Erciyes Üniversitesi
İktisadi ve İdari Bilimler Fakültesi Dergisi
e-ISSN: 2630-6409

Araştırma Makalesi | Research Article
Yayın Tarihi: 30 Nisan 2026 | Published: April 30, 2026
doi: 10.18070/erciyesiibd.1789115

Sorumlu Yazar/ Corresponding Author:
Ece ZEYBEK YILMAZ,
ece.zeybek@hotmail.com.tr

JEL:
M10, M54, M19

Geliş: *22 Eylül 2025*
Received: *September 22, 2025*
Kabul: *23 Şubat 2026*
Accepted: *February 23, 2026*
Yayın: *30 Nisan 2026*
Published: *April 30, 2026*

Atıf / Cited as (APA):
Zeybek Yılmaz, E. & Bayram, A. (2026), Turkish Validity and Reliability Study of Cyber-Paranoia and Fear Scale, Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 73, 151-157, doi: 10.18070/erciyesiibd.1789115

Etik Kurul İzni / Ethics Commitee Permission:
Bu çalışma için etik kurul izni Bolu Abant İzzet Baysal Üniversitesi Sosyal Bilimlerde İnsan Araştırmaları Etik Kurulu'nun 04/06/2024 tarih ve 2024/210 protokol numaralı kararı ile alınmıştır.

TURKISH VALIDITY AND RELIABILITY STUDY OF CYBER-PARANOIA AND FEAR SCALE

ECE ZEYBEK YILMAZ [1*] ***AYHAN BAYRAM*** [2]

[1] *Dr. Öğr. Üyesi, Istanbul Gelişim Üniversitesi/İktisadi, İdari ve Sosyal Bilimler Fakültesi/Havacılık Yönetimi Bölümü, ece.zeybek@hotmail.com.tr*
[2] *Doç. Dr., Bolu Abant İzzet Baysal Üniversitesi, Gerede Uygulamalı Bilimler Fakültesi, Uluslararası Ticaret ve Lojistik Bölümü, ayhan_bayram1987@hotmail.com*

ABSTRACT

This study aims to determine the validity and reliability levels of the Cyber Paranoia and Fear Scale, developed by Mason et al.(2014), within a Turkish sample. Designed to measure the emotional and cognitive impacts of digital threats, this scale serves as a critical tool for identifying whether personal anxieties reach a clinical or social level of paranoia. The research focused on a sample of 250 academics from various universities, utilizing a non-probability convenience sampling method.. The scale, consisting of 11 items and two sub-dimensions, was administered using a four-point Likert system. This specific rating structure was maintained to prevent neutral responses, thereby ensuring participants committed to a clear stance. Data analysis was conducted using SPSS 24 and Amos 24. Exploratory and confirmatory factor analyses verified two primary sub-dimensions with eigenvalues greater than one: "Cyber paranoia" and "Cyber fear". Statistical findings revealed that these two dimensions explained 49.163% of the total variance. Furthermore, the fit indices obtained demonstrated that the scale was structurally highly consistent and bore a high degree of similarity to the original scale structure. Consequently, this adaptation study has contributed to the academic literature by establishing the Cyber Paranoia and Fear Scale as a valid and reliable measurement tool that can be used in research in Turkey.

Keywords: academicians, cyber fear, cyber paranoia, Turkish validity and reliability

