ISSN 2663-8169 Vol. 5, Issue 1: 31-41, DOI: 10.25236/IJNDE.2023.050106

Exploring English Preservice Teachers' Digital Competence Perceptions Regarding the C3 Matrix-cyber Ethics, Cyber Security and Cyber Safety: An Empirical Study Executed in China

Dai Wuyun

School of Foreign Languages, Inner Mongolia Normal University, Hohhot, China

Abstract: *This study was executed with an attempt to figure out Chinese English preservice teachers' digital competence perceptions pertaining the C3 Matrix, namely cyber ethics, cyber security and cyber safety. 221 senior students majoring in English Education in a normal university in northern China participated in the data collection process. Structural equation modelling (SEM) was employed in this study, which contained four latent variables: cyber ethics, cyber security, cyber safety and digital competence. Major findings suggest that how English preservice teachers perceive the C3 Matrix exerts mixed impacts on their digital competence perceptions. First, English preservice teachers' cyber ethics perceptions have great positive impact on how they perceive cyber security and cyber safety. Cyber security and cyber safety then exert similar positive effects on how they perceive their digital competence. What's worth noticing is that although cyber ethics exerts positive influence on digital competence via the agency of cyber security and cyber safety, it alone exerts minor negative effects on the participants' digital competence perceptions, which is thought-provoking since no previous research so far echoed with this outcome.*

Keywords: *Preservice Teachers; Digital Competence; Cyber Ethics; Cyber Security; Cyber Safety*

1. Introduction

The unprecedented development of Information and Communication Technologies (ICT) calls out urgent demand on teachers' digital competence in the domain of education. As digital natives, preservice teachers are expected to be digitally competent so as to be highly qualified in preparing youngsters while facing the unknown future. Notwithstanding people's high hopes for them, the status quo of Chinese English preservice teachers' digital competence is far from content. It's said that Educational Informatization is the basic connotation of Educational Modernization, [1] the Chinese Ministry of Education precisely stresses the importance of innovation of the training program for preservice teachers, which focuses mainly on the enhancement of preservice teachers' overall digital competence. [1] It also promotes that local authorities shall enhance teachers' digital competence through demonstrative training projects and shall make hard efforts on escalating the accuracy of evaluation system and the effectiveness of the training process. [1]

The official document < Comprehensively Deepening the Reform of the Construction of Teachers in the New Era> issued by the Chinese government declares that by the year of 2035, teachers' comprehensive quality, professional level and innovative ability shall be greatly improved, and millions of cadre teachers, hundreds of thousands of excellent teachers and tens of thousands of other educators shall be trained effectively by then. [2] With an attempt to bring this aforementioned vision to life, teachers are encouraged to actively adapt to new technological changes such as informatization and artificial intelligence, which in return raises urgent requests for them to strengthen their comprehensive capacities, with digital competence being the utmost constituent.

Although official documents like ones listed above made it clear that digital competence is of vital importance in teachers' professional development, huge gaps between the implementation status of preservice teachers' training programs and the preset training objectives need to be addressed. [3] The unparalleled spread of modern-day technologies and the on-going COVID-19 pandemic force everyone to be involved in the world-wide digitalization progress. However, there's a scarcity of empirical studies of preservice teachers' digital competence within the domain of Chinese education context. [3] In this

ISSN 2663-8169 Vol. 5, Issue 1: 31-41, DOI: 10.25236/IJNDE.2023.050106

regard, this study aims at investigating the current status quo of digital competence of preservice teachers who are striving for obtaining their bachelors' degree in English Education in a normal university in northern China. The phrase "digital competence" is a well-structured technical term with rich connotation. [3] Hence, to keep the research focused, this study solely copes with preservice teachers' digital competence perceptions, with such related topics as cyber ethics, cyber security and cyber safety underneath it.

In order to explore Chinese English preservice teachers' digital competence perceptions in relation to cyber ethics, cyber security and cyber safety, this paper begins with a general introduction of the status quo of Chinese English preservice teachers' digital competence. After that, literature review focusing on preservice teachers' digital competence and the evolvement of the C3 Matrix, namely cyber ethics, cyber security and cyber safety is presented. This is followed by research methodology, data analysis process, statistical results and research-based discussion. The main structure of this paper ends with conclusions solely based on the empirical data within this research and acknowledgements.

