Id: 1868473

Participatory Educational Research (PER)
Vol.13(3), pp. 199-220, May 2026
Available online at http://www.perjournal.com
ISSN: 2148-6123
http://dx.doi.org/10.17275/per.26.41.13.3

Measuring Cyber Resilience in Middle School Students: Development and Validation of a Scale

Aslıhan İstanbullu*
Department of Computer Technologies, Amasya University, Amasya, Türkiye
ORCID: 0000-0002-1778-859X

Ömer Delialioğlu
Faculty of Education, Computer Education and Instructional Technology, Middle East Technical University, Ankara, Türkiye
ORCID: 0000-0001-6515-3516

Article history

Received:
02.12.2025

Received in revised form:
24.02.2026

Accepted:
04.03.2026

Key words:
cyber resilience, psychometric validation, scale development, digital resilience, middle school students, digital safety.

The increasing integration of digital technologies into students' daily lives has intensified middle school students' exposure to cyber risks, highlighting cyber resilience as a critical competency in contemporary education. This study aims to develop a valid and reliable measurement instrument to assess the cyber resilience capacity of middle school students in the digital age. Grounded in resilience theory and the NIST Cybersecurity Framework, the research introduces the Cyber Resilience Scale (CRS) for students aged 11–14. The scale development process followed systematic methodological procedures. An initial pool of 65 items was generated based on an extensive literature review and the five core functions of the NIST Cybersecurity Framework: Identify, Protect, Detect, Respond, and Recover. Content validity was ensured through expert review, followed by pilot testing to confirm clarity and age appropriateness. Data were collected from 767 middle school students and analyzed using exploratory factor analysis (EFA) to identify the underlying factor structure. Confirmatory factor analysis (CFA) was then conducted to validate the model. The results supported a five-factor structure consistent with the theoretical framework. The final version of the CRS consists of 43 items and explains 59.88% of the total variance. Reliability analyses indicated strong internal consistency, with a Cronbach's alpha coefficient of 0.940 for the overall scale and values ranging from 0.902 to 0.930 for the subscales. Overall, the findings demonstrate that the CRS can support educational practices aimed at strengthening students' ability to manage digital risks.

Introduction

Middle school students (ages 11–14) constitute a significant proportion of global internet users and face escalating cyber threats, including cyberbullying, identity theft, and online fraud (OECD, 2024). Despite widespread digital engagement, research indicates that many students lack cybersecurity awareness and adaptive capacity to safely navigate online environments (European Commission, 2022). This vulnerability underscores the insufficiency of technical safeguards alone and highlights the need for valid and developmentally appropriate measurement instruments to assess individual-level cyber resilience—the capacity

to anticipate, withstand, recover from, and adapt to adverse digital experiences (Masten, 2014; NIST, 2018).

From a measurement perspective, existing approaches to assessing cyber-related capacities in children present three critical psychometric limitations. First, general psychological resilience scales (Connor & Davidson, 2003) lack domain specificity for cyber contexts, failing to capture unique digital stressors such as anonymity, content permanence, and rapid threat evolution. Second, cybersecurity awareness instruments primarily assess declarative knowledge rather than adaptive capacity under stress—measuring what students know rather than whether they can enact protective behaviours during uncertainty or distress (Arpaci & Ateş, 2023). Third, digital citizenship scales emphasize normative online behaviours but provide insufficient evidence of construct validity, factorial structure, or developmental appropriateness for early adolescents (Tutar, Erdem & Şahin, 2023). These psychometric insufficiencies—not merely content gaps—necessitate the development of a validated, theory-driven cyber resilience instrument specifically designed for middle school populations.

Middle school students represent a critical population for cyber resilience measurement for three developmental reasons with direct implications for scale construction. First, cognitive transitions from concrete to formal operational thinking (Piaget, 1972) enable comprehension of abstract cyber concepts (e.g., privacy, digital consequences), while ongoing executive function immaturity creates measurement complexity—students may understand risks conceptually yet fail to regulate behaviour under stress. Second, this developmental stage marks the peak onset of autonomous digital device use with decreasing parental supervision, necessitating self-report instruments validated specifically for this age group. Third, identity formation intensifies during early adolescence (Erikson, 1968), increasing susceptibility to social engineering and reputation-based threats—dimensions that require resilience-oriented rather than knowledge-oriented assessment. Collectively, these characteristics necessitate age-appropriate item wording, response format validation, and construct operationalization distinct from measures developed for adults or younger children.

This study integrates two complementary theoretical frameworks to conceptualize and measure cyber resilience in middle school students. The NIST Cybersecurity Framework (NIST, 2018, 2024), originally developed for organizational risk management, provides a structured model through five core functions: Identify (awareness of assets and threats), Protect (implementation of safeguards), Detect (recognition of incidents), Respond (management strategies), and Recover (restoration processes). When combined with Masten's (2014) developmental resilience theory—which conceptualizes resilience as adaptive capacity involving protective factors, risk regulation, and positive developmental outcomes—these frameworks enable the operationalization of cyber resilience as a multidimensional psychological construct encompassing cognitive awareness, behavioral regulation, and adaptive coping in digitally mediated environments.

Despite recent efforts to characterize cybersecurity competencies for children through skills frameworks (Plintz & Ifenthaler, 2025), such taxonomies describe what children should know rather than provide psychometrically validated instruments for assessing adaptive capacity under stress. Existing measurement approaches fall into three broad categories, each with distinct limitations. First, general psychological resilience measures assess broad adaptive functioning but lack specificity for cyber contexts. Second, cybersecurity awareness and attitude instruments (Arpaci & Ateş, 2023; Bognár & Bottyán, 2024) focus on declarative knowledge or protective tendencies but do not evaluate whether students can enact adaptive

responses during actual cyber incidents. Third, digital citizenship scales (Tutar, Erdem & Şahin, 2023) emphasize normative online behaviours while offering limited developmental and factorial validation for early adolescents. Critically, none of these instruments operationalize cyber resilience as a theoretically integrated, multidimensional construct or demonstrate comprehensive validity evidence for middle school populations.
Therefore, the primary aim of this study is to develop and validate a Cyber Resilience Scale (CRS) for middle school students. This scale is intended to serve as a measurement tool for researchers and practitioners to assess students' cyber resilience capacities across cognitive, behavioral, and adaptive dimensions.

From a measurement science perspective, this study contributes to scale development methodology in three ways. First, it operationalizes cyber resilience—a construct previously conceptualized primarily at organizational and system levels—for individual-level psychological assessment in children, requiring developmental adaptation of both theoretical constructs and psychometric approaches. Second, it demonstrates how organizational cybersecurity frameworks, specifically the NIST Cybersecurity Framework, can be psychometrically validated for personal capacity assessment through rigorous factor analytic procedures, thereby establishing a methodological bridge between organizational and individual measurement paradigms. Third, it provides comprehensive validity evidence through sequential exploratory and confirmatory factor analysis, examines item discrimination properties, reports interfactor correlations for discriminant validity assessment, and establishes internal consistency reliability—addressing methodological standards for instruments in emerging, technology-mediated measurement domains.

The following research questions guide the study:

RQ1: What is the underlying factor structure of cyber resilience among middle school students, and to what extent does the Cyber Resilience Scale demonstrate adequate construct validity?

RQ2: To what extent does the Cyber Resilience Scale demonstrate adequate reliability for measuring cyber resilience among middle school students?

By providing a psychometrically validated instrument, this study contributes to measurement science in the domain of technology-mediated psychological assessment and establishes a foundation for empirical investigation of cyber resilience development in early adolescent populations.

Literature review

Cyber Resilience

The concept of cyber resilience first emerged in the 2000s, during a period when cybersecurity research predominantly focused on risks and threats posed by digital systems (Tzavara & Vassiliadis, 2024). It was introduced as a response to the inadequacy of traditional cybersecurity measures in addressing evolving cyber threats and the growing need for organizations to maintain operations during and after cyberattacks (Bıçakcı & Gücüyener Evren, 2025; Tzavara & Vassiliadis, 2024). The term was officially discussed by the UK Cabinet Office in 2005, and from the 2010s onward, comprehensive frameworks were

developed for organizational and system-level applications. More recently, the concept has begun to be applied at the individual level.