SİBER PARANOYA VE KORKU ÖLÇEĞİNİN TÜRKÇE GEÇERLİLİK VE GÜVENİLİRLİK ÇALIŞMASI

ÖZ

Bu çalışma, dijitalleşen dünyada bireylerin karşılaştığı psikolojik zorlukları anlamlandırmak amacıyla Mason ve arkadaşları (2014) tarafından geliştirilen Siber Paranoya ve Korku Ölçeği'nin Türkiye örneklemindeki geçerlilik ve güvenilirlik düzeyini belirlemeyi hedeflemektedir. Siber dünyadaki tehditlerin bireyler üzerindeki duygusal ve bilişsel etkilerini ölçmeyi amaçlayan bu ölçek, kişisel korku ve endişelerin klinik veya sosyal anlamda bir paranoya seviyesine ulaşıp ulaşmadığını saptamak için kritik bir araç olarak öne çıkmaktadır. Araştırma, metodolojik olarak çeşitli üniversitelerde görev yapan 250 akademisyenden oluşan bir örneklem grubuna odaklanmıştır. Veri toplama sürecinde olasılıksız kolaylık örnekleme yöntemi benimsenmiş ve 11 madde ile 2 alt boyuttan oluşan ölçek katılımcılara sunulmuştur. Katılımcıların belirsiz veya tarafsız kalarak verilerin niteliğini etkilemesini önlemek amacıyla, orijinal yapıdaki Likert tipi cevap anahtarı korunarak dörtlü bir derecelendirme sistemi kullanılmıştır. Bu sayede bireylerin kendilerine en yakın hissettikleri görüşe net bir şekilde yönelmeleri sağlanmıştır. Toplanan verilerin analizi, SPSS 24 ve Amos 24 istatistik yazılımları kullanılarak titizlikle gerçekleştirilmiştir. Yapılan keşifsel ve doğrulayıcı faktör analizleri sonucunda, özdeğerleri birin üzerinde olan "siber paranoya" ve "siber korku" adlı iki temel alt boyut doğrulanmıştır. İstatistiki bulgular, bu iki boyutun toplam varyansın %49,163'ünü açıkladığını ortaya koymuştur. Ayrıca elde edilen uyum indeksleri, ölçeğin yapısal olarak son derece tutarlı olduğunu ve orijinal ölçek yapısıyla yüksek derecede benzerlik taşıdığını kanıtlamıştır. Sonuç olarak, bu adaptasyon çalışması ile Siber Paranoya ve Korku Ölçeği'nin Türkiye'deki araştırmalarda kullanılabilecek geçerli ve güvenilir bir ölçme aracı olduğu akademik literatüre kazandırılmıştır.

Anahtar Kelimeler: akademisyenler, siber korku, siber paranoya, Türkçe geçerlilik ve güvenilirlik

1. Introduction

In parallel with rapid global technological advancements, the integration of computers and information technologies into daily life continues to expand. Individuals increasingly rely on digital platforms to meet diverse needs, ranging from work and education to entertainment, shopping, and socialization. However, this increased time spent in cyberspace and the diversity of digital actions have brought about a surge in cybercrimes, such as cyberbullying, identity fraud, cyber espionage, ransomware attacks, and privacy violations. Consequently, this digital transformation has created a paradoxical situation in which tools designed to facilitate life also become sources of profound psychological distress, leading to heightened fear among intensive technology users (Mason et al., 2014).

Conceptually, fear is defined as a realistic anxiety inherent in human nature, serving as a vital survival mechanism against life-threatening situations (Schuett, 2020; Şahin, 2019). While fear is a natural reaction to physical threats, the dynamics of fear in the digital age are more complex. Freud distinguished between realistic anxiety and neurotic anxiety, suggesting that the struggle to control impulses against social norms can generate secondary fears. In the modern context, this manifests as "cyber fear" or "cyber paranoia." As artificial intelligence and algorithmic monitoring technologies evolve, individuals face not only physical threats but also abstract threats, such as the loss of employment, privacy violations, and unauthorized tracking of personal data (Rilho, 2019).

This atmosphere of digital insecurity triggers "cyber paranoia," a mental state characterized by exaggerated suspicion, fear, and insecurity regarding the use of technology (Freeman & Freeman, 2008). Although cyberbullying and internet addiction have been extensively studied in the literature (Arpaci et al., 2020; Kowalski et al., 2014), the specific construct of "cyber paranoia"—driven by the fear of data tracking and surveillance—has received less attention. Zuboff (2019) highlights that the commodification of personal data in the age of "surveillance capitalism" creates a state of constant vigilance and anxiety in users. Furthermore, recent studies indicate that as digital dependency increases, particularly in professional settings, the psychological burden of potential cyber threats intensifies (Keles et al. 2020). Therefore, there is a distinct need for valid measurement tools that specifically address these paranoid ideations regarding digital privacy and security.

The primary aim of this study is to adapt the "Cyber-Paranoia and Fear Scale" into Turkish and examine its psychometric properties. Validating this scale is crucial for understanding the psychological toll of digital risks in different cultural contexts. In this adaptation study, academics were selected as the target sample. Although academics possess high digital literacy, they represent a high-risk group due to the intellectual property they generate and the critical importance of digital security for their career sustainability (Dikmen & Tuncer, 2017). Therefore, testing the validity of this scale on academics provides an important opportunity to measure cyber paranoia in a group that is both knowledgeable about and highly vulnerable to digital threats.