2. Literature Review

2.1. Digital competence

2.1.1. Definition of Digital Competence

When it comes to the year 2020, the global COVID-19 health crisis caught everybody off guard, people were forced to live in a world where Information and Communication Technologies (ICT) dominates every aspect of life. Under this specific background, teachers being the core in the process of transferring what was done offline into massive online courses, their overall digital competence once again were put under challenge. For teachers, digital competence is rendered as one of their professional competences that they must excel in a world dominated by the state-of-the-art technologies. [4] A decade ago, Ferrari et al. [5] suggested that the concept of digital competence is "a muti-faceted moving target", which means the precise description of the term may vary from one literature to another. According to Ferrari et al. [6], digital competence may be perceived as "the confident, critical and creative use of ICT to maintain goals in relation to work, employability, learning, leisure, inclusion and/or participation in society". Two pertinent features of this statement are worth mentioning: First, it attaches great importance on describing individuals' mastery of ICT; Second, it covers a wide range of usage scenario, which means the connotation of digital competence can be highly context oriented. At the United Nations level, the professional level of teachers' digital competence relies more on how well it functioned in supporting students from underdeveloped world obtaining just the same quality of education as other children from the rest of the world are receiving in the wake of the unprecedented worldwide health crisis. [7] [8] Teachers' digital competence under this circumstance is about ensuring the high standards of distance learning for students from rural areas. To be specific, teachers are expected to be well-prepared in terms of pedagogical technology, teaching content, online learning strategies instruction, online evaluation readiness, etc. [9] At the European level, The Council of the European Union released an official paper on citizens' key competences for lifelong learning, within which digital competence was prescribed as one of the eight key competences of all individuals in today's all-immersed digitalized world. [10] To some extent, the phrase digital competence is viewed as an umbrella term which is composed of multiple constituents like information and data literacy, communication and collaboration, cyber security, problem solving and critical thinking, etc. [10] Similar to that, the "European Framework for the Digital Competence of Educators: DigCompEdu" differentiated the connotation of teachers' digital competence into six interrelated yet separated areas, mainly enunciated as 1) Professional Engagement; 2) Digital Resources; 3) Teaching and Learning; 4) Assessment; 5) Empowering Learners and 6) Facilitating Learners' Digital Competence. [8] This so-called six-faceted assessment framework is further divided into 22 competences, which could be regarded as a hint as to how complicated teachers' digital competence can be. At the Chinese education level, it's reported that up until June in 2021, the overall online education population in China has mounted over 325 million, which occupies 32.1% of the whole netizen community. [11] A huge amount of online population like the one China has needs to be equipped with teachers with high levels of digital competence. In this regard, the assessment, the training and the recognition of Chinese teachers' digital competence need to be seriously coped with.

2.1.2. Evaluation of Digital Competence

Earnest endeavors have been made to come up with effective digital competence evaluation tools, recommendations and instructions. Ferrari et al. [5] analyzed 15 digital competence frameworks whose

ISSN 2663-8169 Vol. 5, Issue 1: 31-41, DOI: 10.25236/IJNDE.2023.050106

target groups were mostly teachers and students, and they concluded that there were six areas of digital competence mentioned repeatedly in the literature selected, namely: 1) information management collaboration, 2) communication and sharing, 3) creation of content and knowledge, 4) ethics and responsibility, 5) evaluation and problem-solving, and 6) technical operations. Within the domain of education, some newly developed frameworks and instruments in relation to the evaluation of teachers and educators' overall digital competence are found in the literature. [3][9] [12] [13][14] Among all these current frameworks and instruments relating to the rating of educators' digital competence, <European Framework for the Digital Competence of Educators>, "DigCompEdu" for short, has been enjoying quite a high level of recognition and reference.

Empirical studies were carried out to corroborate the reliability and validity of the "DigCompEdu". [14][15] Ghomi and Redecker[15] developed a self-assessment tool based on the "DigCompEdu" and tested it against 335 teachers in Germany. By deeply scrutinizing the data they received, they found that the instrument showed a highly plausible internal consistency with a value of .934 for Cronbach's alpha. [15] In addition to that, they further pointed out that subtle, yet undeniable differences were shown among teachers with different subject backgrounds, indicating that the "DigCompEdu" framework was eligible in multiple evaluation contexts. Great contribution was made by Julio Cabero-Almenara and Palacios-Rodríguez[14] who successfully composed an all-rounded demonstration on the detailed content, application and adoption of the < "DigCompEdu" Check-In> questionnaire, which turned out to be a big booster to the subsequent developments of the "DigCompEdu" related evaluation instruments. Later that year, J. Cabero-Almenara et al. [13] summoned over two thousand professors from different universities in Spain to take the online "DigCompEdu" Check-In questionnaire. It was no surprise that the statistical results of their study strongly aligned with Redecker and Ghomi's[15] findings, with a value of .967 for the McDonald's omega coefficient, which, according to the authors, possessed more vantages than Cronbach's Alpha did. [13]

2.2. The C3 Matrix: Cyber Ethics, Cyber Security and Cyber Safety

The rapid growth of information and communication technologies and frequent engagement with digital devices raise high challenges on individuals' knowledge, awareness and perceptions on behave themselves properly and safely in cyberspace such as how to identify false or toxic information and how to protect themselves from cyber-attacks, etc.

The C3 Matrix-cyber ethics, cyber security and cyber safety, initially known as C3 framework, was proposed by Pruitt-Mentle in the year of 2000. She analogized the three concepts in the C3 Matrix to the action of riding bikes: First, as highly civilized human beings, we tend not to deliberately ride our bikes on neighbors' lawn, meaning that cyber ethics is personal choice to some extent; Second, since we do not intend to get into trouble, we maintain our awareness to behave safely by obeying the traffic laws, which analogies netizens' safe practices; Third, to secure the process of bike-riding, we need to make sure all the accessories of the bike are in good condition, implying that individuals must pay attention to some necessary steps or procedures while surfing on the internet. [16] As vividly as these analogies sound, we still need legitimate definitions to better describe these core concepts.

2.2.1. Definition of Cyber Ethics, Cyber Security and Cyber Safety

Flexible intension and extension regarding the connotation of the C3 Matrix-cyber ethics, cyber security and cyber safety was found in the literature.