Although various definitions of cyber resilience exist in the literature, most conceptualize it as the capacity to anticipate, withstand, recover from, and adapt to cyber threats (NIST, 2018; Tzavara & Vassiliadis, 2024). The existence of 19 different organizational and academic definitions underscores the multidimensional and context-dependent nature of the construct (Tzavara & Vassiliadis, 2024). For the purposes of this study, considering the developmental characteristics of middle school students, cyber resilience is operationalized as an individual's capacity to recognize cyber threats, prepare proactively, respond appropriately when attacked, and engage in recovery processes thereafter. This definition encompasses not only technical knowledge and skills but also cognitive awareness, emotional regulation, and psychosocial coping mechanisms—dimensions essential for age-appropriate measurement.

Following the COVID-19 pandemic, the concept of cyber resilience has become increasingly important for both organizations and individuals. A review of the literature reveals limited research focused on defining and measuring cyber resilience at the individual level. Existing tools and approaches are primarily developed for institutional contexts and often fail to address critical dimensions such as individuals' psychosocial resilience, cognitive awareness, and emotional coping skills (Stergiopoulos et al., 2023). This gap is particularly concerning given the vulnerability of children and adolescents in digital environments, underscoring the need for valid and reliable tools to assess their cyber resilience.

Theoretical Framework

Resilience Theory

Resilience theory, rooted in developmental psychopathology, defines resilience as positive adaptation despite adversity (Masten, 2014). According to Masten, resilience is not an extraordinary trait, but a process grounded in ordinary human adaptive capacities—what she terms "ordinary magic." This perspective emphasizes that even under adverse circumstances, individuals can demonstrate healthy development through the influence of protective factors (e.g., supportive relationships, individual characteristics) and the regulation of risk factors within their social, cultural, and ecological systems. Masten's model identifies three fundamental processes that determine adaptive capacity: the presence of protective factors, effective risk regulation, and the achievement of positive developmental outcomes.

The application of resilience theory to cyber contexts enables conceptual understanding of how individuals, particularly children and adolescents, develop coping and recovery capacities in digital environments. Initially conceptualized at institutional and technological system levels, cyber resilience has gradually expanded to encompass individual psychosocial and cognitive adaptation processes. For middle school students undergoing rapid emotional and cognitive development, resilience theory provides a lens for interpreting adaptive mechanisms in response to digital stressors. In this study, Masten's resilience framework informs the conceptualization of cyber resilience as involving the interaction of protective factors (e.g., awareness, self-regulation), risk exposure (e.g., cyberbullying, phishing), and adaptive outcomes (e.g., recovery, learning) within digitally mediated environments, while the NIST Cybersecurity Framework provides the structural basis for measurement operationalization. Within this framework, resilience is conceptualized not as a static trait but as an adaptive process shaped by protective resources, risk exposure, and recovery

mechanisms—principles that directly inform the operationalization of cyber resilience dimensions in the present study (Masten, 2014).

The National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)

NIST CSF, developed by the U.S. National Institute of Standards and Technology, is designed to support organizations in identifying, assessing, and managing cybersecurity risks by aligning organizational processes, workforce capabilities, and technological resources (NIST, 2018; 2024). Originally designed to ensure information system security at institutional and national levels, the framework's core functions offer a theoretically coherent structure that can be adapted to assess individual-level digital security and resilience competencies in educational contexts.

The NIST CSF comprises five sequential yet interconnected core functions. The *Identify* function emphasizes the importance of developing an informed awareness of cybersecurity-related risks associated with digital systems, data, and organizational resources. In educational contexts, this function can be interpreted as students' understanding of digital environments, recognition of common cyber threats, and familiarity with basic security practices.

The *Protect* function focuses on practices aimed at reducing the likelihood of cybersecurity incidents by promoting protective behaviors. For students, this involves adopting preventive habits such as creating strong passwords, managing privacy settings responsibly, and exercising caution when navigating online platforms.

The *Respond* function refers to taking appropriate actions following the identification of a cybersecurity incident. In student-centered settings, this may involve implementing basic response actions, including securing compromised accounts, blocking harmful users, or seeking assistance from trusted adults or institutions.

Finally, the *Recover* function addresses the restoration of digital functioning and the strengthening of resilience after adverse events. Within educational environments, this can be understood as students' ability to regain access to digital accounts, restore disrupted services, and cognitively and emotionally cope with negative online experiences.

When adapted to be developmentally appropriate for middle school students, the NIST framework functions as a structural model that operationalizes cyber resilience across preparatory (Identify, Protect), reactive (Detect, Respond), and restorative (Recover) phases. This adaptation enables measurement of cyber resilience as a multidimensional individual capacity encompassing cognitive awareness, behavioral regulation, threat recognition, adaptive response, and psychological recovery—rather than solely as organizational infrastructure or technical proficiency.

Cyber Resilience for Middle School Students

Nowadays, children acquire a digital identity from the moment they are born and grow up deeply embedded in digital environments throughout their developmental stages. This generation is referred to as "digital natives," a term coined by Marc Prensky, highlighting their immersion in online and offline worlds (Setiawati & Sunra, 2024). Before the age of nine, many children already use smartphones, tablets, or computers, engaging in a range of digital activities from an early age (Pew Research Center, 2020). Although adolescents in

middle school are highly active in online environments, their capacity to cope with the threats they encounter is not yet fully developed.

The digital transformation has expanded the environments in which adolescents interact, giving rise to new areas of digital risk that may threaten their development (Setiawati & Sunra, 2024). Middle school students, who are in the early stages of adolescence, actively use the internet despite not yet having fully developed the capacity to cope with threats encountered online. This age group is particularly vulnerable to digital risks due to the fragility associated with the transition from childhood to adolescence (Pan et al., 2024). Therefore, enabling children to develop competencies that support personal safety and responsible engagement in digital environments should be regarded not as a matter of choice, but as a fundamental developmental requirement (Kurt et al., 2025).

From a developmental perspective, middle school students (ages 11–14) are transitioning from concrete operational to formal operational thinking, enabling them to begin understanding abstract concepts such as online privacy and digital consequences (Piaget, 1972). However, their prefrontal cortex—responsible for risk assessment and impulse control—is still developing, making them particularly vulnerable to risky online behaviors despite increasing cognitive sophistication. This developmental paradox—growing digital autonomy coupled with immature risk assessment—positions middle school as a critical window for cyber resilience education and assessment. Moreover, this developmental stage coincides with heightened social-emotional vulnerability. Middle school students are actively constructing their identities and are particularly susceptible to peer influence and social comparison, processes that are intensified in digital environments (Erikson, 1968). The permanence of digital content, the potential for anonymous harassment, and the blurring of public-private boundaries create unique stressors that intersect with normal adolescent development, underscoring the need for resilience-building interventions specifically tailored to this age group.

Current Study

An examination of the scales developed over the past five years reveals that various measurement tools have been introduced in the fields of cybersecurity and digital citizenship. However, the number of valid and reliable instruments specifically designed to assess the multidimensional cyber resilience skills of children in alignment with their developmental level remains limited. Some of these studies are presented in Table 1 (see Appendix).

In addition to psychometric scales, recent frameworks have contributed to identifying cybersecurity competencies for children. For instance, Plintz and Ifenthaler (2025) developed a comprehensive skills framework for children aged 8-13 through systematic literature review and Delphi validation, mapping technical and behavioral competencies onto NIST framework dimensions across six domains (malicious code, frauds, preventive technologies, abusive content, safety, and data privacy). While their matrix-based framework provides valuable guidance for curriculum development by cataloging what children should know and be able to do, it does not constitute a psychometrically validated measurement instrument. As Plintz and Ifenthaler (2025) themselves acknowledge, "many of the skills mentioned in the literature are rather general... this generalization and the resulting superficiality make it more difficult to effectively address specific problems" (p. 15). This highlights the distinction between skills taxonomies, which describe competencies, and validated scales, which measure the extent to which individuals possess those competencies.