2. Literature review

2.1. Conceptual framework

The Distinction Between Fear and Anxiety in the Digital Context Fear and anxiety are often regarded as related concepts in psychology; however, they possess distinct phenomenological characteristics. Fear refers to an immediate, rational emotional reaction to a present and identifiable danger, whereas anxiety reflects a diffuse response to potential, ambiguous situations that have not yet occurred (Gençöz, 1998). In the context of the digital age, this distinction becomes crucial. With the proliferation of technology, individuals face tangible threats such as financial loss or identity theft, which trigger "cyber fear." However, the ambiguity of the digital realm also fosters "cyber paranoia," a more complex construct associated with the suspicion of constant monitoring. Psychoanalytic interpretations suggest that the virtual reality universe serves as a mirror, reflecting idealized versions of individuals (Apter, 2006). However, this environment also creates a paranoid dimension where users feel marginalized or persecuted by invisible digital entities, a phenomenon now conceptualized as cyber paranoia.

2.2. Cyber paranoia

Persecutory Ideation in Cyberspace Cyber paranoia is defined as an excessive cognitive fear that causes the individual to harbor persecutory thoughts about situations perceived as less threatening by the general population (Statham et al., 2019). Unlike rational caution, cyber paranoia involves a progression from anxiety to delusional assumptions. An individual may initially feel anxious about potential surveillance; however, as this anxiety escalates, it transforms into excessive stress characterized by the belief that oneself, one's environment, and the world at large are under malicious threat (Bennetts et al., 2022). This construct manifests in specific behavioral patterns. Kaya and Ata (2022) describe cyber paranoia as excessive preoccupation with thoughts such as being watched by a camera, phones being bugged, or emails being intercepted. It also extends to social interactions, where individuals may hide their true identities or obsess over whether their posts are "liked." Rajmohan (2016) notes that behaviors such as disabling "read receipts" on WhatsApp due to fear of judgment or assuming that online peers are conspiring against them can be classified within the spectrum of paranoid personality traits or delusional disorders.

2.3. Cyber fear

Rational Caution vs. Irrational Avoidance While cyber paranoia involves delusional elements, cyber fear is often grounded in the realistic possibility of victimization. Research indicates a divergence in how these two constructs affect user behavior. For instance, Zimaitis et al. (2020) found that while cyber paranoia negatively affects attitudes towards social media use and online purchasing, cyber fear does not necessarily inhibit these behaviors. Similarly, Akdemir (2020) revealed that internet users continue to engage in purchasing behavior despite their fear of cybercrime, although they may adopt cautious strategies such as using only trusted sites. This suggests that cyber fear may act as a protective, adaptive mechanism, whereas cyber paranoia acts as a maladaptive barrier. Furthermore, Shahid (2021) highlighted gender differences in these perceptions, noting that female users, particularly in security-related professions, exhibit lower trust in online profiles, stemming from a realistic fear of harassment rather than paranoid delusion.

2.4. The need for adaptation

Assessing the Psychometric Gap The conceptual distinction between "rational fear" (Cyber Fear) and "irrational suspicion" (Cyber Paranoia) necessitates separate measurement dimensions. Mason et al. (2014) developed the "Cyber-Paranoia and Fear Scale" specifically to address this duality. The scale consists of 11 items: 6 measuring the Cyber Paranoia dimension (e.g., belief in conspiracy or surveillance) and 5 measuring the Cyber Fear dimension (e.g., worry about data theft). Although various measurement tools exist in Türkiye regarding internet addiction, cyberbullying sensibility, or general cyber-victimization, there is a lack of specific instruments that quantitatively distinguish between "cyber fear" and "cyber paranoia." Existing scales mostly focus on the behavioral consequences of internet use rather than the specific cognitive distortions associated with paranoia. Therefore, adapting the scale developed by Mason et al. (2014) into Turkish is essential to fill this gap in the literature. This adaptation will allow researchers to determine whether Turkish internet users' concerns stem from realistic caution (fear) or persecutory ideation (paranoia), providing a more nuanced psychometric foundation for future interventions.