Ethical issues are somewhat subjective. It's about principles, beliefs or moral codes that people rely on when they face the dilemma of choice. Similar interpretation about the implication of "ethics" was found in the literature: "Ethics" refers to a series of interrelated codes or principles that people live by; It's about the criteria that they turn to when they need to differentiate right from wrong. [17] Cyber ethics is therefore generally referred to as people's ethical choice in cyberspace.

To be specific, on one hand, from Pruitt-Mentle's[16] point of view, cyber ethics refers to netizens' ethical behaviors, moral duties or obligations within Internet-related contexts. On the other hand, cyber ethics is also about the philosophical aspect of the whole ethics system which specifically related to individuals' network-based manners, awareness, knowledge, etc. [18] In other words, cyber ethics asks for individuals' legal, rational and ethical manner while engaging in an online environment. [19] It is not newly "invented" ethics, but a specific concept refers to old topics. [20]

In general, terms like cyber security and cyber safety are mentioned both in daily internet surfing scenario and when facing cyber dilemma like data breaches. These two terms mostly differ on one

ISSN 2663-8169 Vol. 5, Issue 1: 31-41, DOI: 10.25236/IJNDE.2023.050106

condition: cyber security is often used when facing malicious activities, and cyber safety, on the other hand, is used in describing ordinary online errands. [21]

Calls for people's attention on cyber security are the byproducts of the immense popularization of modern technologies. The catch-all application of Big Data [22] brings people not only the unimaginable convenience in all sorts of ways, but also gives rise to potential consequences like the possibility of malicious cyber-attacks or data breaches. It's at this point that the significance of maintaining cyber security is worth noticing. Generally speaking, the term cyber security has a broad coverage that takes a range from information resources protection to avoiding human rights violation like cyber-attacks and internet fraud and so forth. [23] Cyber security refers to techniques or skills people use when trying to prevent their digital gadgets from exposing to vicious cyberspace. [24] It is about taking effective measures to consolidate a safer and stronger internet environment. These consolidation procedures cover myriads of actions, such as installing anti-virus packages or programs, setting up firewalls, keeping software updated regularly, etc. [16] A more comprehensive and well-structured definition of this term is given by the International Telecommunication Union (ITU): Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. [25]

Cyber safety is broadly defined as the safe and rational adoption of information and communication technologies. [26] It covers such a mixed range of cyber oriented issues as social networking, digital fraud, cyber bullying, cyber plagiarism, etc. [26] It addresses people's ability to act safely and dutifully in an internet-involved environment. [27] Safe internet-related behaviors help secure individuals' personal online information and the legitimacy of their cyber practices. Cyber safety is of great significance in minimizing potential danger from behavioral-based malpractice, but it cannot free people from hardware/software-based troubles. [27]

2.2.2. Evaluation of Cyber Ethics, Cyber Security and Cyber Safety

A national baseline survey regarding the C3 topics was carried out in the U.S educational settings in 2009. [28] As it turned out, participants like in-service teachers were not completely competent in C3 education, and neither did they feel content towards the C3-related training they received, which led to their unpreparedness of delivering the C3 content to students. [28] The researcher further pointed out that both teachers and teacher educators expressed their needs of undertaking professional training regarding the C3 topics to better cultivate the next generation [28]. Mosalanejad et al. [18] conducted 25 individual semi-structured interviews and 5 focused group interviews on university students with different major backgrounds, and they concluded that various elements such as culture, family background and religions are influential in one's cyber ethics developing process. This finding does make sense, considering how external environment exerts certain effects on individuals' value forming courses.

Pusey and Sadera [29] created a C3 Awareness and Instrumental Preparedness instrument which was composed of 75 C3 topics. Then, they asked 312 preservice teachers from a Mid-Atlantic university to take the test, which required them to self-evaluate their knowledge of these topics and their competence of teaching these topics in pedagogical contexts. As statistical results indicated, the respondents' knowledge level of C3 topics was far from satisfying, and so did their perception of teaching these topics for educational purposes. [29]

Since these three concepts of the C3 Matrix are intrinsically interrelated with each other, [30] researchers took a step further to the exploration of the evaluation of them, which led to the invention of the iKeepSafe Digital Citizenship C3 Matrix that covered three levels of proficiency: basic, intermediate and proficient. [27] For educators, the C3 Matrix could be utilized both as a guidance on how to instruct students regarding cyber ethics, cyber security and cyber safety, and as an instrument for the evaluation of their competency on specific subjects. In this study, all of the C3 Matrix elements were put into examination, each of which were assigned with questions with similar yet unique content within them.

2.3. Research Questions and Hypotheses

Two research questions (RQs) were proposed to reveal the status quo and attributes of Chinese English preservice teachers' digital competence perceptions in relation to cyber ethics, cyber security and cyber safety:

RQ1: What are Chinese English preservice teachers' perceptions of their digital competence?

RQ2: What characterizes the relationship between Chinese English preservice teachers' C3 Matrix

ISSN 2663-8169 Vol. 5, Issue 1: 31-41, DOI: 10.25236/IJNDE.2023.050106

perceptions in the domain of digital competence?

Five hypotheses were composed to elaborate the relationship between English preservice teachers' digital competence perceptions and their views on the C3 Matrix-cyber ethics, cyber security and cyber safety (see Figure 1).

Two hypotheses demonstrate how English preservice teachers' perceptions of cyber ethics affect their views on cyber security and cyber safety:

H1. English preservice teachers' perceptions of cyber ethics predict their views on cyber security.

H2. English preservice teachers' perceptions of cyber ethics predict their views on cyber safety.