According to Table 1, for instance, the scale developed by Kovancı et al. (2021) focuses on measuring middle school students' perceptions of moral values in digital environments, incorporating ethical dimensions such as fairness, compassion, and privacy. Similarly, the scale developed by Arpaci & Sevinç (2021) evaluates individuals' attitudes toward cybersecurity practices across six factors (e.g., privacy, control/ownership, integrity). While these scales assess the technical aspects of cybersecurity, they do not address emotional or behavioral resilience skills.

The Cybersecurity Scale developed by Arpaci & Ateş (2023) assesses individuals' awareness and attitudes toward cybersecurity practices across six factors. However, this scale also focuses primarily on concepts such as security awareness and tendencies toward technical protection, while excluding areas such as psychological resilience and strategies for seeking social support in response to digital threats.

The "Human CRS" developed by Joinson et al. (2023) aims to measure individuals' capacity to cope with cyber threats by incorporating psychological components such as self-efficacy, social support, and learning. However, this scale was designed for adults and has not been adapted to meet the developmental needs of middle school students.

The scale developed in the study by Tutar, Erdem and Şahin (2023) aims to measure the level of digital citizenship by evaluating behavioral tendencies across various domains, including technology use and education. However, this scale also does not focus on individuals' emotional and social coping mechanisms during digital crises.

The Digital Fluency Scale developed by Altunkaynak and Çağımlar (2023) aims to assess teachers' competencies in using digital technologies, focusing on technical and cognitive proficiencies. However, this scale does not measure psychological resilience against emotional or social threats that children may encounter in online environments.
The Personal Cybersecurity Awareness Scale developed by Bognár & Bottyán (2024) examines university students' cybersecurity behaviors across five factors, incorporating important themes such as proactive behaviors and financial security awareness. However, it does not include psychosocial resilience skills that are appropriate to the developmental characteristics of middle school students.

Most of the digital citizenship, digital fluency, and cybersecurity scales developed in the current literature are grounded in specific theoretical frameworks. For example, the study by Altunkaynak & Çağımlar (2023) is based on the theory of digital fluency and the technological development perspective of Web 1.0-2.0-3.0, while Joinson et al. (2023) developed their Human CRS within the framework of psychological resilience theory. Although Arpaci & Ateş (2023) structured their cybersecurity scale according to NIST cybersecurity principles, the scale focuses solely on individuals' technical knowledge, awareness, and behavioral tendencies.

Existing scales generally focus on technical proficiency, digital skills, or behavioral dimensions; however, there remains a need for a developmentally appropriate measurement tool that holistically evaluates children's psychological, social, and emotional responses to adverse experiences in online environments. Furthermore, some scales lack clearly articulated theoretical foundations and appear to have been shaped solely based on literature reviews or findings from factor analyses.

The CRS developed in this study was designed to evaluate individuals' multidimensional responses to digital threats, including psychological resilience, seeking social support, and post-crisis recovery. The scale is grounded in two theoretical frameworks: the internationally recognized NIST framework and Masten's Developmental Resilience Theory (2001), which explains individual resilience. This framework enables the assessment of not only protective behaviors against digital risks but also children's coping skills from a developmental perspective. Developed specifically to measure cyber resilience skills appropriate to children's developmental stages, this study addresses a significant gap in the literature and offers an original and comprehensive contribution to the field.

Methodology

Study Group

The study sample consisted of students attending public middle schools located in five different districts of Ankara. To reflect a range of socioeconomic backgrounds, schools were chosen using a convenience-based approach from both urban and suburban settings. The participants were between 10 and 15 years of age, with a mean age of 12.8 years (SD = 1.2). Detailed demographic information regarding the sample is provided in Table 2.

Ethical approval for the study was granted by the Ethics Committee of xxx University. Prior to data collection, informed consent procedures were completed with both the students and their parents or legal guardians. Participation was based on voluntariness, and students were clearly informed of their right to discontinue participation at any stage of the study without any negative consequences.

Table 2. Demographic characteristics of the study group

Variable	Category	n	%
Gender	Male	344	44,9
	Female	423	55,1
Grade Level	5th Grade	10	1,3
	6th Grade	299	39,0
	7th Grade	236	30,7
	8th Grade	222	28,9
Daily Internet Use	0-1 hours	117	15,3
	1-3 hours	346	45,1
	3-5 hours	171	22,3
	5+ hours	109	14,2
Exposure to Cyberattacks	Others	24	3,1
	Yes	46	6,0
	No	640	83,4
	Not Sure	81	10,6
Cyberattack in Family or Social Circle	Yes	78	10,2
	No	499	65,1
	Not Sure	190	24,8
Perceived Cybersecurity Knowledge and Skills	Yes	410	53,5
	No	187	24,4
	Not Sure	170	22,2

Of the participants, 44.9% were male (n=344) and 55.1% were female (n=423). The distribution by grade level was as follows: 39.0% in Grade 6, 30.7% in Grade 7, 28.9% in Grade 8, and 1.3% in Grade 5. Regarding daily internet usage, 45.1% of participants reported using the internet for 1-3 hours per day, 22.3% for 3-5 hours, 15.3% for 0-1 hour, 14.2% for

more than 5 hours, and 3.1% fell into the "other" category.

When asked about prior exposure to cyberattacks, 6.0% of participants indicated they had personally experienced a cyberattack, 83.4% answered no, and 10.6% were unsure. Similarly, 10.2% reported that someone in their family or social circle had experienced a cyberattack, 65.1% indicated no such experience, and 24.8% were unsure. Regarding perceived cybersecurity knowledge and skills, 53.5% of participants believed they possessed sufficient knowledge and skills, 24.4% felt they did not, and 22.2% were uncertain.

Of the 865 students who initially participated, 98 cases (11.3%) were excluded due to incomplete responses (>10% missing data per case) or outlier values identified through Mahalanobis distance ($p < .001$), resulting in a final analytic sample of N = 767. Detailed data screening procedures are described in Section 3.3.

Scale development process

The development of the Cyber Resilience Scale (CRS) followed the systematic scale development procedures outlined by Erkuş (2019). To generate an initial item pool, a comprehensive literature review was conducted, examining theoretical frameworks and prior research related to cybersecurity, cyber resilience, and digital competence. Based on this review, the theoretical foundation and dimensions of the scale were established, drawing primarily on the NIST CSF and Resilience Theory (Masten, 2001; 2014). An initial item pool of 65 items was developed aligned with these theoretical frameworks.

Lawshe (1975) and McKenzie et al. (1999) recommend obtaining input from at least five experts to establish content validity during scale development. Following this guidance, eight experts reviewed the items for content validity and clarity. The expert panel consisted of three faculty members specializing in Computer Education and Instructional Technology, one measurement and evaluation specialist, one language expert, and three classroom teachers. Based on the experts' evaluations, several necessary revisions were made: unclear or inappropriate items were removed, recommended items were added, and certain items were revised for clarity and developmental appropriateness.

Following the expert review process, a pilot form of the scale was prepared consisting of 65 items using a 5-point Likert-type response format (1 = "Strongly Disagree", 2 = "Disagree", 3 = "Neutral", 4 = "Agree", 5 = "Strongly Agree").

Data Analysis

The pilot form containing 65 items was administered to 865 middle school students during the Fall 2024 semester through paper-and-pencil administration in classroom settings. Students completed the scale under teacher supervision, with an average completion time of approximately 15-20 minutes. Following data collection, missing data and outlier analyses were conducted. Cases with more than 10% missing data were excluded. Outliers were identified using Mahalanobis distance ($p<.001$) and visual inspection of box plots. Following the examination of box plots, 98 cases were excluded from the dataset, yielding a final sample size of 767 participants. Statistical analyses were carried out using SPSS and LISREL software.