3. Method

3.1. Universe and sample

The sample group was determined by non-probability convenience sampling method. Convenience sampling refers to the process of selecting individuals who are readily accessible and willing to participate in the research. In this context, given time, cost, and logistical constraints,

the sample was selected from participants who were physically close to the researcher and available (Saunders et al. 2019). The Turkish adaptation study of the Cyber-Paranoia and Fear Scale was conducted with 250 academicians working at various universities. In order to determine the suitability of the scale's factor structure for Turkish culture, a survey was administered to 254 individuals in person and online. After eliminating incorrectly or incompletely filled-out surveys, the remaining 250 surveys were subjected to analysis. The reason for selecting academics as the research sample is that this group faces a high degree of intellectual property risk in the cyber environment, and that digital security is directly related to the sustainability of academic careers. In addition, academics' high digital awareness enables more qualified and conscious feedback to be obtained when measuring complex psychological structures such as cyber paranoia and fear. This makes them an ideal sample group for examining the concepts of cyber paranoia and fear. Also, this selection aims to test the scale's validity not only among general users but also among high-risk professional groups. In this respect, a sample of 250 people is sufficient for the Cyber-Paranoia and Fear Scale consisting of 11 items (Zorlu & Ünübol, 2018).

3.2. Data collection tools

The research was conducted through interviews with academics from various universities between June 11 and July 15, 2024. The sample group was asked to answer statements regarding the Cyber-Paranoia and Fear Scale, as well as gender, age, marital status, and the type of university they work at. Delusions about technology, and the Internet in particular, are becoming increasingly common, and fear-reality statistics show that computer-related fears are widespread. These fears form a continuum from the widely understandable and realistic to the unrealistic and frankly paranoid. The Cyber-Paranoia and Fear scale developed by Mason et al. investigated the validity of this construct in a non-clinical population by creating a new self-report scale. The Cyber-Paranoia and Fear Scale aims to measure threat perception related to information technologies arising from or enabled by computers, smartphones, social networks and digital surveillance. The psychometric properties of the Cyber-Paranoia and Fear Scale are reported, along with those of an established measure of scepticism and paranoia, in 181 participants, including a subgroup of 50 information technology professionals. Exploratory factor analysis revealed the existence of two interrelated dimensions, which we termed cyber-paranoia (6 items) and cyber-fear (5 items). The exploratory factor analysis revealed a two-factor structure consisting of 11 items, explaining 36% of the total variance. There is a significant correlation between the factors (r = 0.45). Cyber paranoia consists of six items with loadings ranging from 0.48 to 0.68. Cyber fear loadings range from 0.53 to 0.71 across five items. Both subscales are internally consistent and produce a normal score distribution. The Cronbach Alpha values of the subscales are .75 and .74, respectively. On the scale, a four-point Likert scale was used as in the original structure, especially to prevent participants from remaining neutral and to enable them to choose the option they feel closest to. The maximum score that can be obtained from the scale is 44. The difference of cyber-paranoia from general trait paranoia seems to reflect the clinical difference of "internet" and other technology-related delusions. Providing information to increase technological competence and awareness may reduce cyber-paranoia.

3.3. Procedure

At first, two specialists translated the original English version of the Cyber-Paranoia and Fear Scale into Turkish, then retranslated the Turkish version into English. The necessary revisions were made to items where meaning shifts were detected in order to ensure consistency between the two forms. In the final stage, final checks were carried out to ensure suitability for the Turkish language and culture, taking into account the opinions of academics specializing in the field, and the scale was made ready for implementation. The construct validity of the scale was tested using SPSS 24 and AMOS 24 statistical programs. The study was evaluated using descriptive, validity, exploratory factor analysis (EFA), confirmatory factor analysis (CFA), and correlation analysis. EFA is used to explore the underlying factor structure of the scale. Especially during the scale development phase or when the factor structure is not clearly known beforehand, EFA should be used (Fabrigar & Wegener, 2011). CFA is used to test a predetermined factor model. Therefore, in order to perform CFA, a structure must first be determined via EFA (Brown, 2015). The scale's reliability was calculated using the Cronbach's Alpha coefficient. Participants were asked to fill out a volunteer form and detailed information about the study was provided. Data were analyzed at a 95% confidence level.

