findings highlight the need to incorporate structured cybersecurity education into teacher training programs, focusing on practical knowledge and closing knowledge gaps. This study is among the first in Kazakhstan to systematically diagnose the digital security competencies of future elementary school teachers and proposes a structured assessment methodology to support curriculum development.**

***Keywords*—cybersecurity, digital hygiene, future teachers, primary education, digital literacy**

I. Introduction

In the context of the rapid development of digital technologies and the mass digitization of all spheres of public life, the issue of ensuring cybersecurity is becoming increasingly important [1, 2]. However, despite growing digital risks, future elementary school teachers often enter the profession without sufficient training in digital hygiene and cybersecurity. This gap in teacher education raises concerns about their ability to protect themselves and their students in the digital environment. Accordingly, there is a pressing need to assess their current level of digital security competence and identify areas for improvement to inform curriculum development.

The educational environment is no exception: the use of digital resources, educational platforms, and online communication is becoming an integral part of the educational process, starting from the primary level [3, 4]. The digital threats faced by both students and teachers are increasing. A particularly vulnerable category is children of primary school age, who do not have a sufficient level of critical thinking and digital awareness [5–7]. The implementation of this study is directly related to ensuring a safe digital childhood, developing digital citizenship in the younger generation, and reducing the risks associated with digital threats in the school environment [8]. Training teachers who can both teach and protect their students online is essential to establishing a sustainable, technologically literate, and secure learning environment [9]. That is why a primary school teacher should act not only as a bearer of educational content but also as a guarantor of a safe digital space for students [10]. However, effective performance of this role is possible only if the teacher possesses the necessary knowledge, competencies, and attitudes in the field of digital security. In this regard, special attention should be paid to the formation of a culture of cybersecurity and digital hygiene skills among participants in the educational process [11].

In contemporary academic discourse, issues related to the development of a cybersecurity culture among university students are actively studied and discussed [12–14]. A meta-analysis revealed models and conditions aimed at developing a culture of cybersecurity among university students, which are primarily technological and focus on teaching methods and technologies for protecting information [15–18]. Despite extensive research on this issue, there is a clear gap in studies addressing the specifics of developing a cybersecurity culture among pre-service teachers, particularly in primary education [19–21]. It is assumed that the training and competencies of pre-service primary school teachers should provide them with a sufficient level of protection against possible information risks. Although the importance of cybersecurity in education is widely recognized, empirical research specifically focusing on pre-service teachers in Kazakhstan remains limited and underdeveloped. This study addresses that gap by systematically assessing knowledge, motivation, and competence in digital safety [22–24].

According to research, enhancing teachers' digital literacy

and cybersecurity skills should occur during professional training [25, 26]. Nevertheless, in the context of Kazakhstan, this field remains underexplored and insufficiently addressed in current educational standards [27, 28]. The subjects of information security and digital hygiene are not adequately included in the core curriculum for preparing future teachers within the current educational standards and curricula of pedagogical universities, particularly in the area of primary education. As a result, graduates of pedagogical universities lack the necessary skills to manage issues related to maintaining digital security in learning environments. Thus, it is evident that a comprehensive study of the level of cybersecurity awareness among prospective teachers is required [29–32].

The significance of this research lies in (i) the development and theoretical substantiation of a set of diagnostic tools aimed at assessing the current level of readiness of pre-service Primary School Teachers (PSPTs) to ensure cybersecurity in the educational process as an integral component of the professional competence of future specialists in the field of high technologies; (ii) expanding the scope of scientific knowledge in the field of developing a culture of cybersecurity among future teachers, with an emphasis on fostering critical thinking and a conscious attitude toward cybersecurity as one of the key aspects of modern life; and (iii) providing an opportunity to optimize the educational process in pedagogical universities by developing the necessary competencies in the field of cybersecurity among students, thereby adapting teacher training to the current challenges of the digital age.

This study has scientific novelty. Firstly, it is the first in Kazakhstan to focus on the systematic diagnosis of cybersecurity competence among future primary school teachers. It provides a structured assessment methodology and identifies specific deficiencies. Secondly, the study employs a standardized questionnaire adapted to the cultural and educational context of the country, ensuring the relevance and validity of the data obtained. Thirdly, the emphasis on this issue makes the work significant for providing both methodological and empirical foundations for the modernization of pedagogical programs in Kazakhstan [33–35]. Thus, the presented study aligns with the priority areas of educational development in Kazakhstan and can serve as a methodological basis for implementing state policy in the field of digitalization and cybersecurity in education.

A. Research Questions

What are the levels of knowledge, digital competence, and motivational readiness among future primary school teachers in the areas of digital security and digital hygiene, and how do these components interact in shaping their overall preparedness to create and maintain a safe digital environment in primary education?

B. Research Objectives

The purpose of this research is to determine the levels of awareness, digital competence, and motivational readiness of future primary school teachers in the areas of digital security and digital hygiene, as well as to identify existing gaps and opportunities for improving their professional training within the context of educational digitalization.

II. Literature Review

A. Cybersecurity in Education

The challenges of the era of intensive digitalization and the need to train competitive specialists with practical skills to protect against current cyber threats based on the latest technologies are among the most pressing issues in modern society. The professional training of students and the development of information competencies play an essential role and have significant potential in fostering a culture of safe behavior in cyberspace [36]. However, research findings consistently reveal a low level of cybersecurity culture among students and emphasize the need for its development during professional training [37, 38].

Cyberspace is exposed to cyber threats wherever information and communication technologies are utilized [39]. A considerable body of research addresses its technological, legal, economic, social, and humanitarian dimensions [40]. Many scholars examine cybersecurity in educational institutions within the broader framework of digital literacy among students engaged in the learning process [41]. Other studies analyze the risks associated with educating and raising the younger generation in the digital era, particularly in the context of distance learning, including challenges that emerged during the COVID-19 pandemic [42, 43]. Contemporary research also focuses on identifying effective forms, methods, tools, and technologies to address the problem of ensuring cybersecurity for students across different age groups [44].

B. Digital Hygiene

The concept of digital hygiene has multiple interpretations [45]. In general, digital hygiene is understood as a set of rules that, when followed, enable individuals to use information technologies safely and minimize the risks associated with their application for specific tasks [46]. There is considerable debate regarding which rules of safe behavior are central to an individual's digital hygiene and which risks can be mitigated through adherence to these practices [47]. Interpretations of digital hygiene naturally connect to the classical theories of the information society developed in the early 2000s by scholars such as Webster, Eriksen, and Castells [48]. However, in many studies, the scope of digital hygiene remains limited, focusing primarily on individual protection against cybercrime rather than encompassing broader aspects of safe and responsible digital use.

Furthermore, it is reasonable that research conceptualizing digital hygiene as a set of rules for reducing risks has gained significant attention and demand in many countries worldwide [49]. However, the heuristic potential of this field is somewhat constrained by its narrow definition, which primarily frames digital hygiene as a collection of specific guidelines aimed at protecting against criminal activity, while neglecting other important aspects of the safe and responsible use of information technology.