Three hypotheses demonstrate how English preservice teachers' perceptions of cyber ethics, cyber security and cyber safety affect their views on digital competence:

H3. English preservice teachers' perceptions of cyber ethics predict their views on digital competence.

H4. English preservice teachers' perceptions of cyber security predict their views on digital competence.

H5. English preservice teachers' perceptions of cyber safety predict their views on digital competence.

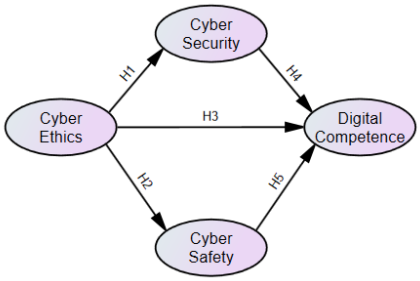

Figure 1: Theoretical model demonstrating research hypotheses and constructs.

3. Methodology

3.1. Participants

221 senior students majoring in English Education anonymously and voluntarily participated in the data collection process. The overall data collection procedure lasted over a month in length and all the participants were aware of the purpose of the study and were assured there will be no potential privacy leakage during or after this research, since personal information like real names, date of birth, place of birth was not characterized as the interest of this study. The whole sample comprised 76.49% females (169 in total) and 23.51% males (52 in total). All participants were in similar age ranging from 21 to 23.

3.2. Instruments

Participants were asked to anonymously answer a 19-item online questionnaire which contains four subscales: cyber ethics, cyber security, cyber safety and digital competence. The detailed statements within each aspect and their statistical attributes were listed in Table 1.

3.2.1. English Preservice Teachers' Digital Competence Scale

Researchers have been squabbling about the best way to evaluate teachers' digital competence, and the one released by the European Commission <Digital Competence of Educators> [9] is widely acknowledged as a standardized reference, as its internal consistency and reliability were repeatedly testified by previous research. [13][14] As Bandura [31] once pointed out, successful former experiences boost individuals' self-efficacy, which further impacts their perceptions on related subjects. Since the original < "DigCompEdu" Check-in> questionnaire was designed for in-service teachers and educators, and the participants in this study were teacher students who differ from in-service teachers regarding working experiences and pedagogical perceptions, the current research adopted five items out of the original questionnaire [14] and tailored them accordingly so that they could be more suitable for the current condition of the respondents. A five-point Likert scale was used to rate respondents' perceptions on the subjects, which took a range from 1 to 5 points: 1= "strongly agree", 2= "agree", 3= "not sure", 4=

ISSN 2663-8169 Vol. 5, Issue 1: 31-41, DOI: 10.25236/IJNDE.2023.050106

"disagree" and 5= "strongly disagree".

3.2.2. English Preservice Teachers' C3 Matrix Scale

14 statements were formed from the literature [19] [32] for the assessment of English preservice teachers' C3 Matrix-related perceptions: five statements were developed to measure English preservice teachers' cyber ethics, five items for cyber security, [24][33] and four statements for the measurement of cyber safety. All these aforementioned statements were equipped with a five-point Likert scale, with each point containing connotation as follows: 1= "strongly agree", 2= "agree", 3= "not sure", 4= "disagree" and 5= "strongly disagree".

Table 1: Means, standard deviations, skewness, kurtosis, and factor loadings

Scale Items	M(SD)	Skewness	Kurtosis	Standardized Factor Loadings (SE)
Cyber Ethics Scale (McDonald's ω=0.82)				
Before I publish any content online, I will consider its possible impact on others.	1.74(0.61)	0.22	-0.58	0.58(0.33) ***
When the content I want to publish involves others, I will ask for their permission first.	2.09(0.82)	0.14	-0.87	0.57(0.32) ***
I know how to evaluate the credibility of online information.	2.60(1.13)	0.24	-0.75	0.54(0.29) ***
I know how to deal with cyber bullying and cyber harassment.	2.45(1.06)	0.47	-0.31	0.63(0.39) ***
I don't quote or download online materials with obscure copyright.	1.87(0.70)	0.43	-0.04	0.67(0.45) ***
Cyber Security Scale (McDonald's ω=0.89)				
I check whether the webpage I browse has a connection security ID (https://) and a web security certificate.	1.90(0.69)	0.55	1.03	0.83(0.69) ***
When downloading or installing software, I will first confirm the security of the website or program I use.	1.99(0.72)	0.53	0.81	0.84(0.71) ***
I don't subscribe websites that I don't trust.	1.79(0.59)	0.35	0.94	0.74(0.55) ***
I install firewalls on my electronic products like computers, tablets, etc.	1.88(0.67)	0.79	2.29	0.80(0.65) ***
I scan for viruses before opening e-mails from unknown sources.	2.27(0.93)	0.38	-0.36	0.73(0.53) ***
Cyber Safety Scale (McDonald's ω=0.79)				
I install virus detection software on my computer.	2.08(0.80)	0.39	0.01	0.82(0.68) ***
I keep my electronic products updated on a regular basis.	2.00(0.85)	1.13	1.73	0.62(0.38) ***
I don't leave my personal information on public computers.	1.78(0.72)	0.65	0.20	0.74(0.54) ***
I set different security passwords for different accounts.	2.01(0.83)	0.47	-0.35	0.61(0.38) ***
Digital Competence Scale (McDonald's ω=0.90)				
Well-developed digital competence can improve the efficiency of everyday life.	1.81(0.64)	0.29	-0.15	0.75(0.57) ***
I am content with my current digital competence level.	1.88(0.69)	0.66	1.39	0.85(0.72) ***
Advanced digital competence may benefit me more when facing career choices.	1.92(0.66)	0.33	0.03	0.79(0.63) ***
I know how to further develop my digital competence.	1.88(0.68)	0.36	0.08	0.85(0.72) ***
I need to enhance my current digital competence level so I can be better prepared for job hunting in the future.	1.88(0.68)	0.76	1.87	0.78(0.61) ***