Approval and consent to participate in this study obtained ethical approval from XXXX University Ethics Committee for Human Research in the Social Sciences (Date: 04.06.2024, Meeting Number: 2024/05). The research adhered to the ethical guidelines outlined in the 1964 Declaration of Helsinki and its subsequent amendments. Each participant provided informed consent prior to participation. Written informed consent was obtained from all participants.

4. Results

Information on the results of the research is as follows: Demographic data of the research participants are presented in Table 1.

TABLE 1 | Demographic data on the sample group (n=250)

Demographic Characteristics								
Gender	*n*	*Percentage (%)*	**Marital Status**	*n*	*Percentage (%)*	**University Type**	*n*	*Percentage (%)*
Female	142	56.8	**Married**	169	67.6	**Foundation University**	60	24.0
Male	108	43.2	**Single**	81	32.4	**Public University**	190	76.0

Of the sample group, 56.8% were female and 43.2% were male; 67.6% were married and 32.4% were single; 24% were working at foundation universities and 76% at public universities. It was also determined that the average age of the sample group was 41.09±8.32. Within the scope of the study, exploratory factor analysis (EFA) was conducted for the construct validity of the scale and the reliability of the scale was calculated with Cronbach Alpha reliability coefficients. In conducting exploratory factor analysis, principal component analysis was used as the factor extraction method. This method focuses on representing the total variance (information) in the data with the minimum number of components possible. The first principal component (PC1) explains the highest variance in the data, while the second principal component (PC2) explains the largest portion of the remaining variance, provided it is orthogonal to the first (Jolliffe & Cadima, 2016). Thus, the size of the data set is minimized without significant loss of information. The Cyber-Paranoia and Fear Scale consists of 11 items and includes two sub-dimensions. The sub-dimensions of the Cyber-Paranoia and Fear Scale are cyber paranoia and cyber fear. When the means and standard deviations of the sample group's responses to the scale items are examined, it is seen that item 6 has the highest mean and item 2 has the lowest mean.

TABLE 2 | Distribution of the scale according to factors

Items	$\bar{X}$ ±SD	1st Factor Cyber Paranoia	2nd Factor Cyber Fear	Corrected Item-Total Correlation	AVE	CR	Cronbach Alpha
1. Increased use of computers has a negative impact on children's brains.	2.99±0.94	.753		.333			
2. I think the global internet will collapse soon with terrible consequences.	1.97±0.92	.739		.307	.50	.74	.669	.815
3. I avoid using the internet for personal matters as much as possible so that my information does not fall into the hands of others.	2.24±0.95	.615		.358			

TABLE 2 (Continued)| Distribution of the scale according to factors

Items	$\bar{X}$ ±SD	1st Factor Cyber Paranoia	2nd Factor Cyber Fear	Corrected Item-Total Correlation	AVE	CR	Cronbach Alpha
4. I think people should be concerned that their movements can be tracked through smartphones.	3.14±0.85		.792	.694			
5. Terrorists use the internet to find new ways to plan new attacks on the public.	2.98±0.90		.760	.609			
6. Payment cards (credit cards, shopping cards, etc.) allow officials to track my travels and purchases.	3.30±0.88		.746	.524			
7. Closed circuit television cameras (CCTV) are used illegally to monitor people.	2.79±0.91		.730	.461			
8. I am worried that my social media accounts (Facebook, Instagram, etc.) may be edited by others without my permission.	2.88±0.99		.660	.526	.50	.88	.831
9. Companies that store data about customers are very vulnerable to the theft of my private information.	3.08±0.81		.684	.472			
10. I think people are not concerned enough about threats arising from their use of technology.	3.03±0.86		.680	.507			
11. I am concerned about the effects of electromagnetic waves emitted by cell phones/ base stations.	3.04±0.94		.530	.527			
Eigenvalue		1.842	3.566				
Explained variance %		16.749	32.414				