Prior to conducting factor analysis, the adequacy of the dataset was evaluated through the Kaiser–Meyer–Olkin (KMO) measure and Bartlett’s test of sphericity. The results indicated a

KMO value exceeding .80, along with a statistically significant Bartlett's test ($p < .001$), demonstrating that the dataset was appropriate for factor analytic procedures (Field, 2024).

Exploratory Factor Analysis (EFA) was then conducted to explore the latent factor structure of the scale and to examine the relationships among items. Factor extraction was performed using principal component analysis, and an oblique rotation method (Promax) was applied to facilitate clearer interpretation of factor loadings, given the expected correlations among factors. Oblique rotation is recommended when correlations among factors are theoretically justified, as is the case with the interrelated dimensions of cyber resilience (Tabachnick, Fidell, & Ullman, 2018).

During the EFA process, items were evaluated based on factor loadings greater than .30, and the number of factors to retain was determined using multiple criteria: (1) eigenvalue >1 (Kaiser criterion), (2) scree plot inspection (Cattell, 1966), (3) percentage of total variance explained (>50%), and (4) theoretical interpretability and alignment with the NIST framework dimensions (Everitt & Vehkalahti, 2019). Items with factor loadings below .30 or cross-loadings on multiple factors were removed iteratively, and the EFA was repeated until a clear and theoretically interpretable factor structure emerged.

After completing the exploratory phase, Confirmatory Factor Analysis (CFA) was applied to examine the extent to which the proposed factor structure aligned with the theoretical framework. A first-order CFA was implemented in LISREL using the maximum likelihood estimation method. The five-factor structure derived from the NIST framework—Identify, Protect, Detect, Respond, and Recover—was specified with inter-factor correlations freely estimated. No error covariances were imposed prior to model testing.

Model adequacy was assessed through a set of complementary fit indices, including the chi-square to degrees of freedom ratio (χ^2/df), Root Mean Square Error of Approximation (RMSEA), Standardized Root Mean Square Residual (SRMR), Comparative Fit Index (CFI), Tucker–Lewis Index (TLI), and Goodness of Fit Index (GFI). Interpretation of these indices was based on commonly accepted threshold values reported in the literature (Schermelleh-Engel et al., 2003).

To support the validity of the scale, item discrimination analysis was conducted. Following the method recommended by Gravetter and Wallnau (2019), participants were divided into upper and lower groups based on total scale scores, with each group representing 27% of the sample. Independent samples t-tests were used to compare mean item scores between the upper and lower groups. Statistically significant differences ($p<.001$) between groups indicate that items possess adequate discriminative power.

Scale reliability was examined by evaluating internal consistency estimates (Table 3). Cronbach's alpha values were computed for both the overall scale and its subdimensions. In line with commonly accepted guidelines, alpha values of .70 and above were interpreted as reflecting satisfactory levels of internal consistency (Tabachnick et al., 2018).

Table 3. Factor loadings of the scale items

Item No	Factor 1 (Identify)	Item No	Factor 2 (Protect)	Item No	Factor 3 (Detect)	Item No	Factor 4 (Respond)	Item No	Factor 5 (Recover)
I1	.703	P15	.712	D27	.691	R32	.685	RC39	.658
I2	.692	P16	.705	D28	.682	R33	.678	RC40	.649
I3	.688	P17	.698	D29	.675	R34	.670	RC41	.638
I4	.677	P18	.691	D30	.664	R35	.661	RC42	.624
I5	.670	P19	.685	D31	.653	R36	.652	RC43	.612
I6	.660	P20	.679			R37	.641	RC44	.601
I7	.652	P21	.671			R38	.625		
I8	.645	P22	.660						
I9	.637	P23	.649						
I10	.630	P24	.637						
I11	.620	P25	.624						
I12	.613	P26	.609						
I13	.607								
I14	.601								
Eigenvalue	11.47		3.21		2.12		1.74		1.02
Variance (%)	26.07		10.89		9.13		12.92		6.44
Total Variance (%)	= 65.45								

Results

Findings regarding the validity of the scale

Validity and reliability analyses of the Cyber Resilience Scale were conducted through EFA and CFA, item discrimination analyses, and internal consistency coefficients. The findings from these analyses are presented below.

Construct validity

Exploratory Factor Analysis (EFA) was conducted to determine the construct validity of the developed scale. Prior to EFA, the Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy and Bartlett's test of sphericity were performed to assess the suitability of the data for factor analysis. The KMO value was calculated as .943, indicating that the sample size was at an "excellent" level for factor analysis (Field, 2024; Worthington & Whittaker, 2006). Bartlett's test of sphericity yielded a significant result ($\chi^2(946) = 11636.563$, $p < .001$), indicating that correlations among variables were sufficient to warrant factor analysis (Kalaycı, 2010).

During the EFA process, the 43 items of the cyber resilience scale were analyzed using the principal component analysis method. The eigenvalue >1 criterion was used to determine the number of factors, and only factors with eigenvalues above 1 were interpreted (Çokluk, Şekercioğlu, & Büyüköztürk, 2014). Additionally, if an item demonstrated high factor loadings on multiple factors with differences less than .10, it was removed from the analysis, as such items may compromise the measurement structure (DeVellis, 2014). Accordingly, Promax rotation (oblique rotation), which allows for correlations among factors, was

employed. To visually support the determination of the number of factors, a scree plot is presented in Figure 1.

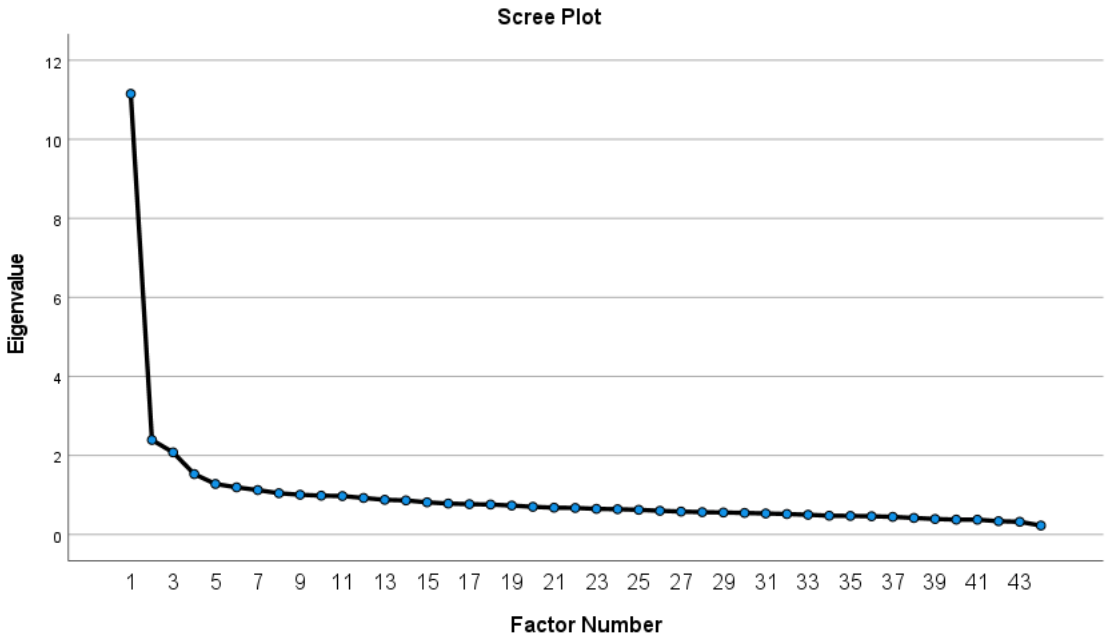

Figure 1. Scree plot

As shown in Figure 1, the eigenvalues demonstrate a significant break after the fifth factor, with the curve leveling off and dropping below one. This indicates a five-factor structure for the scale, according to Cattell's scree test approach (Cattell, 1966). Although there were six factors with eigenvalues above 1, the five-factor model was preferred based on theoretical consistency and interpretability of the factor structure.