C. Digital Competence (DC) and Cyber Awareness (CA)

Although these terms are often used interchangeably in the literature, this study clearly distinguishes Digital Competence (DC), Cyber Awareness (CA), and Digital Hygiene (DH) as conceptually distinct categories, as summarized in Table 1.

Table 1. The distinction between DC, CA, and DH

Term	Focus	Definition
DC	Pedagogical/ Professional use	Ability to effectively use digital tools and technologies in teaching contexts
CA	Knowledge and vigilance	Understanding digital threats and recognizing risky online behavior
DH	Behavioral habits	Daily practices that support digital safety and minimize risks

D. Research Gap and Contribution

Despite the growing interest in cybersecurity in education, the actual levels of awareness, digital competence, and motivational readiness among future primary school teachers in Kazakhstan remain underexplored. This gap highlights the urgent need for empirical evidence to inform curriculum development and policy planning. The present study makes a novel contribution by introducing the first structured, Kazakhstan-specific diagnostic tool designed to assess digital safety capacities among pre-service primary school teachers [50].

III. Materials and Methods

This study was conducted within the framework of a quantitative approach using a descriptive (diagnostic) design [51]. The primary objective of this design is to obtain objective, quantitatively measurable data on the current state of digital literacy and security among students. The descriptive design enables the systematic identification of the prevalence and structure of knowledge, skills, and attitudes, which is essential for the diagnostic stage and for informing the subsequent development of practical recommendations.

A. Collection of Research Samples

The study involved 120 third-year students from the Faculty of Education, specializing in Primary Education at Korkyt Ata Kyzylorda University, Kazakhstan. This participant group was selected because it represents the target population of future elementary school teachers, whose digital competence and cybersecurity awareness are critical for ensuring safe and effective teaching in increasingly digitalized learning environments. Korkyt Ata Kyzylorda University was chosen due to its representative profile within Kazakhstan's teacher education system and its active engagement in digital education initiatives. A purposive sampling technique was employed to include participants directly relevant to the study objectives—namely, pre-service teachers nearing the completion of their academic training. While this approach enhances contextual relevance, it also limits the generalizability of the findings, which is acknowledged in the study's limitations. At a significance level of $\alpha = 0.05$ and an expected medium effect size (Cohen's $d \approx 0.5$), the sample size ensures a statistical power of approximately 0.80, consistent with accepted standards for detecting significant effects. The gender distribution comprised 75% female and 25% male participants, reflecting the national trend in teacher training programs. This demographic profile—predominantly female and under 23 years of age—is typical of pre-service teaching cohorts in Kazakhstan and provides important context for interpreting the results.

The characteristics of the participants are presented in Table 2. The data indicate that the sample is predominantly female (75%) with a mean age of approximately 21 years. Most students reported frequent use of the internet for educational purposes (85%), while their self-assessed knowledge of information security was rated at a moderate level (mean=2.7 out of 5).

Table 2. Participant characteristics

Characteristic	Frequency (n)	Percentage (%)	M	SD
Gender				
Female	90	75.0%		
Male	30	25.0%		
Age (years)	—	—	20.9	1.3
Course year (fixed for all participants: 3rd year)	—	—	3	—
Experience using digital educational resources	—	—	3.8	0.9
Frequency of internet use for educational purposes				
often or very often	102	85.0%		
Self-assessed level of information security knowledge	—	—	2.7	1.1

Fig. 1 illustrates the gender and age distribution of the participants in the study.

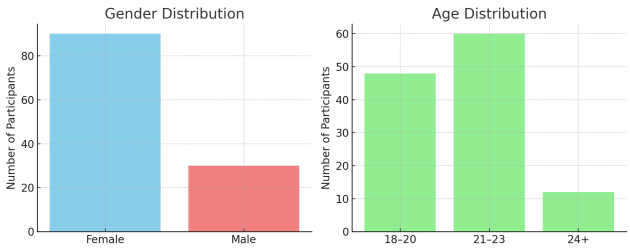

Fig. 1. Distribution of participants by gender and age group.

The participant distribution indicates that the vast majority of respondents were female, with males comprising only 25% of the sample. The age distribution shows that most participants were between 21 and 23 years old, followed by those aged 18 to 20. The smallest proportion of respondents belonged to the age group of 24 years and older.

B. Study Procedure

The study was conducted from January to April 2024 at Korkyt Ata University in Kyzylorda, Kazakhstan. Prior to data collection, official permission was obtained from the faculty leadership. All 120 third-year students enrolled in the primary education program were informed about the objectives of the study, the voluntary nature of participation, the anonymity of data processing, and their right to withdraw at any time without providing an explanation. Informed consent was obtained from all participants.

The survey was administered in person during scheduled classes, with the agreement of course instructors, to avoid disruption of the educational process. Before completing the questionnaire, the researcher provided a brief introduction explaining the purpose of the study, the structure of the questionnaire, and the procedure for completion, and addressed any questions from the participants. The average completion time was approximately 20 min.

The questionnaires did not include personal identifying information, ensuring confidentiality. Collected data were immediately entered into an electronic database. For quality

control, all questionnaires were checked for completeness and accuracy. Questionnaires with missing responses or obvious errors were excluded from the analysis; as a result, five questionnaires were removed, which did not significantly affect the sample size. This procedure ensured the collection of reliable and representative data on the current level of awareness and digital hygiene among future teachers, which is critical for the development of educational programs.

C. Internal Reliability Control and Ethical Aspects

To increase the reliability of the results, the questionnaire was pre-tested on a pilot sample of 15 students to evaluate the clarity, relevance, and consistency of the items. Based on the feedback, several questions were rephrased to enhance comprehension and reduce ambiguity. This process contributed to face validity, ensuring that the items appeared appropriate and understandable to respondents.

To ensure content validity, the questionnaire items were developed based on a comprehensive review of the scientific literature and existing validated instruments related to digital competence, cybersecurity awareness, and digital hygiene in education. Two subject-matter experts in educational technology and cybersecurity reviewed the items to confirm their alignment with the research constructs.

The questionnaire was administered by a single researcher, who provided uniform instructions and ensured consistent conditions for all participants. This approach minimized systematic error and enhanced procedural validity. Data were checked for completeness and consistency; questionnaires with missing responses or logically contradictory answers were excluded from the analysis.

The study adhered to ethical standards for research involving human subjects. Participants were informed about the objectives, procedures, anonymity of responses, and their right to voluntary participation. They could refuse or withdraw from the study at any time without consequences. All data were stored on secure, password-protected servers and used exclusively for academic purposes, with access restricted to the research team. The study involved no interventions that could cause harm to participants and received approval from the University Ethics Committee.