***p<0.001

ISSN 2663-8169 Vol. 5, Issue 1: 31-41, DOI: 10.25236/IJNDE.2023.050106

3.3. Analytical Procedures

Two major procedures were involved in the data analysis process. First, descriptive attributes such as means, standard deviation and the tendency of univariate normality were depicted using the software SPSS. Then, to answer the research questions and check the potential relationship between the research hypotheses, Structural Equation Modeling (SEM) was employed using the software Amos. SEM has become a widely acknowledged statistical instrument in various domains of social science, since it excels in corroborating the acceptability and fitness of theoretical models which are constructed by observed variables and latent variables. [34] It manifests a series of interrelated procedures rather than just a single calculating step, which suits well for studies with multiple variables. SEM is also excellent in providing numerous parameters of the given data which can be used to evaluate the fitness of the hypothesized models. The model proposed in this study is shown in Figure 1.

A series of common indices like the Goodness of Fit Index (GFI), the Adjusted Goodness of Fit Index (AGFI), the Comparative Fit Index (CFI), the Tucker-Lewis Index (TLI), the Standardized Root Mean Square Residual (SRMR), the Root Mean Square Error of Approximation (RMSEA) and Chi-square value ($\chi 2$) were calculated to check the fitness and the validity of the hypothesized model (see Figure 1).

Although unified rules of thumb do not always work equally due to diverse conditions, [34] common cutoff criteria recommended by mathematicians and statisticians still need to be strictly followed when checking the value of these aforementioned indices. For the Maximum Likelihood (ML) method-based evaluation, the common cutoff values for each index are as follows: the values of CFI and TLI are close to 0.95 or higher, [34] [35] the value of RMSEA is close to 0.06 or lower, [34]and the value of SRMR is close to 0.08 or lower (Hu & Bentler, 1999; Brown, 2015; Kenny, 2020). [34] [36]

4. Results

As previously mentioned, this study used a five-point Likert scale as the sole data evaluation tool, which means the results are highly qualified to undertake a series of quantitative analysis.

4.1. Attributes of Items

Before commencing any further SEM analysis, descriptive statistics like Mean (M), Standard Deviation (SD), skewness and kurtosis are computed respectively. Skewness depicts the distribution trend of the data in comparison to a normal distribution, and kurtosis is used to describe the level of the flatness of the data. [37] Skewness indicates that the shape of a unimodal distribution is asymmetrical comparing to its Mean: A positive skewness shows that most of the values are lower than their Means, and a negative skewness indicates just the opposite. As for the kurtosis, in comparison to a normal curve of a unimodal symmetric distribution: A positive kurtosis implies a heavier tail and a higher peak, and a negative kurtosis connotes the opposite. Only variables whose values of skewness are higher than 3 and kurtosis are over 10 considered to be problematic, other than that the data shall be viewed as univariate normally distribute. [38] As displayed in Table 1, all the items in this study show applaudable values of skewness and kurtosis, with a slight flotation ranging from 0.14 to 1.13, and -0.87 to 1.87, respectively.

4.2. Measurements of the Hypothesized Model

The Chi-square ($\chi 2$) value of the model reached a significant level ($p=0.000$), which is reasonable since the Chi-square test is extremely sensitive to a small sample size (I. K. R. Hatlevik & Hatlevik, 2018), and this study only contains 221 respondents. Nevertheless, other common indices came off as relatively applaudable: GFI=0.898, AGFI=0.861, CFI=0.965, TLI=0.957, RMSEA=0.053 and SRMR=0.0483.

Factor loadings symbolize the correlations between research items and the constructs in the model. The cutoff criterion of a valid factor loading is close to 0.60 or higher. [39] In this study, the factor loadings of all latent variables in the model mostly reached the cutoff criteria (see Table 1), which took a slight range from 0.54 to 0.85, suggesting a legitimate level of convergent validity. McDonald's omega coefficient, instead of Cronbach's alpha coefficient was used to testify the internal consistency between each latent variable and its observed variables, since the former excels in profuse ways compared to the latter. [13][40] [41] The McDonald's omega coefficient of the four latent variables in this study are: 0.82 for cyber ethics, 0.89 for cyber security, 0.79 for cyber safety and 0.90 for digital competence (see Table 1).

ISSN 2663-8169 Vol. 5, Issue 1: 31-41, DOI: 10.25236/IJNDE.2023.050106

The correlation matrix of the constructs is shown in Table 2. All three elements in the C3 Matrix significantly correlate with each other and they all relate potently with digital competence. Overall, all latent variables display positive correlations amongst each other.