Eigenvalues, explained variance, and cumulative variance values were reported in the factor analysis results. According to the findings obtained after Promax rotation, the total explained variance of the 43-item scale was determined to be 59.88%. This rate, obtained from the rotated factor solution, is considered adequate for multidimensional scales in the social sciences (Büyüköztürk, 2002; Tabachnick & Fidell, 2018). Detailed information regarding eigenvalues and variance distribution is presented in Table 4.

Table 4. Eigenvalues and explained variance

Factor	Eigenvalue	EV (%)	CV (%)	ER	EVR (%)	CVR (%)
1	11.47	26.07	26.07	5.31	13.20	13.20
2	3.21	10.89	36.96	4.82	11.56	24.76
3	2.12	9.13	46.09	4.67	10.23	34.99
4	1.74	12.92	59.01	4.51	13.74	48.73
5	1.02	6.44	65.45	3.87	11.15	59.88

Note. EV = Explained Variance; ER = Eigenvalue Rotated; CV = Cumulative Variance; EVR = Explained Variance Rotated; CVR = Cumulative Variance Rotated

According to the results, Factor 1 (Identify) contains items I1-I14, with factor loadings ranging from .601 to .703. This factor reflects cyber awareness and threat recognition behaviors. The factor's eigenvalue was calculated as 11.47, accounting for 26.07% of the total variance.

Factor 2 (Protect) consists of items P15-P26, with factor loadings ranging from .609 to .712. This factor encompasses individuals' protection and prevention behaviors in digital environments. The factor's eigenvalue is 3.21, and its explained variance ratio is 10.89%.

Factor 3 (Detect) consists of items D27-D31, with factor loadings ranging from .653 to .691. This dimension is related to skills in detecting and recognizing digital threats. Its eigenvalue is 2.12, and its variance explanation ratio is 9.13%.

Factor 4 (Respond) includes items R32-R38, with factor loadings ranging from .625 to .685. This factor reflects individuals' strategies for responding to digital threats. The factor's eigenvalue is 1.74, and its explained variance ratio is 12.92%.

Factor 5 (Recover) consists of items R39-R43, with factor loadings ranging from .601 to .658. This dimension encompasses recovery and sustainability behaviors following digital threats. The factor's eigenvalue is 1.02, and its explained variance ratio is 6.44%.
The total variance explanation ratio was found to be 59.88%. A value greater than 40% is considered sufficient in the literature (Büyüköztürk et al., 2019). Table 5 displays sample items and factor titles for the scale.

Table 5. Distribution of items by factors and sample items

Factor	Item Numbers	Sample Item
Identify	I1–I14	"I can recognize when I encounter a fake website."
Protect	P15–P26	"I keep an up-to-date antivirus program on my devices."
Detect	D27–D31	"I can notice when I face a risky situation online."
Respond	R32–R38	"I respond appropriately in cases of cyberbullying."
Recover	RC39–RC44	"After experiencing a digital problem, I can return to a secure digital state."

As shown in Table 5, items grouped under the first factor focus on statements such as identifying personal information, being aware of digital assets, and recognizing online threats; this factor was named "Identify" and consists of 14 items. The second factor includes online protection behaviors such as password security, software updates, and data backup, and was therefore named "Protect," containing 12 items. Items under the third factor focus on skills such as recognizing online threats, distinguishing suspicious content, and detecting threats in digital environments; this factor was named "Detect" and consists of 5 items. The fourth factor encompasses behaviors such as responding quickly and appropriately to digital problems and seeking solutions in cases of digital violence or bullying. Accordingly, this factor was named "Respond" and consists of 7 items. The fifth and final factor includes processes such as returning to safe digital environments after digital problems, emotional recovery, seeking support, and learning; this factor was named "Recover" and consists of 5 items.

No significant differences were observed between the initially predicted factor-item distribution and the distribution obtained after factor analysis. In other words, the item distributions made before the analysis aligned with those obtained after factor analysis, demonstrating strong theoretical consistency with the NIST Cybersecurity Framework dimensions.

Confirmatory Factor Analysis

Based on the exploratory factor analysis, the CRS was determined to consist of five factors and a total of 43 items. To evaluate whether this empirically derived structure was consistent

with the proposed theoretical model, CFA was subsequently applied (DeVellis, 2014).

A first-order CFA was implemented using LISREL with maximum likelihood estimation. The model specification was based on a five-factor structure aligned with the core dimensions of the NIST framework—Identify, Protect, Detect, Respond, and Recover—with correlations permitted among latent factors. The findings obtained from the confirmatory analysis, together with the corresponding fit indices and their acceptable threshold values reported in the literature, are presented in Table 6.

Table 6. Confirmatory factor analysis fit indices

Index	**Model Value**	**Acceptable Threshold**	**Interpretation**
CMIN/DF	2.367	< 3.00	Good fit
GFI	.88	≥ .90 (ideal), ≥ .85 (acceptable)	Acceptable fit
AGFI	.86	≥ .90 (ideal), ≥ .85 (acceptable)	Acceptable fit
NFI	.95	≥ .90	Excellent fit
IFI	.97	≥ .90	Excellent fit
CFI	.97	≥ .90	Excellent fit
RMSEA	.045	≤ .08 (acceptable), ≤ .05 (good)	Good fit
SRMR	.050	≤ .08	Good fit

As shown in Table 6, the chi-square fit index (CMIN/DF), which evaluates the fit of the data to the model, was found to be 2.367, indicating "good fit." The goodness of fit index (GFI), which is less sensitive to sample size, was observed as .88, and its adjusted version (AGFI) was calculated as .86; both values indicate "acceptable fit."
The normed fit index (NFI), which evaluates the model's accuracy independently of sampling error, was .95; the comparative fit index (CFI) and incremental fit index (IFI) were both .97, all indicating "excellent fit."

The standardized root mean square residual (SRMR) value was .050, and the root mean square error of approximation (RMSEA) value was .045, both indicating "good fit." All fit indices met or exceeded the recommended cutoff criteria proposed by Schermelleh-Engel et al. (2003). Figure 2 presents the model derived from the analysis, depicting the relationships between the latent constructs and their respective items.