D. Instruments

The research instrument was a structured questionnaire consisting of five sections: demographics, cybersecurity awareness, digital hygiene, digital competence, and motivational readiness. It was developed by the authors based on a synthesis of validated international tools and frameworks in digital literacy and cybersecurity, including UNESCO and European Commission guidelines [52], and subsequently adapted to the Kazakhstani educational context.

The questionnaire included 21 items, distributed as follows:

Section A: Demographics (3 items)—captured gender, age, and year of study.

Section B: Cybersecurity Awareness (5 items)—assessed students' understanding of secure password practices, phishing detection, software updates, data privacy, and safe use of social networks. Responses were measured on a 5-point Likert scale (1=strongly disagree, 5=strongly agree).

Section C: Digital Hygiene (4 items)—evaluated behaviors such as software updates, antivirus use, password storage practices, and prior digital safety training. These were multiple-choice items with predefined categorical options.

Section D: Digital Competence (5 items)—assessed confidence in using digital tools in educational settings, safe communication, data protection, and ability to teach digital safety. Responses were measured on a 5-point Likert scale.

Section E: Motivational Readiness (4 items)—measured willingness and perceived responsibility to engage in cybersecurity education, including one reverse-coded item (E4). Responses were measured on a 5-point Likert scale.

The questionnaire was piloted with 15 students to ensure clarity and cultural relevance. Content validity was reinforced through expert review by two specialists in education and cybersecurity. Minor adjustments were made to item wording for improved comprehension. The final version of the instrument is provided in Appendix A (see Table A1).

E. Reliability of the Instrument

The validity of the questionnaire was ensured through expert review by two specialists in education and cybersecurity, who evaluated the content for relevance, clarity, and cultural appropriateness. Additionally, a pilot study with 15 students was conducted to assess face validity and identify any ambiguities in the items. Based on the feedback and pilot data, minor revisions were implemented to improve clarity and comprehension.

Regarding reliability, internal consistency was evaluated using Cronbach's alpha coefficients. The cybersecurity awareness scale achieved an alpha of 0.78, while the digital competence scale reached 0.83, both indicating acceptable levels of reliability. These findings confirm that the instrument provides consistent and dependable measures of the constructs under investigation. This process enhances the credibility of the data collected and strengthens the study's methodological rigor.

F. Data Analysis

In addition to descriptive statistics (means, standard deviations, frequencies, and percentages) and independent-samples t-tests used to examine group differences by gender, the data analysis included reliability testing through Cronbach's alpha and the application of reverse coding where necessary. To enhance the analytical depth, future research is recommended to incorporate more advanced statistical techniques, such as factor analysis to validate the questionnaire's construct validity, as well as multivariate methods (e.g., regression analysis, structural equation modeling) to explore interrelationships between variables more comprehensively. This study provides a foundational quantitative overview, while recognizing the potential for deeper inferential analysis in subsequent research. Table 3 summarizes the data analysis methods employed at different stages of the study.

Table 3. Data analysis methods at different research stages

Stage	Analysis method
Cybersecurity awareness	Mean, standard deviation
Digital hygiene practices	Frequency, percentage
Self-assessment of competence	Descriptive statistics
Motivational readiness	Mean, standard deviation; reverse-coding applied to E4
Group differences (gender)	Independent-samples t-test (p <0.05)

IV. Result

A. Cybersecurity Awareness

Table 4 presents the descriptive statistics summarizing participants' awareness of key aspects of cybersecurity.

Table 4. Cybersecurity awareness: Descriptive statistics on key items

Item	M	SD
Knowledge of safe password practices	3.1	1.0
Ability to recognize phishing emails	2.8	1.2
Awareness of importance of software updates	3.3	0.9
Understanding risks of sharing personal data online	2.5	1.1
Knowledge of secure use of social networks	2.6	1.2
Overall self-assessed cybersecurity knowledge	2.7	1.1

Mean scores ranging from 2.5 to 3.3 indicate low to moderate levels of knowledge. The item concerning the importance of software updates recorded the highest mean score, whereas items such as knowledge of the safe use of social networks and understanding the risks associated with sharing personal data online showed the lowest mean scores. The relatively high standard deviations suggest considerable variability among participants, indicating the presence of subgroups with differing levels of cybersecurity understanding—from minimal awareness to more informed users.

The overall self-assessment of cybersecurity knowledge, based on a single item, demonstrates a general trend of moderate to low awareness. This finding underscores a critical gap in fundamental cybersecurity knowledge among future teachers, consistent with previous research emphasizing the necessity of targeted educational interventions [53]. Addressing this gap is essential for fostering safer digital environments in schools.

Fig. 2 illustrates the variability in participants' ability to identify phishing attempts and navigate social media safely, highlighting inconsistencies in their existing training. This visualization provides additional insights by displaying variability, median values, and potential outliers in participants' responses, thereby complementing the tabular data.

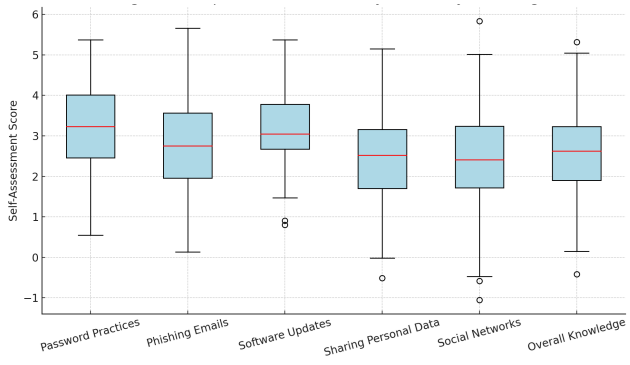

Fig. 2. Boxplot illustrating variability in self-assessed cybersecurity knowledge among participants.

Self-assessment results indicate the greatest variability in participants' confidence regarding safe social network usage and phishing recognition. Overall, cybersecurity literacy remains at a moderate level, reinforcing the need for targeted and more intensive training in these critical areas.

B. Digital Hygiene

Table 5 provides a summary of participants' daily digital hygiene practices, including behaviors related to software updates, antivirus utilization, password management, and previous experience with digital security training.

Table 5. Digital hygiene practices among participants

Practice	Category	Frequency (n)	Percentage (%)
Software update frequency	Always	50	41.7%
	Sometimes	58	48.3%
	Never	12	10.0%
Use of antivirus software	Yes, regularly	72	60.0%
	Sometimes	38	31.7%
	No	10	8.3%
Password storage method	Stored openly	28	23.3%
	Stored securely	92	76.7%
Received digital safety training	Yes, through university courses	45	37.5%
	Yes, through self-education	30	25.0%
	No	45	37.5%

Analysis of participants' digital hygiene behaviors reveals several critical patterns. While the majority of respondents reported regularly updating software and utilizing antivirus programs, approximately 10% indicated never updating their systems, and nearly one-quarter admitted to storing passwords insecurely. The relatively high prevalence of antivirus use suggests a baseline awareness of protective measures. However, password management practices remain inconsistent. Although many participants rely on secure methods such as memorization or password managers, 23.3% store passwords in plain text (e.g., in notepads or mobile phone notes), and a practice that significantly increases vulnerability to data breaches.