Table 2: Correlation matrix for all constructs

Latent Variables	1st	2nd	3rd	4th
1st. Cyber Ethics	-			
2nd. Cyber Security	0.899***	-		
3rd. Cyber Safety	0.774***	0.696	-	
4th. Digital Competence	0.748	0.733**	0.793***	-

**p<0.01, ***p<0.001

The outcomes of the structural equation modeling that fructified the research hypotheses are demonstrated in Figure 2. English preservice teachers' cyber ethics perceptions predict their views on cyber security (H1: β=.90, p <.001) and cyber safety (H2: β=.77, p <.001). Components of the C3 Matrix, namely cyber ethics, cyber security and cyber safety affect respondents' digital competence perceptions in different significant levels and in mixed ways. Cyber security has high positive impact on digital competence (H4: β=.63, p <.01), cyber safety also affects digital competence positively (H5: β=.39, p <.001), but its influence is not as significant as the former. On the contrary, the regression path between cyber ethics and digital competence suggests that cyber ethics itself exerts negative minor effects on participants' digital competence perceptions, but it did not prove to be statistically significant (H3: β=-.11).

Statistical calculation reveals that variables functioned well in explaining the variation in the model. It is 81% for cyber security perceptions, 60% for cyber safety perceptions and 69% for digital competence perceptions.

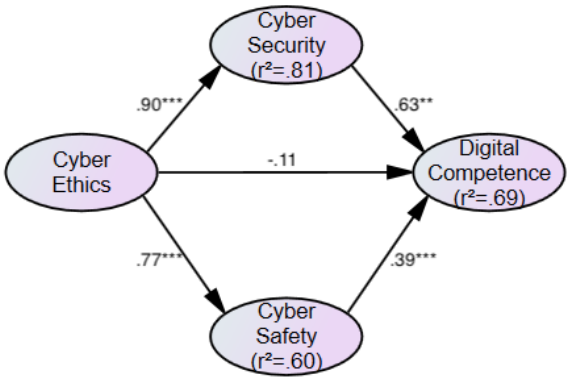

*Figure 2: Standardized estimates for SEM analysis of the model. **p<0.01, ***p<0.001*

5. Discussion

This paper proposed a theoretical model regarding English preservice teachers' digital competence perceptions and testified it with empirical data received from 221 senior students in a normal university in northern China. The model contained four latent variables, namely cyber ethics, cyber security, cyber safety and digital competence. Each of these latent variables was assigned with several observed variables: five items were precisely designed for the measurement of the participants' cyber ethics perceptions, five for cyber security perceptions, five for digital competence perceptions and four for cyber safety perceptions (see Table 1). Five hypotheses were formulated in advance to guide the study and predict the intricate relationship amongst the latent variables. Statistical results corroborated all the hypotheses and variation of the model is well explained (see Figure 2).

To begin with, statistical results of this study confirmed that English preservice teachers' cyber ethics perceptions have great positive impacts on how they perceive cyber security and cyber safety. This finding echoed with previous research that preservice teachers' knowledge of cyber ethics is in synergy with their understandings of cyber security and cyber safety. [29] It was noted that both institutions like teacher training centers and education regulation agencies and professionals like in-service teachers called for the need for further improvement on the C3 Matrix content. [28][29] Preservice teachers' unpreparedness on C3 Matrix content could be devastating considering they are expected to enlighten

ISSN 2663-8169 Vol. 5, Issue 1: 31-41, DOI: 10.25236/IJNDE.2023.050106

the potential cyber-related awareness for students in the future.

In addition to that, constituents of the C3 Matrix exert uneven effects on participants' digital competence perceptions. Both cyber security and cyber safety have positive impact on preservice teachers' digital competence perceptions, with cyber security exerts stronger effects compared to its counterpart. This result is supported by previous finding.[24] It was reported that preservice teachers hold positive attitudes towards cyber security issues in an information and technology immersed environment, [24] [42] which serves as catalyst for their urges for further improvement regarding professional digital competence development.

Apart from these two points aforementioned, how cyber ethics coordinates with digital competence is worth elaborating. Statistical outcomes of structural equation modeling in this study reveals that cyber ethics alone exerts minor negative influence on English preservice teachers' digital competence perceptions. This result is surprisingly unexpected compared to the correlations between the other two elements of the C3 Matrix and the participants' digital competence perceptions. Myriads of reasons could give rise to this outcome. Limited number of research items may be inadequate to reveal participants' holistic perceptions on the related subjects, since there were only five items assigned to each subscale. Another possible explanation lies in the fact that the amount of the empirical data in this study needs to be expanded to some degree, since indices in structural equation modeling are highly sensitive to sample size. There is a scarcity of empirical studies that integrate the C3 Matrix with preservice teachers' digital competence in the domain of teacher education, so the outcomes yielded in this research still needs further verification in the future.

To recapitulate in short, structural equation modeling verified all the hypotheses in this study: cyber ethics positively and significantly correlates with cyber security and cyber safety; the C3 Matrix as a whole exert mixed effects on English preservice teachers' digital competence perceptions, but the relationship between cyber ethics and digital competence needs further corroboration.

6. Conclusions

This study proposed a theoretical model in relation to four variables, namely cyber ethics, cyber security, cyber safety and digital competence, with the former three concepts being jointly referred as C3 Matrix. [16][27] The results of the structural equation modeling revealed that both cyber security and cyber safety have strong positive association with cyber ethics, and they positively coordinate with digital competence. There is an interesting finding regarding the relationship between English preservice teachers' cyber ethics perceptions and their views on digital competence. As statistical calculation revealed, cyber ethics exerts positive impact on digital competence via the agency of cyber security and cyber safety. However, its direct impact on digital competence seemed to be minorly negative, but it didn't reach any level of statistical significance. This appears to be a hot dispute where further verification is needed.