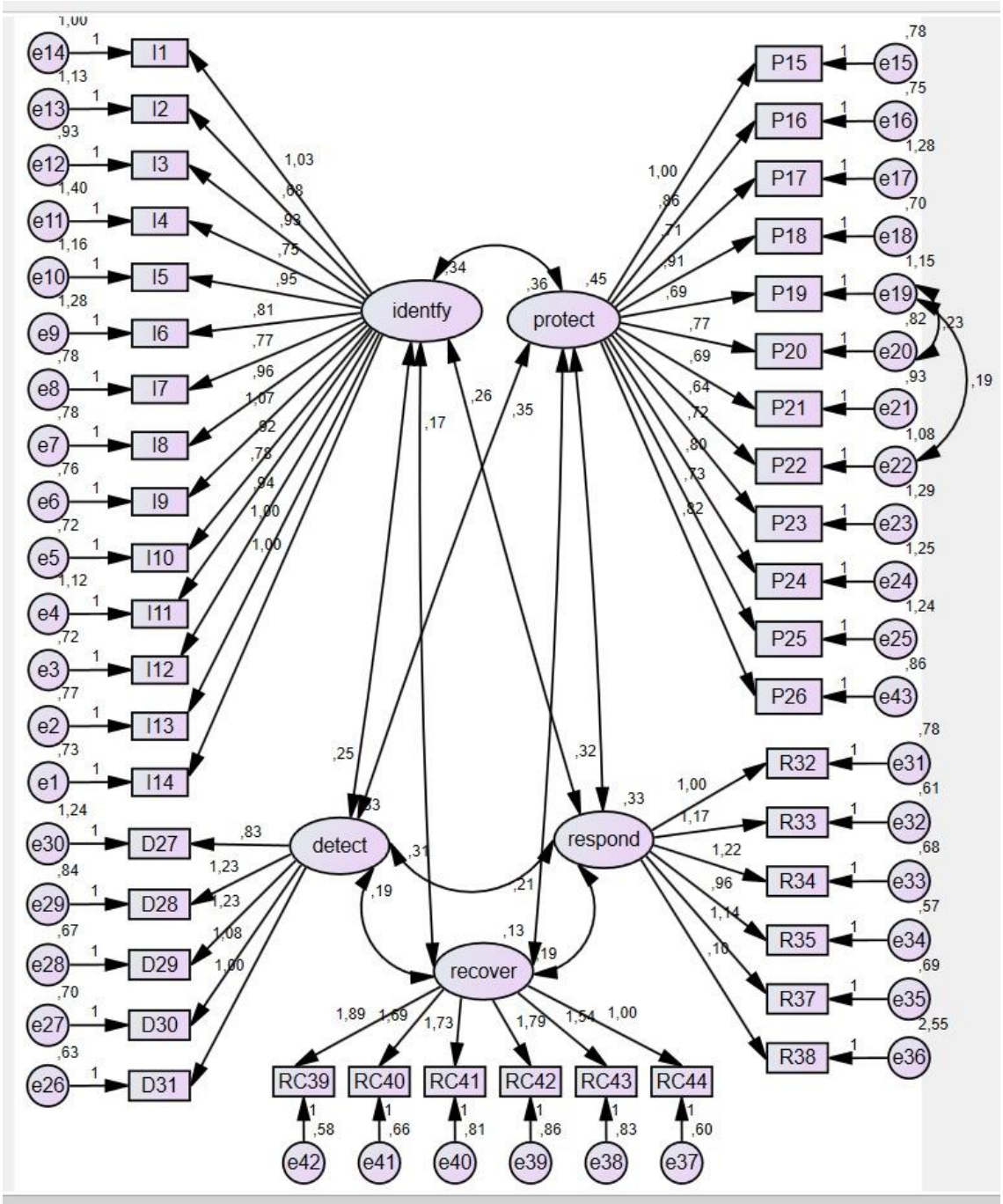

Figure 2. Confirmatory factor analysis diagram

As shown in Figure 2, the standardized correlation results indicate how well each item represents its corresponding factor. Accordingly, factor loadings range from .60 to .78 for the Identify factor, .64 to .83 for the Protect factor, .65 to .85 for the Detect factor, .61 to .79 for the Respond factor, and .68 to .88 for the Recover factor. To improve the model, covariance paths were drawn between error terms e19-e20 and e19-e22, based on the relationships between items P19-P20 and P19-P22, respectively (Schreiber et al., 2006). The finding that standardized values between observed factors are .61 and above, with each below 1, indicates that the items adequately represent the variables (Aytaç & Öngen, 2012).

Item discrimination

The ability of the Cyber Resilience Scale items to differentiate between individuals with varying levels of the measured construct was examined through item discrimination analysis. To this end, participants were divided into two groups based on total scale scores, representing the upper 27% and lower 27% of the distribution.

Differences in item-level mean scores between these two groups were analyzed using independent samples t-tests in order to evaluate whether the items effectively distinguished between high- and low-scoring participants. The statistical significance of these differences was assessed in line with established methodological recommendations (Büyüköztürk, 2002; Büyüköztürk et al., 2019). The results of the item discrimination analyses are presented in Table 7.

Table 7. t-Test Analysis Results for Lower and Upper Group Mean Scores

Groups	**N**	**Mean**	**SD**	**df**	**t**	**p**
Lower 27%	207	130.45	12.94	412	56.76	.000*
Upper 27%	207	206.27	11.52			

Note. *p < .001

As shown in Table 7, a significant difference was found between the lower 27% and upper 27% groups (t(412) = 56.76, p < .001). Table 7 presents the results of item analysis regarding the differences between the lower 27% and upper 27% groups, conducted to determine the adequacy of all items in the scale in terms of the characteristics they measure.

Table 8. CRS Lower 27% and Upper 27% intergroup t-Test results

F1 (Identify)	t	F2 (Protect)	t	F3 (Detect)	t	F4 (Respond)	t	F5 (Recover)	t
I1	22.4	P15	27.8	D27	23.6	R32	24.1	RC39	25.5
I2	25.6	P16	24.7	D28	22.7	R33	26.3	RC40	27.1
I3	23.9	P17	26.2	D29	25.4	R34	27.0	RC41	28.0
I4	24.3	P18	25.0	D30	24.5	R35	25.9	RC42	26.7
I5	21.7	P19	26.8	D31	22.9	R36	23.8	RC43	27.3
I6	23.2	P20	25.4			R37	22.7		
I7	25.1	P21	23.3			R38	24.6		
I8	26.7	P22	24.9						
I9	27.3	P23	26.5						
I10	25.8	P24	25.9						
I11	26.1	P25	27.4						
I12	27.0	P26	26.7						
I13	24.6								
I14	23.5								
Total (F1, F2, F3, F4, F5)=56.76; p<.001									

As shown in Table 8, the differences between the Cyber Resilience Scale lower 27% and upper 27% groups were determined to be significant. The obtained values ranged from 21.7 to 28.0, with all t-values significant at p < .001. Therefore, it can be stated that the differences are significant and the discriminative power is high for each factor, item, and the entire scale.

Findings regarding scale reliability

Following the validity analyses, a measurement instrument consisting of 43 items grouped under five factors was finalized. The complete list of scale items is presented in

Appendix B. The reliability of the instrument was examined to determine the extent to which the items consistently represent the targeted construct. Reliability evidence constitutes an important complement to factor analytic results, as it reflects the internal consistency and coherence of item responses within the proposed factor structure (Büyüköztürk, 2002; Kalaycı, 2010; Yiğit, Bütüner, & Dertlioğlu, 2008).

Internal Consistency

Various approaches are described in the methodological literature for estimating scale reliability, including test–retest, parallel forms, split-half techniques, and internal consistency coefficients. Among these, Cronbach's alpha is widely used in studies employing Likert-type measurement instruments (Büyüköztürk, 2002). However, because Cronbach's alpha assumes tau-equivalence, it may underestimate reliability when item loadings vary (McNeish, 2018). To provide a more comprehensive picture of scale reliability, the present study reports three complementary reliability coefficients: Cronbach's alpha (α), McDonald's omega (ω), and the Spearman–Brown corrected split-half coefficient (rSB). McDonald's omega, which accounts for differences in factor loadings across items, is increasingly recommended as a preferred reliability estimator for multidimensional scales (McDonald, 1999; Revelle & Zinbarg, 2009). Split-half reliability further examines the internal consistency of scale items by correlating scores from two randomly assigned halves of the scale, with the Spearman–Brown formula applied to correct for test length (Nunnally & Bernstein, 1994). All three estimates were calculated for the total scale and each subscale following factor analysis (Sönmez, 2005), and the results are presented in Table 9.

Table 9. Internal Consistency Reliability of the Cyber Resilience Scale

Dimensions	**N Items**	**Cronbach's α**	**McDonald's (ω)**	**Split-Half rSB**	**Reliability Level**
CRS	43	.940	.942	.923	High
Identify	14	.930	.932	.912	High
Protect	12	.927	.929	.908	High
Detect	5	.902	.905	.887	High
Respond	7	.921	.923	.903	High
Recover	5	.915	.917	.896	High

α = Cronbach's alpha; ω = McDonald's omega; rSB = Spearman–Brown corrected split-half coefficient

As shown in Table 9, all three reliability indices demonstrated excellent consistency across the total scale and each subscale. Cronbach's alpha for the total scale was α = .940, and subscale values ranged from α = .902 (Detect) to α = .930 (Identify). McDonald's omega coefficients were marginally higher than the corresponding alpha values in all cases (ω = .942 for the total scale; range: .905–.932 across subscales), indicating that the alpha and omega estimates are highly consistent in the present dataset. Spearman–Brown corrected split-half coefficients were also high, ranging from rSB = .887 (Detect) to rSB = .923 (total scale), further confirming internal consistency across the two halves of each measure. According to the literature, a value above .60 is considered reliable (George & Mallery, 2003; Büyüköztürk, 2002; Pedersen & Liu, 2003; Field, 2024), and according to Çokluk et al. (2014), values between .80 and 1.00 are considered highly reliable. Given that all three reliability indices consistently exceeded .88 across the total scale and all subscales, the Cyber Resilience Scale can be considered to demonstrate excellent internal consistency.