Kaiser-Meyer-Olkin (KMO) and Bartlett's test results were analyzed for the scale's factor analysis. The results of the exploratory factor analysis for the Cyber-Paranoia and Fear Scale (KMO=0.875; X^2=701.293; df=55; p=.000) show that the scale is suitable for factor analysis. The minimum factor loading was set at 0.35, and if the loading of an item on the scale was above this value and 0.10 or higher than the item's loading on other factors, the item was counted in that factor (Barnes et al., 2001). The Varimax factor analysis method was used to identify two factors, each consisting of 11 items, explaining 49.163% of the scale. The first factor (Cyber Paranoia) consists of three items with loadings ranging between .615 and .753. The factor explained 16.749% of the total variance and its eigenvalue was 1.842. The second factor (Cyber Fear) consists of eight items with loadings ranging from .530 to .792. This factor explained 32.414% of the total variance, with an eigenvalue of 3.566. The Cronbach Alpha coefficient for the scale was .815, which shows that the reliability of the scale is quite good (Kayış, 2010).

The Average Explained Variance (AVE) and Composite Reliability (CR) values were calculated using Excel based on the factor loadings obtained from the AFA, using the formulas proposed by Fornell and Larcker (1981). The analysis yielded AVE values of 0.497 and 0.493 for the subscales, respectively. Although these values are marginally below the 0.50 threshold, CR values were considered for convergent validity. Fornell and Larcker (1981) state that when the AVE value is below 0.50, if the CR value is above 0.60, the convergent validity of the structure is acceptable (Lam, 2012). Given that the CR values obtained in the study ranged from 0.7464 to 0.8847, it was concluded that the scale's factor structure was found to be valid and reliable. For the sake of simplification in the table, both AVE values are presented as 0.50. These values show that the validity of the scale is within acceptable limits. The scree slope graph of the study is given in Figure 1.

FIGURE 1 | Scree plot graph

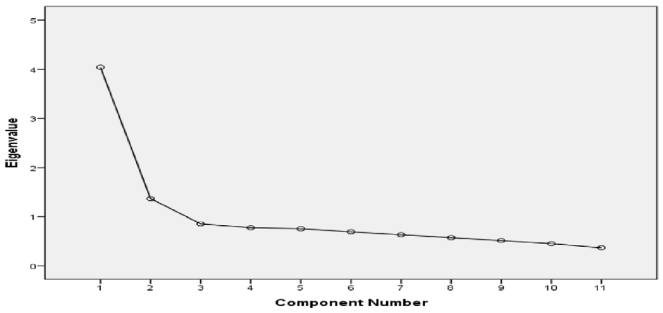
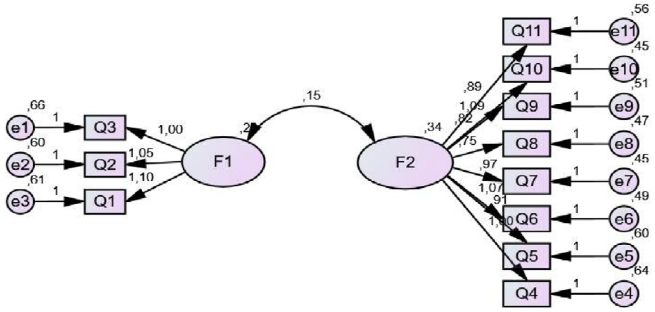


Figure 1. According to the results of the study, the scree plot analysis conducted to test whether the 2-factor scale was validated or not showed that the 2-factor structure was validated. The confirmatory factor analysis diagram of the Cyber-Paranoia and Fear Scale is shown in Figure 2.

FIGURE 2 | DFA diagram of the cyber-paranoia and fear scale



Confirmatory factor analysis was conducted to evaluate the validity of the two-factor structure of the Cyber-Paranoia and Fear Scale that emerged as a result of the exploratory factor analysis. The CFA results used to evaluate the validity of the model, which consists of a two-factor structure emerging from exploratory factor analysis, are presented in Table 3.