These findings highlight an urgent need to integrate structured digital hygiene education into teacher preparation programs to mitigate risks associated with insecure behaviors. Additionally, while some participants reported prior exposure to cybersecurity training through university courses or self-directed learning, nearly half lacked any formal or informal instruction in digital security, underscoring a substantial digital literacy gap that must be addressed within pedagogical curricula.

C. Digital Competence

Table 6 presents self-assessments of confidence in digital tools and security skills relevant to teaching.

Table 6. Self-assessment of digital competence among participants

Skill	M	SD
Using digital tools for teaching	3.4	0.9
Protecting personal information	3.0	1.0
Communicating safely with students in digital environments	3.1	0.8
Recognizing online threats and risks	2.8	1.1
Ability to teach primary students the basics of digital safety	2.6	1.2

Participants exhibited moderate overall digital proficiency ($M = 3.2$), with the lowest confidence observed in their ability to teach cybersecurity ($M = 2.6$), indicating a significant training gap. This finding underscores the insufficient emphasis on cybersecurity pedagogy within current teacher education programs, aligning with prior research that calls for comprehensive curricular reform [54, 55]. The highest scores were recorded in the domain of using digital tools for educational purposes, indicating that pre-service teachers feel

relatively confident in applying ICT within professional contexts. Similarly, participants expressed moderately high confidence in safeguarding personal data and engaging in safe online communication with students, suggesting partial assimilation of key digital safety principles. Conversely, the lowest scores were associated with recognizing online threats and, in particular, with teaching digital safety to primary school students—highlighting substantial gaps in pedagogical preparation for cybersecurity education. The relatively high standard deviations observed across most items point to significant variability in participants' digital competence levels, reinforcing the need for differentiated and personalized instructional approaches within teacher training programs. This variability highlights the necessity of implementing differentiated and personalized approaches within teacher training programs to ensure that all future educators achieve a foundational level of cybersecurity competence. Collectively, these findings underscore the critical importance of systematically integrating both digital security content and corresponding instructional methodologies into teacher education curricula. Such integration is essential not only to strengthen pre-service teachers' individual digital literacy but also to equip them with the pedagogical capacity to foster safe and responsible digital learning environments in primary schools. Although participants demonstrated a strong motivation to enhance their knowledge of digital safety, current teacher education programs appear to underemphasize its pedagogical component, leaving a significant gap in practical preparedness.

Fig. 3 illustrates these differences visually.

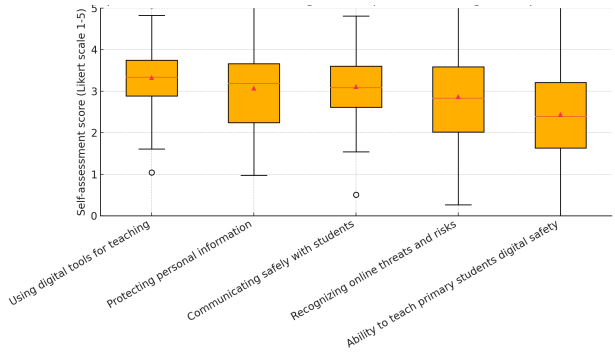

Fig. 3. Self-assessment of digital competence.

Skills related to the use of digital tools for teaching exhibit the highest median values and the lowest variability, indicating a generally strong level of confidence among participants in applying ICT in professional practice. Conversely, lower median scores and wider interquartile ranges are evident for competencies such as threat recognition and, most notably, the ability to teach digital safety to young learners. This pattern suggests two critical issues: limited confidence in these domains and substantial disparities in preparedness among future teachers. Such findings point to inconsistent or insufficient integration of cybersecurity pedagogy within the current teacher education curriculum. This results in uneven readiness to address digital safety in primary classrooms.

D. Motivational Readiness

Table 7 presents participants' motivational readiness regarding digital safety.

Participants demonstrated a high level of motivation to teach digital safety and a strong willingness to pursue additional training in this area. There was particularly strong consensus on the importance of educating children about safe digital practices and on the participants' personal desire to enhance their own competencies through further professional development. These findings suggest a favorable attitudinal foundation for integrating digital security modules into teacher education curricula.

Table 7. Descriptive statistics on motivational readiness

Item	M	SD
E1. Importance of teaching children about digital safety	4.4	0.7
E2. Sense of personal responsibility for digital safety	4.1	0.9
E3. Willingness to receive further training	4.5	0.6
E4. Digital safety is not teachers' responsibility *(reverse-coded)*	3.9	1.0

Table 8 summarizes gender-based differences in motivational attitudes and digital competencies.

Table 8. Gender-based differences in mean scores

Variable	Female (M ± SD)	Male (M ± SD)	t-value	p-value
Cybersecurity awareness (avg.)	2.8 ± 1.0	2.5 ± 1.1	1.35	0.18
Digital competence (avg.)	3.2 ± 0.9	2.9 ± 1.0	1.56	0.12
Motivational readiness (avg.)	4.3 ± 0.6	4.0 ± 0.7	2.14	**0.034**

Female participants reported slightly higher scores across all measured domains, with a statistically significant difference ($p < 0.05$) observed in motivational readiness. This indicates that female students exhibit a stronger sense of responsibility and a greater willingness to engage in digital safety practices compared to their male counterparts. These findings align with previous research suggesting that female pre-service teachers often demonstrate higher levels of compliance and readiness in relation to pedagogical innovations, including digital safety initiatives.

To visually represent these findings, Fig. 4 illustrates the average agreement scores on motivation to learn and teach digital safety across the sample, highlighting gender differences in motivational readiness.

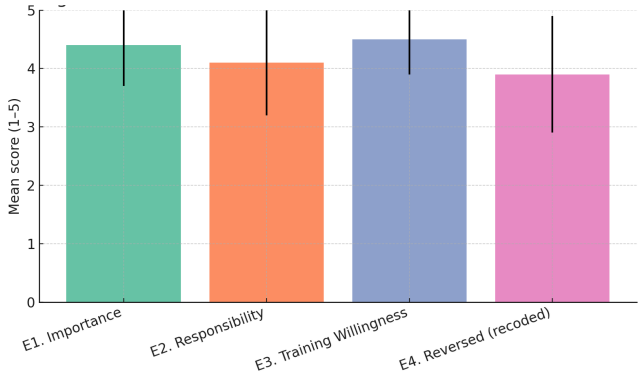

Fig. 4. Average agreement scores per item of the motivational readiness scale.