Results, Discussion and Recommendations

This study developed and validated the CRS for middle school students by addressing two primary research questions related to construct validity and reliability. The findings provide strong psychometric evidence for a theoretically coherent five-factor structure aligned with the NIST CSF. Both exploratory and confirmatory factor analyses supported this structure, with model fit indices meeting or exceeding widely accepted criteria (Schermelleh-Engel et al., 2003). Internal consistency coefficients for all subscales and the total scale exceeded the .90 threshold, indicating excellent reliability (Çokluk et al., 2014).

Beyond its psychometric adequacy, the CRS demonstrates conceptual strengths when compared with existing instruments in related domains. The total explained variance (59.88%) is considered adequate for multidimensional constructs in the social sciences (Büyüköztürk, 2002; Tabachnick & Fidell, 2018), while also suggesting that cyber resilience is influenced by contextual factors beyond individual competencies, such as family digital practices, school-level cyber education quality, and peer norms. This interpretation aligns with socio-ecological perspectives emphasizing that children's digital resilience emerges through interactions between individual and environmental systems.

The CRS differs from existing digital citizenship and cybersecurity-related scales in several important ways. Digital citizenship scales (Kuş et al., 2017; Tutar, Erdem & Şahin, 2023) primarily emphasize cognitive awareness and behavioral norms but do not capture psychological processes such as emotional coping with cyberbullying, digital stress regulation, or post-incident recovery. Similarly, the Cybersecurity Scale developed by Arpaci & Ateş (2023) focuses on technical security competencies and awareness but does not assess social support-seeking or adaptive coping capacities. Although the Human CRS proposed by Joinson et al. (2023) incorporates psychological resilience dimensions, it was developed for adult populations and does not account for the developmental characteristics of children and early adolescents.

The theoretical integration of the NIST framework (NIST, 2018) with Masten's Resilience Theory (Masten, 2001, 2014) represents a key contribution of this study. While the NIST framework provides a functional structure for conceptualizing cybersecurity-related behaviors, resilience theory enables a developmental interpretation of how children regulate emotions, seek support, and adapt under conditions of digital stress. This dual-framework approach allows cyber resilience to be conceptualized not merely as a set of technical skills, but as a multidimensional psychosocial capacity that is activated under uncertainty, time pressure, and emotional strain. This distinction is theoretically significant, as knowing how to perform secure behaviors does not necessarily translate into consistently enacting them under stress (Masten, 2014).

The alignment of the CRS factor structure with NIST dimensions further suggests that middle school students differentiate between proactive preparation (Identify, Protect), threat detection, immediate response, and longer-term recovery processes. The relatively larger number of items in the Identify dimension may reflect the developmental importance of threat awareness during early adolescence, a period in which students transition from concrete to more abstract forms of reasoning and require greater scaffolding to recognize diverse digital risks before effective protective or adaptive actions can occur.

From an applied perspective, the CRS offers meaningful implications for educational practice. Educators and school counselors can use the scale to identify students with specific

vulnerability patterns, such as strong threat awareness but limited response or recovery capacities. This enables a shift from generic digital citizenship instruction toward targeted, profile-informed interventions that address emotional regulation, coping strategies, and help-seeking behaviors alongside technical knowledge. Such an approach aligns with contemporary educational frameworks emphasizing personalized and evidence-based interventions (OECD, 2021; Redecker, 2017).

By operationalizing cyber resilience as an adaptive psychosocial construct rather than a purely technical skill set, the CRS advances current conceptualizations of digital safety in childhood and early adolescence. The scale is well suited for use in intervention-based research, comparative studies, and educational program evaluation. It enables researchers to examine developmental trajectories of cyber resilience, evaluate the effectiveness of cyber safety interventions, and explore relationships between cyber resilience and broader digital well-being outcomes. At the practice and policy levels, aggregated CRS data may inform the design of school-based digital safety initiatives and support evidence-based decision-making in digital citizenship education.

Overall, the CRS represents a significant step toward understanding and supporting children's capacity to navigate digital risks in developmentally appropriate ways. Future research addressing the identified limitations—particularly through longitudinal designs, multi-informant data, and advanced modeling techniques—will further strengthen the scale's utility and contribute to the development of safer and more supportive digital environments for adolescents.

Declarations

Acknowledgments: *This research was supported by TÜBİTAK BİDEB 2218 Domestic Post-Doctoral Research Fellowship Program (Project No: 122C266). The author gratefully acknowledges this support.*
Funding: *This work was supported by the Scientific and Technological Research Council of Turkey (TÜBİTAK) under Grant 122C266 through the BİDEB 2218 Domestic Post-Doctoral Research Fellowship Program.*
Ethics Statements: *This study was approved by the Institutional Ethics Committee (Approval obtained: April 2024). All procedures performed in studies involving human participants were in accordance with the ethical standards of the institutional research committee and with the 1964 Helsinki declaration and its later amendments.*
Conflict of Interest: *The authors declare that they have no conflict of interest.*
Informed Consent: *Informed consent was obtained from all individual participants included in the study. For participants under 18 years of age, informed consent was obtained from their parents/legal guardians prior to their participation.*
Data availability: *The data that support the findings of this study are available from the corresponding author upon reasonable request. Due to privacy and ethical considerations, the raw data cannot be made publicly available but can be shared for verification purposes under appropriate data sharing agreements.*

References

Altunkaynak, M., & Çağımlar, Z. (2023). Digital fluency: A scale development study. *Journal of Dokuz Eylul University Buca Faculty of Education, 58*, 2541–2559. https://doi.org/10.53444/deubefd.1286954

Arpaci, I., & Ateş, E. (2023). Development of the cybercrime awareness scale (CAS): A validity and reliability study in a Turkish sample. *Online Information Review, 47*(4), 633–643. https://doi.org/10.1108/OIR-01-2022-0023

Arpaci, I., & Sevinc, K. (2022). Development of the cybersecurity scale (CS-S): Evidence of validity and reliability. *Information Development*, *38*(2), 218–226. https://doi.org/10.1177/0266666921997512

Bıçakcı, S., & Gürcüyener Evren, A. (2025). A magic remedy or a black box? Examining the resilience narrative against cyber crises. *Reflective, 1*. https://doi.org/10.47613/reflektif.2025.202

Bognár, L., & Bottyán, L. (2024). Evaluating Online Security Behavior: Development and Validation of a Personal Cybersecurity Awareness Scale for University Students. *Education Sciences*, *14*(6), 588. https://doi.org/10.3390/educsci14060588

Bognár, L., & Bottyán, L. (2024). Evaluating Online Security Behavior: Development and Validation of a Personal Cybersecurity Awareness Scale for University Students. *Education Sciences*, *14*(6), 588. https://doi.org/10.3390/educsci14060588

Büyüköztürk, Ş. (2002). Factor analysis: Basic concepts and its use in scale development. *Educational Administration: Theory and Practice, 32*, 470–483.

Büyüköztürk, Ş., Çokluk, Ö., & Köklü, N. (2019). *Statistics for the social sciences* (28th ed.). Ankara, Turkey: Pegem Academy.