TABLE 3 | Results of confirmatory factor analysis

Compliance Index	Good Compliance	Accepted Compliance	Model	Compliance
X^2/sd (59.748/43)	$0 \le x^2/sd \le 3$	$3 \le x^2/sd \le 5$	1.389	Good Compliance
RMSEA	0 ≤ REMSEA ≤ .05	.05 ≤ REMSEA ≤ .08	.040	Good Compliance
GFI	0.95 ≤ GFI ≤ 1.00	.90 ≤ GFI ≤ .95	.961	Good Compliance
AGFI	0.90 ≤ AGFI ≤ 1.00	.85 ≤ AGFI ≤ .90	.939	Good Compliance
RMR	RMR ≤ .05	.05 ≤ RMR ≤.08	.040	Good Compliance
CFI	0.95 ≤ CFI ≤ 1.00	.90 ≤ CFI ≤ .95	.975	Good Compliance
CAIC	Comparison smaller than CAIC		209.742 < 785.936	Accept
ECVI	Comparison smaller than ECVI		.425 < 2.957	Accept
AIC	Comparison smaller than AIC		105.748 < 736.200	Accept

The primary-level CFA results for the Cyber-Paranoia and Fear Scale indicate that it supports a two-factor structure. As a result of the primary-level CFA, it was concluded that the modification indices were at a good level, and the CAIC, ECVI, and AIC values were accepted (Schermelleh-Engel et al., 2003). In the original scale development study (Mason et al., 2014), the construct validity of the scale was examined using EFA, and a two-dimensional structure was identified. However, this structure was not tested using CFA in the original study. In this study, First-Order CFA was applied to test the validity of the factor structure obtained with EFA in the original study within the Turkish culture. Since the main objective of the study was to verify whether the subscales identified in the original form (cyber paranoia and cyber fear) differentiated in the target population, the analyses were based on the first-order model. Because the sub-dimensions theoretically represent psychologically independent states, a first-order structure measuring the consistency of the original pattern was preferred over a second-order CFA testing a higher-order latent variable at this stage. The CFA results revealed that the two-factor structure of the scale is compatible with Turkish culture. The correlation values between cyber paranoia and fear, along with their sub-dimensions, are given in Table 4.

TABLE 4 | Correlation values (n=250)

	$\bar{X}$ ±SD	(1)	(2)	(3)
(1) Cyber Paranoia and Fear	31.44±5.92	1		
(2) Cyber Paranoia	7.20±2.04	.648*	1	
(3) Cyber Fear	24.20±4.85	.947*	.370*	1

As a result of the correlation analysis: The correlation coefficient between cyber paranoia and fear and cyber paranoia sub-dimension (r=.648; p<.05) is positive, moderate and statistically significant. The correlation coefficient between cyber paranoia and fear and cyber fear sub-dimension (r=.947; p<.05) is positively high and statistically significant. The correlation coefficient between cyber paranoia and cyber fear sub-dimensions (r=.370; p<.05) is positively weak and statistically significant.

The widespread use of information technologies leads to an increase in cyberbullying and thus causes people to experience sadness, frustration, and fear (Akdeniz & Dogan, 2024). In a study examining whether cyber paranoia about artificial intelligence and the privacy of personal data would reduce the use of social networks, the results were not as expected: although people reported feeling fear and even having paranoid thoughts, they did not reduce their use of social networks. It is thought that technological addiction is among the main reasons for this situation (Rilho, 2019). On the contrary, it was found that people who experienced cyber victimization felt insecure and paranoid (Wright, 2016). As a result of the transition to remote work in many professions during the COVID-19 pandemic, cybercrimes were committed by sending e-mails with the information that "up-to-date information about the disease was shared". These include crimes such as phishing, access to work information and account numbers. During the relevant period, many workplaces suffered heavy financial losses. For this reason, the importance of educating employees not to open every incoming e-mail has emerged (Ahmad, 2020). With the spread of digitalization, power asymmetries emerge between technology and the individual. Although technology providers say users can stop using online applications if they choose, the cost of not using technology is higher. For example, not being able to see job advertisements, not keeping up with current developments, and not being able to access useful platforms used by colleagues. On the other hand, power asymmetry can also occur due to the fact that the user agreements offered in the use of social networking platforms and search engines cannot be read by everyone, and even if they are read, the individual does not have the right to make changes to these agreements. The spread of remote work during COVID-19 has raised concerns about the online world, such as privacy and ethics (Veliz, 2021). This anxiety process affects the formation of cyber paranoia and fear behavior.