Apart from what have been mentioned above, limitations of this study should be directly pointed out. First, the sole data collection instrument was a 19-item online questionnaire. Although a five-point Likert scale assigned to the questionnaire displayed participants' perceptions to some extent, such quantitative method may not be able to uncover respondents' complete comprehension on related subjects, which means there are still myriads of details need to be unveiled. In addition to that, the sample size of this study is rather small, only 221 valid data was put under analysis. Although standardized estimates like CFI and TLI reached statistical cutoff criteria, the model could have mounted a higher level of solidity given a bigger volume of empirical data. Last of all, the structural equation model only contained 19 items, which means a vast amount of research items were sacrificed in the pursuit of forming a statistically acceptable model. There is a strong possibility that potential explanation of the hidden attributes of English preservice teachers' digital competence perceptions were omitted together with the original items that were tossed away.

Researchers once denoted that such complicated factors as culture, family background and religion preferences affect how an individual perceive the world,[18] this study only investigated preservice teachers' general perceptions pertaining C3 Matrix in the domain of digital competence and did not take individual differences into account. Although empirical data in this study confirmed that participants' digital competence perceptions definitely correlate with their views on the C3 Matrix, it didn't reveal the internal details regarding individual variations. In-depth analysis on how and to what extent these factors are liable on shaping individuals' cyber perceptions is worth conducting in the future.

ISSN 2663-8169 Vol. 5, Issue 1: 31-41, DOI: 10.25236/IJNDE.2023.050106

7. Recommandations

More empirical studies about preservice teachers' digital competence should be carried out in the domain of teacher education. For future reference, further research needs to focus more on the facets listed below. To begin with, as people's perception being a subjective attribute, individual differences like gender, age, working experience, cultural backgrounds, etc. should be taken into consideration when interpreting research outcomes. Furthermore, as certain groups of people can't speak for all, it's of great importance that participants submitting the empirical data match as perfect as possible with the original population that they came from, which further indicates the significance of selecting the right group and the adequate volume of respondents for the study. At last, mixed research methods are recommended, since scales only excel in measuring qualitative features. The upcoming research in relation to the current one should focus more on the collection of qualitative data so as to better apprehend preservice teachers' digital competence perceptions.

Acknowledgements

The author wishes to thank all the participants who voluntarily took part in the data collection process. This research couldn't be completed without their participation.

References

[1] Chinese Ministry of Education. (2018). Action Plan for Educational Informatization 2.0, (6), 1-9.
[2] The State Council of the CPC Central Committee. (2018). Opinions on Comprehensively Deepening the Reform of the Construction of Teachers in the New Era, (4), 3-9.
[3] Wu Junqi., Ren feixing, & Li Meng. (2021). Teachers' Digital Competence: Connotation, Evolution (9), 86-90.
[4] Basilotta-Gómez-Pablos, V., Matarranz, M., Casado-Aranda, L.-A., & Otto, A. (2022). Teachers' digital competencies in higher education: a systematic literature review. International Journal of Educational Technology in Higher Education, (1), 19.
[5] Ferrari, A., Punie, Y., & Redecker, C. (2012). Understanding Digital Competence in the 21st Century: An Analysis of Current Frameworks. Springer-Verlag, (4), 79-92
[6] Ferrari, A., Punie, Y., & Brečko, B. N. (2013). DIGCOMP: A Framework for Developing and Understanding Digital Competence in Europe. European union, (11),48-50
[7] Gordillo, A., Barra, E., López-Pernas, S., & Quemada, J. (2021). Development of Teacher Digital Competence in the Area of E-Safety through Educational Video Games. Sustainability, (15),13.
[8] UNESCO. (2020). Distance learning strategies in response to COVID-19 school closures (2),1-8.
[9] Redecker, C., & Punie, Y. (2017). European Framework for the Digital Competence of Educators<DigCompEdu>, (17),92-95.
[10] European Union. (2018). Proposal for a Council recommendation on key competences for lifelong learning. Official Journal of the European Union, (4),6-10.
[11] China Internet Network Information Center. (2021). The 48th China Statistical Report on Internet Development, (48),76-79.
[12] INTEF. (2017). Common Digital Competence Framework for Teachers, (12),83-87.
[13] Cabero-Almenara, J., Gutierrez-Castillo, J. J., Palacios-Rodriguez, A., & Barroso-Osuna, J. (2020). Development of the Teacher Digital Competence Validation of DigCompEdu Check-In Questionnaire in the University Context of Andalusia (Spain). Sustainability, (15), 12-17.
[14] Cabero-Almenara, J., & Palacios-Rodríguez, A. (2020). Marco Europeo de Competencia Digital Docente «DigCompEdu». Traducción y adaptación del cuestionario «DigCompEdu Check-In». (1), 213-234.
[15] Ghomi, M., & Redecker, C. (2019). Digital Competence of Educators (DigCompEdu): Development and Evaluation of a Self-assessment Instrument for Teachers' Digital Competence. Proceedings of the 11th International Conference on Computer Supported Education, (2), 541-548.
[16] Pruitt-Mentle, D. (2000). C3 Framework Cyberethics, Cybersafety and Cybersecurity. Promoting Responsible Use. Educational Technology Policy, Research and Outreach, (1), 1-6.
[17] Heller, P., B. (2012). Technoethics: The Dilemma of Doing the Right Moral Thing in Technology Applications. International Journal of Technoethics, (1), 14-27.
[18] Mosalanejad, L., Dehghani, A., & Abdolahifard, K. (2014). The Students' Experiences of Ethics in Online Systems: A Phenomenological Study. Turkish Online Journal of Distance Education, (5), 205-212.