These findings indicate that motivational readiness to engage with digital safety education is generally strong among future primary school teachers. However, the reverse-coded item, which assessed the perception that

digital security is not a teacher's responsibility, exhibited a wider distribution of responses. This variability suggests that while most participants recognize their role in promoting digital safety, a subset of respondents remains uncertain about the extent of teacher responsibility in this domain. Such differences highlight the need for clearer role definition and explicit inclusion of digital security competencies within teacher education curricula.

V. Discussion

The findings indicate a moderate overall level of digital literacy among participants, with notable gaps in cybersecurity awareness. While technical digital skills are comparatively stronger than pedagogical readiness, the overall self-assessment of digital competence remains moderate. Participants demonstrate reasonable confidence in basic digital tasks, such as using digital tools for learning and safeguarding personal information. However, their preparedness to teach digital safety is significantly weaker, suggesting insufficient integration of cybersecurity pedagogy into teacher education programs. These results are consistent with prior research by Falloon [56] and From [57], which highlight that technical dimensions of digital competence typically develop more rapidly than pedagogical aspects.

Furthermore, the inclusion of motivational indicators demonstrates that participants not only possess basic digital competencies but also exhibit a strong willingness to assume pedagogical responsibility for cybersecurity. Responses to the reverse-coded item (E4) suggest that while most students recognize digital safety as a shared responsibility between educators and IT professionals, they do not view it as exclusively an IT issue. This perspective aligns with the argument of Kumpikaitė-Valiūnienė *et al.* [58], who stress that digital competence frameworks should extend beyond technical skills to include ethical responsibility and motivational readiness.

A comparison of the present findings with prior research reveals both convergences and divergences. For instance, studies by Mohamed Hashim *et al.* [59] and Küsel *et al.* [60] similarly report that higher education institutions tend to emphasize the development of practical digital skills, while the pedagogical integration of cybersecurity education remains underrepresented. This parallels the current results, where technical digital competencies scored higher than pedagogical preparedness for teaching digital safety.

Kazakhstan, similar to its Central Asian neighbors, remains behind OECD countries such as Finland and Estonia in the systematic integration of cybersecurity education. In these advanced systems, cybersecurity competencies are introduced early in teacher preparation programs and reinforced through national curricula. By contrast, Uzbekistan and Kyrgyzstan—sharing similar socio-educational conditions with Kazakhstan—encounter comparable challenges in embedding digital safety within teacher education. This comparative perspective highlights the urgent need for Kazakhstan to adopt comprehensive, policy-driven approaches modeled on international best practices, ensuring that cybersecurity education becomes an integral component of teacher training rather than an optional add-on.

This comparison underscores the urgent need to revise teacher education frameworks and implement targeted professional development programs that address both digital security and critical thinking skills [61]. Prior research demonstrates that embedding digital safety within teacher training curricula leads to a more balanced and comprehensive digital competence profile among future educators [62]. Against this backdrop, the findings of the present study reveal a pronounced gap in the methodological and substantive integration of cybersecurity into teacher preparation programs in Kazakhstan, indicating that current approaches remain insufficient to meet the demands of modern digital learning environments.

The results align with the findings of Pérez-Navío *et al.* [63], who reported that teachers frequently overestimate their technological proficiency, particularly in aspects related to ethical and responsible use. Similarly, Guillén-Gámez *et al.* [64] highlighted a persistent imbalance between the technological and pedagogical dimensions of digital competence, a pattern that is also evident in the present study. This imbalance suggests that while technical skills receive considerable emphasis in teacher education, the pedagogical integration of digital safety remains insufficiently addressed.

This study advances the discourse on digital pedagogical literacy by identifying critical vulnerabilities in pre-service teacher preparation. In particular, it underscores the necessity of reframing digital security as an integral component of pedagogical competence rather than treating it as a peripheral or technical issue.

The findings of this study reveal significant deficiencies in knowledge, behavioral practices, and pedagogical readiness related to cybersecurity among pre-service primary school teachers in Kazakhstan. These gaps underscore the pressing need for the systematic integration of comprehensive, context-sensitive digital safety education into teacher preparation curricula. Furthermore, the observed variability in digital competencies highlights the importance of adopting personalized and scaffolded learning pathways that account for differing baseline skills. Addressing these shortcomings is essential not only for strengthening individual digital resilience but also for equipping future educators to foster secure and responsible digital learning environments in primary education, thereby bridging existing gaps in teacher education programs.

The findings of this study provide actionable insights for teacher training institutions in Kazakhstan to revise and strengthen curricula on cybersecurity and digital hygiene. By pinpointing critical knowledge deficits alongside motivational strengths, institutions can design targeted interventions, such as competency-based learning modules and scenario-based training, that address both technical skills and pedagogical integration. Additionally, the structured assessment instrument developed for this research offers a practical tool for monitoring digital competence and can be adapted for use in comparable educational settings beyond Kazakhstan, particularly in Central Asian countries facing similar challenges in implementing comprehensive digital safety education.

A. Limitations of the Study

This study is subject to several limitations that should be

considered when interpreting the findings. First, the sample was restricted to students from a single pedagogical university in Kazakhstan, which constrains the generalizability of the results to the broader population of pre-service teachers in the country. Second, the exclusive reliance on quantitative methods—specifically, a structured questionnaire—limited the ability to explore the underlying factors contributing to the observed gaps in digital competence. Future research would benefit from a mixed-methods approach, incorporating qualitative interviews, focus groups, and classroom observations to provide deeper insights into motivational and contextual influences. Third, the use of self-reported measures may have introduced social desirability bias or inaccuracies due to recall errors. To mitigate this, subsequent studies should include objective assessments, such as performance-based tasks or digital simulations, to triangulate the data. Finally, the findings represent a snapshot of digital literacy at the time of data collection and do not capture potential developments following curricular updates or institutional interventions. Longitudinal studies are recommended to track changes over time and evaluate the impact of emerging educational initiatives.

B. Recommendations

1) Mandate the Integration of Cybersecurity and Digital Hygiene into Teacher Education Curricula

Teacher training programs should include dedicated, compulsory modules on cybersecurity and digital hygiene. These modules must be embedded across pedagogical courses to ensure the systematic development of digital safety competencies from the outset of teacher education.

2) Standardize Instructional Tools and Practical Digital Safety Training

All teacher education institutions should be required to provide approved instructional materials and deliver hands-on training sessions. This approach ensures that future teachers develop both theoretical knowledge and practical skills for maintaining secure digital environments.

3) Implement Compulsory Professional Development for In-Service Teachers

Continuous training on cybersecurity and digital hygiene should be made a mandatory element of professional development for current teachers. This requirement will keep teaching practices aligned with evolving digital threats and updated educational standards.

4) Establish a National System for Regular Assessment of Digital Competence

Education authorities should enforce systematic evaluations of digital and cybersecurity competencies for both pre-service and in-service teachers. The results of these assessments should inform curriculum revisions and the design of targeted interventions.