Cattell, R. B. (1966). The Scree Test for the Number of Factors. *Multivariate Behavioral Research*, *1*(2), 245-276. https://doi.org/10.1207/s15327906mbr0102_10

Çokluk, Ö., Şekercioğlu, G., & Büyüköztürk, Ş. (2014). *Multivariate statistics for the social sciences: SPSS and LISREL applications* (3rd ed.). Ankara, Turkey: Pegem Academy.

Connor, K. M., & Davidson, J. R. T. (2003). Development of a new resilience scale: The Connor-Davidson Resilience Scale (CD-RISC). *Depression and Anxiety*, *18*(2), 76-82. https://doi.org/10.1002/da.10113

DeVellis, R. F. (2017). *Scale Development: Theory and Applications* (4th bs). Sage Publications.

Erikson, E. H. (1968). *Identity youth and crisis* (No. 7). WW Norton & company.

Erkuş, A. (2019). *Measurement and scale development in psychology—I: Basic concepts and procedures* (4th ed.). Ankara, Turkey: Pegem Academy.

European Commission. (2022). A digital decade for children and youth: The new European strategy for a better internet for kids (BIK+) (COM(2022) 212 final). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022DC0212

Everitt, B. S., & Hothorn, T. (2011). *An Introduction to Applied Multivariate Analysis with R*. Springer.

Field, A. (2013). *Discovering Statistics Using IBM SPSS Statistics* (4th bs). Sage Publications.

Gravetter, F. J., & Wallnau, L. B. (2017). *Statistics for the Behavioral Sciences* (10th bs). Cengage Learning.

Joinson, A. N., Dixon, M., Coventry, L., & Briggs, P. (2023). Development of a new 'human cyber-resilience scale'. *Journal of Cybersecurity*, *9*(1), tyad007. https://doi.org/10.1093/cybsec/tyad007

Korkmaz, Ö., Kovanci, Ö., & Uğur Erdoğmuş, F. (2021). Validity and reliability study of the scale of middle school students' perceptions of moral values in digital environments. *Journal of Erzincan University Faculty of Education, 23*(2), 298–315. https://doi.org/10.17556/erziefd.646377

Kurt, A., Uzun, İ. B., Açıcı, B. N., Tunç, A. C., & Büyükatar, B. (2025). The Relationship between Cyber Wellness and Psychological Resilience in Children: A Cross-Sectional Study. *Genel Tıp Dergisi*, *35*(2), 352-361. https://doi.org/10.54005/geneltip.1539354

Kuş, Z., Güneş, E., Başarmak, U., & Yakar, H. (2017). Development of a Digital Citizenship Scale for Youth: A Validity and Reliability Study. *Journal of Computer and Education Research*, *5*(10), 298-316. https://doi.org/10.18009/jcer.335806

Lawshe, C. H. (1975). A Quantitative Approach to Content Validity. *Personnel Psychology*, *28*(4), 563-575. https://doi.org/10.1111/j.1744-6570.1975.tb01393.x

Masten, A. S. (2001). Ordinary Magic: Resilience Processes in Development. *American Psychologist*, *56*(3), 227-238. https://doi.org/10.1037/0003-066X.56.3.227

Masten, A. S. (2014). Invited Commentary: Resilience and Positive Youth Development Frameworks in Developmental Science. *Journal of Youth and Adolescence*, *43*(6), 1018-1024. https://doi.org/10.1007/s10964-014-0118-7

McKenzie, J. F., Wood, M. L., Kotecki, J. E., Clark, J. K., & Brey, R. A. (1999). Establishing Content Validity: Using Qualitative and Quantitative Steps. *American Journal of Health Behavior*, *23*(4), 311-318. https://doi.org/10.5993/AJHB.23.4.9

McNeish, D. (2018). Thanks coefficient alpha, we'll take it from here. *Psychological Methods, 23*(3), 412–433. doi:10.1037/met0000144

National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1* (No. NIST CSWP 04162018; s. NIST CSWP 04162018). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162018

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (No. NIST CSWP 29; s. NIST CSWP 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

New perspectives on measuring cybersecurity (OECD Digital Economy Papers No. 366; OECD Digital Economy Papers, C. 366). (2024). https://doi.org/10.1787/b1e31997-en

Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory* (3rd ed.). New York, NY: McGraw-Hill.

OECD (2024). New perspectives on measuring cybersecurity. OECD Digital Economy Papers, No. 366. OECD Publishing. https://doi.org/10.1787/b1e31997-en

Pan, Q., Lan, M., Tan, C. Y., Tao, S., Liang, Q., & Law, N. (2024). Protective factors contributing to adolescents' multifaceted digital resilience for their wellbeing: A socio-ecological perspective. *Computers in Human Behavior*, *155*, 108164. https://doi.org/10.1016/j.chb.2024.108164

Pedersen, E. R., & Kurz, J. (2016). Using Facebook for Health-Related Research Study Recruitment and Program Delivery. *Current Opinion in Psychology*, *9*, 38-43. https://doi.org/10.1016/j.copsyc.2015.09.011

Pew Research Center. (2020, July 28). *Children's engagement with digital devices, screen time*. https://www.pewresearch.org/internet/2020/07/28/childrens-engagement-with-digital-devices-screen-time/

Piaget, J. (1972). *Psychology and epistemology: Towards a theory of knowledge* (P. A. Wells, Çev.). Allen Lane.

Plintz, N. B., & Ifenthaler, D. (2025). Empowering children online: A holistic skills framework for cybersecurity. *Educational Technology Research and Development*. https://doi.org/10.1007/s11423-025-10565-z

Redecker, C. (2017). *European Framework for the Digital Competence of Educators: DigCompEdu* (No. EUR 28775 EN). Publications Office of the European Union. https://doi.org/10.2760/159770

Schermelleh-Engel, K., Moosbrugger, H., & Müller, H. (2003). Evaluating the Fit of Structural Equation Models: Tests of Significance and Descriptive Goodness-of-Fit Measures. *Methods of Psychological Research Online*, *8*(2), 23-74.

Schreiber, J. B., Nora, A., Stage, F. K., Barlow, E. A., & King, J. (2006). Reporting Structural Equation Modeling and Confirmatory Factor Analysis Results: A Review. *The Journal of Educational Research*, *99*(6), 323-338. https://doi.org/10.3200/JOER.99.6.323-338

Setiawati, R., & Sunra, L. (2024). Cyberculture in Higher Education: Narrowing the digital gap between Mark Prensky's "Digital Natives" and "Digital Immigrants". *International Journal of Humanities and Social Sciences*, *4*(1), 57-61.

Sönmez, V. (2005). *Teacher's handbook in curriculum development* (11th ed.). Ankara, Turkey: Anı Publishing

Tabachnick, B. G., & Fidell, L. S. (2013). *Using Multivariate Statistics* (6th bs). Pearson.

Tutar, H., Erdem, A. T., & Şahin, N. (2024). Digital Citizenship Scale (DCS): A Validity and Reliability Study. *Alanya Academic Review*, *8*(1), 310-327. https://doi.org/10.29023/alanyaakademik.1337114

Tzavara, V., & Vassiliadis, S. (2024). Tracing the evolution of cyber resilience: A historical and conceptual review. *International Journal of Information Security*, *23*(3), 1695-1719. https://doi.org/10.1007/s10207-023-00811-x

Worthington, R. L., & Whittaker, T. A. (2006). Scale Development Research: A Content Analysis and Recommendations for Best Practices. *The Counseling Psychologist*, *34*(6), 806-838. https://doi.org/10.1177/0011000006288127

Yılmaz, O., & İbret, B. Ü. (2023). A Scale Development Study to Determine Middle School Students' Digital Citizenship Levels." *Journal of Muş Alparslan University Faculty of Education*, 3(1), 59-77.

Yiğit, N., Bütüner, S. Önder, & Dertlioğlu, K. (2008). Development of an Instructional Website Evaluation Scale. *Necatibey Faculty of Education Electronic Journal of Science and Mathematics Education, 2*(2), 38-51