ISSN 2663-8169 Vol. 5, Issue 1: 31-41, DOI: 10.25236/IJNDE.2023.050106

[19] Milton, J., Giæver, T. H., Mifsud, L., & Gassó, H. H. (2021). Awareness and knowledge of cyberethics: A comparative study of preservice teachers in Malta, Norway, and Spain. Nordic Journal of Comparative and International Education (NJCIE), (4), 18-37.
[20] Engen, B. K., Giæver, T. H., & Mifsud, L. (2018). Wearable Technologies in the K-12 Classroom: Cross-Disciplinary Possibilities and Privacy Pitfalls. Journal of Interactive Learning Research, (3), 323-341.
[21] Salim, H. M. (2014). Cyber Safety: A Systems Thinking and Systems Theory Approach to Managing Cyber Security Risks, Massachusetts Institute of Technology, (9), 144-156.
[22] Sagiroglu, S., & Sinanc, D. (2013). Big Data: A review. International Conference on Collaboration Technologies and Systems (CTS), San Diego, CA, USA, (11), 2-6.
[23] Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers & Security, (38), 97-102.
[24] Haseski, H. İ. (2020). Cyber Security Skills of Pre-Service Teachers as a Factor in Computer-Assisted Education. International Journal of Research in Education and Science (IJRES), (3), 484-500.
[25] International Telecommunications Union (ITU). (2008). ITU-TX.1205: Series X: Data networks, open system communications and security: Telecommunication security: Overview of Cybersecurity 2008, (12), 7-14.
[26] Third, A., Forrest-Lawrence, P., & Collier, A. (2014). Addressing The Cyber Safety Challenge: from risk to resilience, (7), 24-33
[27] C3 Matrix. (2015). Cyber-safety, cyber-security, cyber-ethics (C3), Digital literacy skills, (5), 3-10.
[28] Pruitt-Mentle, D. (2009). National Cyber ethics, Cyber safety, Cybersecurity Baseline Study. The Education Digest, (3), 1-11.
[29] Pusey, P., & Sadera, W. A. (2011). Cyber ethics, Cyber safety, and Cybersecurity: Preservice Teacher Knowledge, Preparedness, and the Need for Teacher Education to Make a Difference. Journal of Digital Learning in Teacher Education, (2), 1-7.
[30] KADIOĞLU, E. A. (2019). Design, Development and Implementation of An Information Security and Cyber ethics Course for Preservice Teachers: A Designed-based Research, Middle East Technical University, (4), 270-276.
[31] Bandura, A. (2006). Guide for Constructing Self-efficacy Scales, (14), 28-32.
[32] McGarr, O., & McDonagh, A. (2020). Exploring the digital competence of pre-service teachers on entry onto an initial teacher education programme in Ireland. Irish Educational Studies, (1), 115-128.
[33] Erol, O., Şahin, Y. L., Yılmaz, E., & Haseski, H. İ. (2015). Personal Cyber Security Provision Scale Development Study. International Journal of Human Sciences, (2), 31-34.
[34] Hu, L. T., & Bentler, P. M. (1999). Cutoff Criteria for Fit Indexes in Covariance Structure Analysis: Conventional Criteria Versus New Alternatives. Structural Equation Modelling-a Multidisciplinary Journal, (1), 1-55.
[35] Marsh, H. W., Hau, K. T., & Wen, Z. L. (2004). In search of golden rules: Comment on hypothesis-testing approaches to setting cutoff values for fit indexes and dangers in overgeneralizing Hu and Bentler's (1999) findings. Structural Equation Modelling-a Multidisciplinary Journal, (3), 320-341.
[36] Kenny, D. A. (2020). Measuring Model Fit, (5), 4-12.
[37] Hatlevik, O. E. (2016). Examining the Relationship between Teachers' Self-Efficacy, their Digital Competence, Strategies to Evaluate Information, and use of ICT at School. Scandinavian Journal of Educational Research, (5), 555-567.
[38] Lau, W. W. F., & Yuen, A. H. K. (2015). Factorial invariance across gender of a perceived ICT literacy scale. Learning and Individual Differences, (41), 79-85.
[39] Hatlevik, I. K. R., & Hatlevik, O. E. (2018). Examining the Relationship between Teachers' ICT Self-Efficacy for Educational Purposes, Collegial Collaboration, Lack of Facilitation and the Use of ICT in Teaching Practice. Front Psychol, (9), 9-13.
[40] Revelle, W., & Zinbarg, R. E. (2008). Coefficients Alpha, Beta, Omega, and the glb: Comments on Sijtsma. Psychometrika, (1), 145-154.
[41] Y.Peters, G.-J. (2014). The alpha and the omega of scale reliability and validity. The European Health Psychologist, (2), 8-12.
[42] Al-Janabi, S., & Al-Shourbaji, I. (2016). A Study of Cyber Security Awareness in Educational Environment in the Middle East. Journal of Information & Knowledge Management, (1), 22-30.