5) Foster Institutional Collaboration with Cybersecurity Professionals

Teacher education institutions must collaborate with cybersecurity experts and relevant organizations to co-develop course content and training activities. Such partnerships ensure technical accuracy, practical relevance, and alignment with Kazakhstan's national digital education strategy.

VI. Conclusion

This study demonstrates that pre-service primary school teachers in Kazakhstan exhibit insufficient cybersecurity awareness and uneven digital competence, particularly in relation to teaching digital safety. The findings reveal critical gaps in knowledge, behavioral practices, and motivational readiness concerning digital security and hygiene.

To address these deficiencies, teacher education programs must be revised to systematically integrate cybersecurity pedagogy into core curricula. Key measures include the implementation of dedicated modules on digital safety, incorporation of hands-on training, and continuous assessment of digital competencies using validated instruments. Furthermore, personalized and scaffolded learning pathways can accommodate the varying skill levels among future teachers, ensuring a solid foundation for all participants.

Collaboration between universities, schools, and IT professionals is essential to provide real-world learning experiences that translate theoretical knowledge into practical skills. Effective implementation also requires clearly defined institutional policies, such as:

1) Integrating cybersecurity learning outcomes into national teacher standards;
2) Training faculty members to model best practices in digital safety; and
3) Allocating resources for ongoing professional development and digital upskilling.

Ultimately, equipping future teachers with robust digital security competencies will enhance their individual literacy and empower them to cultivate safer and more resilient digital learning environments for their students. Future research should further investigate cross-national comparisons to identify best practices and policy innovations that can inform Kazakhstan's approach to teacher preparation in digital security.

Appendix

Appendix provides the full version of the questionnaire used in this study. It contains all items grouped into five sections together with their response formats. This instrument formed the basis for the analyses reported in the results section.

Table A1. Questionnaire

Section	Item	Question / Statement	Response options
A. Demographics	A1	Gender	☐ Female ☐ Male
	A2	Age	☐ 18–20 ☐ 21–23 ☐ 24 and older
	A3	Year of study	☐ 3rd year
B. Cybersecurity awareness	B1	Knowledge of safe password practices	① ② ③ ④ ⑤

	B2	Ability to recognize phishing emails	① ② ③ ④ ⑤
	B3	Awareness of importance of software updates	① ② ③ ④ ⑤
	B4	Understanding risks of sharing personal data online	① ② ③ ④ ⑤
	B5	Knowledge of secure use of social networks	① ② ③ ④ ⑤
C. Digital hygiene	C1	How often do you update your software?	☐ Always ☐ Sometimes ☐ Never
	C2	Do you use antivirus software?	☐ Yes, regularly ☐ Sometimes ☐ No
	C3	How do you store your passwords?	☐ Stored openly (e.g., notebook, notes app) ☐ Stored securely (e.g., password manager, memorized)
	C4	Have you received training in digital safety?	☐ Yes, through university courses ☐ Yes, through self-education ☐ No
D. Digital competence	D1	Using digital tools for teaching	① ② ③ ④ ⑤
	D2	Protecting personal information	① ② ③ ④ ⑤
	D3	Communicating safely with students online	① ② ③ ④ ⑤
	D4	Recognizing online threats and risks	① ② ③ ④ ⑤
	D5	Teaching digital safety to primary students	① ② ③ ④ ⑤
E. Motivational readiness *(Rate on a scale of 1 to 5; 1 – Strongly disagree, 5 – Strongly agree)*	E1	I believe it is important to teach children about digital safety.	① ② ③ ④ ⑤
	E2	I feel personally responsible for creating a safe digital environment.	① ② ③ ④ ⑤
	E3	I would like to receive additional training on digital hygiene.	① ② ③ ④ ⑤
	E4 *(reverse-coded)*	I think digital safety is mostly the responsibility of IT professionals, not educators.	① ② ③ ④ ⑤
Note: E4 is reverse-coded. During analysis, its score should be inverted (e.g., 1 → 5, 2 → 4, etc.) to align with the motivational scale.			

CONFLICT OF INTEREST

The authors declare no conflict of interest.

AUTHOR CONTRIBUTIONS

Conceptualization, AA and AZ; methodology, AK; software, AZ; validation, AT, KZ and AZ; formal analysis, AA; investigation, AK; resources, AZ; data curation, AK; writing—original draft preparation, AT; writing—review and editing, KZ; visualization, AK; supervision, AZ; project administration, AA; funding acquisition, AZ. All authors have read and agreed to the published version of the manuscript.

REFERENCES

[1] D. P. F. Möller, "Cybersecurity in digital transformation," *Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices*, Springer, Cham, vol. 103, pp. 1–70, 2023. doi: 10.1007/978-3-031-26845-8_1

[2] S. S. Goswami, S. Sarkar, K. K. Gupta, and S. Mondal, "The role of cyber security in advancing sustainable digitalization: Opportunities and challenges," *Journal of Decision Analytics and Intelligent Computing,* vol. 3, no. 1, pp. 270–285, Dec. 2023. doi: 10.31181/jdaic10018122023g

[3] F. Ferri, P. Grifoni, and T. Guzzo, "Online learning and emergency remote teaching: Opportunities and challenges in emergency situations," *Societies*, vol. 10, no. 4, p. 86, Nov. 2020. doi: 10.3390/soc10040086

[4] S. Timotheou *et al.*, "Impacts of digital technologies on education and factors influencing schools' digital capacity and transformation: A literature review," *Education and Information Technologies*, vol. 28, no. 6, pp. 6695–6726, Nov. 2023. doi: 10.1007/s10639-022-11431-8

[5] Ł. Tomczyk, "Skills in the area of digital safety as a key component of digital literacy among teachers," *Education and Information Technologies*, vol. 25, no. 1, pp. 471–486, 2020. doi: 10.1007/s10639-019-09980-6

[6] O. Shkvyr, I. Haidamashko, and S. Tafintseva, "Developing critical thinking in younger pupils using ICT," *Broad Research in Artificial Intelligence and Neuroscience,* vol. 11, no. 2, pp. 230–242, 2020. doi: 10.70594/brain/11.2/85

[7] F. Martin *et al.,* "Teacher and school concerns and actions on elementary school children digital safety," *TechTrends*, vol. 67, no. 3, pp. 561–571, 2023. doi:10.1007/s11528-022-00803-z

[8] A. R. Lauricella, J. Herdzina, and M. Robb, "Early childhood educators' teaching of digital citizenship competencies," *Computers & Education*, vol. 158, 103989, 2020. doi: 10.1016/j.compedu.2020.103989

[9] Z. Yu, "Sustaining student roles, digital literacy, learning achievements, and motivation in online learning environments during the COVID-19 pandemic," *Sustainability*, vol. 14, no. 8, 4388, 2022. doi: 10.3390/su14084388

[10] J. Bacak *et al.,* "Elementary educator perceptions of student digital safety based on technology use in the classroom," *Computers in the Schools,* vol. 39, no. 2, pp. 186–202, 2022. doi: 10.1080/07380569.2022.2071233

[11] S. Baraković and J. B. Husić, "Cyber hygiene knowledge, awareness, and behavioral practices of university students," *Information Security Journal: A Global Perspective,* vol. 32, no. 5, pp. 347–370, 2023. doi: 10.1080/19393555.2022.2088428

[12] R. Armas and H. Taherdoost, "Building a cybersecurity culture in higher education: proposing a cybersecurity awareness paradigm," *Information,* vol. 16, no. 5, 336, 2025. doi: 10.3390/info16050336

[13] E. C. K. Cheng and T. Wang, "Institutional strategies for cybersecurity in higher education institutions," *Information*, vol. 13, no. 4, 2022. doi: 10.3390/info13040192

[14] S. Yusif and A. Hafeez-Baig, "Cybersecurity policy compliance in higher education: a theoretical framework," *Journal of Applied Security Research,* vol. 18, no. 2, pp. 267–288, 2023. doi: 10.1080/19361610.2021.1989271

[15] M. N. AL-Nuaimi, "Human and contextual factors influencing cyber-security in organizations, and implications for higher education institutions: a systematic review," *Global Knowledge, Memory and Communication*, vol. 73, no. 1/2, pp. 1–23, 2024. doi: 10.1108/GKMC-12-2021-0209

[16] L. Bottyán, "Cybersecurity awareness among university students," *Journal of Applied Technical and Educational Sciences,* vol. 13, no. 3, pp. 363–363, 2023. doi: 10.24368/jates363

[17] K. Matyokurehwa *et al.,* "Cybersecurity awareness in Zimbabwean universities: Perspectives from the students," *Security and Privacy*, vol. 4, no. 2, 2021. doi: doi.org/10.1002/spy2.141

[18] M. E. Erendor and M. Yildirim, "Cybersecurity awareness in online education: A case study analysis," *IEEE Access*, vol. 10, pp.

52319–52335, 2022. doi: 10.1109/ACCESS.2022.3171829
[19] M. A. Ayanwale *et al.*, "A structural equation approach and modelling of Pre-service teachers' perspectives of cybersecurity education," *Education and Information Technologies,* vol. 29, no. 3, pp. 3699–3727, 2024. doi: 10.1007/s10639-023-11973-5
[20] N. Torres-Hernández and M. J. Gallego-Arrufat, "Indicators to assess preservice teachers' digital competence in security: A systematic review," *Education and information technologies,* vol. 27, no. 6, pp. 8583–8602, 2022. doi: 10.1007/s10639-022-10978-w
[21] İ. Reisoğlu and A. Çebi, "How can the digital competences of pre-service teachers be developed? Examining a case study through the lens of DigComp and DigCompEdu," *Computers & Education*, vol. 156, 103940, 2020. doi: 10.1016/j.compedu.2020.103940
[22] J. B. Ulven and G. Wangen, "A systematic review of cybersecurity risks in higher education," *Future Internet*, vol. 13, no.2, 39, 2021. doi: 10.3390/fi13020039
[23] W. J. Triplett, "Addressing cybersecurity challenges in education," *International Journal of STEM Education for Sustainability,* vol. 3, no. 1, pp. 47–67, 2023. doi: 10.53889/ijses.v3i1.132
[24] M. F. Safitra, M. Lubis, and H. Fakhrurroja, "Counterattacking cyber threats: A framework for the future of cybersecurity," *Sustainability*, vol. 15, no.18, 13369, 2023. doi: 10.3390/su151813369
[25] K. Potyrała and Ł. Tomczyk, "Teachers in the lifelong learning process: examples of digital literacy," *Journal of Education for Teaching,* vol. 47, no. 2, pp. 255–273, 2021. doi: 10.1080/02607476.2021.1876499
[26] S. AlDaajeh *et al.,* "The role of national cybersecurity strategies on the improvement of cybersecurity education," *Computers & Security*, vol. 119, 102754, 2022. doi: 10.1016/j.cose.2022.102754
[27] U. Abdigapbarova *et al.,* "Shaping digital communication culture in prospective teachers: The role of digital etiquette training in Kazakhstan," *International Journal of Innovative Research and Scientific Studies,* vol. 8, no. 1, pp. 2121–2132, 2025. doi: 10.53894/ijirss.v8i1.4903
[28] G. Kurebayeva *et al.,* "From tradition to innovation: Pre-Service teachers' perceptions of digital transformation in language learning," *Forum for Linguistic Studies,* vol. 7, no. 3, pp. 351–361, 2025. doi: 10.30564/fls.v7i3.8768
[29] M. Ayyash *et al.,* "Cybersecurity education and awareness among parents and teachers: A survey of Bahrain," *IEEE Access,* vol. 12, pp. 86596–86617, 2024. doi: 10.1109/ACCESS.2024.3416045
[30] H. Guo and H. Tınmaz, "A survey on college students' cybersecurity awareness and education from the perspective of China," *Journal for the Education of Gifted Young Scientists*, vol.11, no. 3, pp. 351–367, 2023. doi:10.17478/jegys.1323423
[31] W. C. H. Hong *et al.,* "The influence of social education level on cybersecurity awareness and behaviour: A comparative study of university students and working graduates," *Education and information technologies*, vol. 28, no. 1, pp. 439–470, 2023. doi: 10.1007/s10639-022-11121-5
[32] M. Zwilling *et al.,* "Cyber security awareness, knowledge and behavior: A comparative study," *Journal of Computer Information Systems,* vol. 62, no. 1, pp. 82–97, 2022. doi: 10.1080/08874417.2020.1712269
[33] S. Nurgaliyeva *et al.,* "Examining the relationships between teachers' job satisfaction and technological competencies," *International Journal of Education in Mathematics, Science and Technology,* vol. 11, no. 4, pp. 898–912, May 2023. doi: /10.46328/ijemst.3375
[34] S. Zhussupbayev *et al.,* "The effect of using computer assisted instruction method in history lessons on students' success and attitudes," *International Journal of Education in Mathematics Science and Technology*, vol. 11, no. 2, pp. 424–39, Jan. 2023. doi: 10.46328/ijemst.3136
[35] S. Nurgaliyeva *et al.,* "COVID-19 online learning challenges: Kazakhstan secondary schools case study," *Frontiers in Education,* vol. 9, 1448594, Oct. 2024. doi: 10.3389/feduc.2024
[36] M. Khader, M. Karam, and H. Fares, "Cybersecurity awareness framework for academia," *Information*, vol. 12, no. 10, 417, 2021. doi: 10.3390/info12100417
[37] Y. Sui, "The investigation of cybersecurity education among college students: Aiming to address the scarcity of skilled professionals," *The Educational Review, USA*, vol. 8, no. 6, pp. 801–807, 2024. doi: 10.26855/er.2024.06.002
[38] B. Wibowo *et al.,* "Cyber resilience to digital threats for education institutions 4.0," *International Journal of Management Science and Application*, vol. 4, no.1, pp. 35–45, 2025. doi: 10.58291/ijmsa.v4i1.370
[39] F. Douzet and A. Gery, "Cyberspace is used, first and foremost, to wage wars: proliferation, security and stability in cyberspace," *Journal of Cyber Policy,* vol. 6, no. 1, pp. 96–113, 2021. doi: 10.1080/23738871.2021.1937253
[40] M. Marelli, "Hacking humanitarians: Defining the cyber perimeter and developing a cybersecurity strategy for international humanitarian organizations in digital transformation," *International Review of the Red Cross*, vol. 102, no. 913, pp. 367–387, 2020. doi: 10.1017/S1816383121000151
[41] F. J. R. Estrada, C. E. George-Reyes, and L. D. Glasserman-Morales, "Security as an emerging dimension of Digital Literacy for education: A systematic literature review," *Journal of e-Learning and Knowledge Society*, vol. 18, no. 2, pp. 22–33, 2022. doi: 10.20368/1971-8829/1135440
[42] T. Sari and F. Nayır, "Challenges in distance education during the (COVID-19) pandemic period," *Qualitative Research in Education,* vol. 9, no. 3, pp. 328–360, Oct. 2020. doi: 10.17583/qre.2020.5872
[43] D. Sosa and M. José, "Emergency remote education, family support and the digital divide in the context of the COVID-19 lockdown," *International Journal of Environmental Research and Public Health*, vol. 18, no. 15, 7956, 2021. doi: 10.3390/ijerph18157956
[44] B. Jerman Blažič and A. J. Blažič, "Cybersecurity skills among European high-school students: A new approach in the design of sustainable educational development in cybersecurity," *Sustainability,* vol. 14, no. 8, 4763, 2022. doi: 10.3390/su14084763
[45] A. Vishwanath *et al.,* "Cyber hygiene: The concept, its measure, and its initial tests," *Decision Support Systems*, vol. 128, 113160, 2020. doi: 10.1016/j.dss.2019.113160
[46] A. Mishra *et al.,* "Attributes impacting cybersecurity policy development: An evidence from seven nations," *Computers & Security*, vol. 120, 102820, 2022. doi: 10.1016/j.cose.2022.102820
[47] K. Sultan and A. Ahmed, "A framework for regulating digital lives in the context of digital etiquettes and responsibilities," *Online Media and Society*, vol. 3, pp. 273–281, 2022. doi: 10.71016/oms/ta3bkv41
[48] F. Schulze *et al.,* "Air quality effects on human health and approaches for its assessment through microfluidic chips," *Genes*, vol. 8, no. 10, 244, 2017. doi: 10.3390/genes8100244
[49] C. Yegen, A. M. Kirik, and A. Çetinkaya, "Sustainability, digital security, and cyber hygiene during the COVID-19 pandemic," *New Normal in Digital Enterprises: Strategies for Sustainable Development.* Singapore: Springer Nature Singapore, pp. 91–105, 2023. doi: 10.1007/978-981-19-8618-5_5
[50] M. Temirkhanova, G. Abildinova, and C. Karaca, "Enhancing digital literacy skills among teachers for effective integration of computer science and design education: A case study at Astana International School, Kazakhstan," *Frontiers in Education,* vol. 9, 2024.
[51] J. L. Sidel, R. N. Bleibaum, and K.W. C. Tao, "Quantitative descriptive analysis," *Descriptive analysis in Sensory Evaluation*, pp. 287–318, 2018. doi: 10.1002/9781118991657.ch8
[52] J. Mattar, C. C. Santos, and L. M. Cuque, "Analysis and comparison of international digital competence frameworks for education," *Education Sciences*, vol. 12, no. 12, 2022. doi: 10.3390/educsci12120932
[53] R. Pirta-Dreimane *et al.*, "Application of intervention mapping in cybersecurity education design," *Frontiers in Education*, vol. 7, 998335, 2022. doi: 10.3389/feduc.2022.998335
[54] I. Adeshola and D. I. Oluwajana, "Assessing cybersecurity awareness among university students: Implications for educational interventions," *Journal of Computers in Education,* pp. 1–23, 2024. doi: 10.1007/s40692-024-00346-7
[55] G. Childers *et al.,* "K-12 educators' self-confidence in designing and implementing cybersecurity lessons," *Computers and Education Open*, vol. 4, 2023. doi: 10.1016/j.caeo.2022.100119
[56] G. Falloon, "From digital literacy to digital competence: The teacher digital competency (TDC) framework," *Educational Technology Research and Development*, vol. 68, no. 5, pp. 2449–2472, 2020. doi: 10.1007/s11423-020-09767-4
[57] J. From, "Pedagogical digital competence--between values, knowledge and skills," *Higher Education Studies,* vol. 7, no. 2, pp. 43–50, 2017. doi: 10.5539/hes.v7n2p43
[58] V. Kumpikaitė-Valiūnienė *et al.*, "Influence of digital competence on perceived stress, burnout and well-being among students studying online during the COVID-19 lockdown: A 4-country perspective," Psychology research and behavior management, pp. 1483–1498, 2021. doi: 10.2147/PRBM.S325092
[59] M. A. Mohamed Hashim, I. Tlemsani, and R. D. Matthews, "A sustainable university: Digital transformation and beyond," *Education and Information Technologies*, vol. 27, no. 7, pp. 8961–8996, 2022. doi: 10.1007/s10639-022-10968-y
[60] J. Küsel, F. Martin, and S. Markic, "University students' readiness for using digital media and online learning—Comparison between Germany and the USA," *Education Sciences*, vol. 10, no.11, 2020. doi: 10.3390/educsci10110313
[61] K. I. Tuxtayevich *et al.,* "Different approaches to enhance critical thinking in digital education," *SPAST Reports*, vol. 1, no. 7, Aug. 2024.

doi: 10.69848/sreports.v1i7.5086
[62] J. M. García-Vandewalle García *et al.,* "Analysis of digital competence of educators (DigCompEdu) in teacher trainees: The context of Melilla, Spain," *Technology, Knowledge and Learning,* vol. 28, no. 2, pp. 585–612, 2023. doi: 10.1007/s10758-021-09546-x
[63] E. Pérez-Navío, M. T. Ocaña-Moral, and M. D. C. Martínez-Serrano, "University graduate students and digital competence: Are future secondary school teachers digitally competent?" *Sustainability*, vol. 13, no. 15, 8519, 2021. doi: 10.3390/su13158519
[64] F. D. Guillén-Gámez *et al.,* "Analysis of teachers' pedagogical digital competence: Identification of factors predicting their acquisition," *Technology, Knowledge and Learning*, vol. 26, no. 3, pp. 481–498, 2021. doi: 10.1007/s10758-019-09432-7