In a study revealing that as the use of the Internet becomes more widespread, employees' privacy decreases, employers (administrative representatives of the employer, HR specialists, etc.) make determinations about what employees follow or like on social platforms, how much of their working time they spend on the Internet while on the job, their family background, childhood, and past work experiences. As such practices become widespread, it has been revealed that employees have an incentive to avoid creating records to hide their actions. It can be said that paranoid behaviors "to protect privacy" such as writing what is written in e-mails on the basis that it can be seen by others, and receiving health services to prevent the creation of these records for reasons such as access to medical records (Bhave et al., 2020). In another study on the privacy of employees, it was emphasized that employees do not have the option not to share data, and that employers can access all kinds of data about the employee (contact and bank information, marital status, number of children, contract and salary information, certificates, picture identity documents, employee photos, internet access logs, sexual orientation, religion, location tracking, etc.), which causes anxiety in employees due to violation of privacy. For these reasons, it is thought that taking measures to protect privacy in businesses and authorizing employees about what kind of information they want to share will cause changes in the field of information technologies (Polst et al., 2019). Another privacy concern is balancing transparency and confidentiality of information stored in e-government applications. There is a fear that the confidentiality of information about both citizens in e-government and some private and public organizations may be compromised by cyber-attacks. The fact that records containing personal information, such as employees' social security numbers, performance evaluations, disciplinary penalties, substance abuse counseling, etc., are in the government database causes civil servants in particular to fear losing their jobs. As the use of social media, mobile devices and cloud computing increases, even in small settlements, public employees fear cyber-attacks by hackers, cyber criminals and even coworkers with low job satisfaction (Macmanus et al., 2013).

In a study on cyber paranoia, there are also studies that praise paranoia for its ability to protect information about the individual, family, and work. In this context, it has been stated that governments also exhibit paranoid behaviors. However, the reasons for this include increased attacks on banking and financial institutions, the pharmaceutical and chemical industries, and the oil and energy sectors, as well as the increase in e-mails designed to facilitate secret infiltration of workplaces through computer networks. Therefore, educating the public about cybersecurity is stated as the responsibility of the government. Thus, cyber defense is accepted as the responsibility not only of the government but also of every citizen. In the research, a user who does not have a social network and does not have information such as e-mail address and web page on the internet, and whose information is limited to information such as conferences, etc., is not actually paranoid and is defined as a "protective level of awareness" that should be applied by everyone (Laplante & DeFranco, 2010).

5. Discussion and conclusion

As a result of the study, it was determined that the Cronbach Alpha reliability coefficients calculated for the Cyber-Paranoia and Fear Scale and its sub-dimensions were at a sufficient level. The EFA and CFA regarding the construct validity of the scale showed results supporting the two-dimensional model as in the original scale (Table 2-3). In addition, statistically significant relationships were found as a result of the correlation analysis between cyber paranoia and fear and their sub-dimensions. The significant correlation coefficient between cyber paranoia and fear and its sub-dimensions indicated that the sub-dimensions of the scale measured similar constructs and the two-dimensional structure of the scale was compatible with Turkish culture. In the original structure of the scale, items that were evenly distributed between the two dimensions were found to be concentrated in the cyber fear dimension in the Turkish version (3 cyber paranoia, 8 cyber fear). In particular, the shift of items 5, 8, and 11 from cyber paranoia to the cyber fear dimension indicates a semantic shift. This situation shows that the perception of cybersecurity in Turkey exhibits a more 'threat and consequence-oriented' structure. While the 'paranoia' items in the original scale measure an individual's cognitive suspicions, in the Turkish sample, these suspicions have been replaced by direct

emotional anxiety (fear). This structural differentiation may stem from the sample group consisting of academics. For academics, data security in the digital environment is not just a personal preference; it also protects intellectual property and academic work. Therefore, the possibility of surveillance or interference in the cyber environment quickly surpasses an ambiguous stage of suspicion (paranoia) in this group and evolves into a concrete fear of loss (fear). The shift of cyber paranoia items toward the cyber fear dimension in the Turkish sample is consistent with the high uncertainty avoidance tendency defined by Hofstede (2001); as in such cultures, ambiguous threats (paranoia) are quickly coded as concrete concerns (fear). Furthermore, academics' professional sensitivity to data security leads them to assess cyber risks with a higher 'perception of harm' than ordinary users (Nicholas et al., 2017).

This study fills an important gap in the Turkish literature by introducing a clinically based measurement tool that focuses on the psychological implications of cybersecurity rather than its technical aspects. Unlike the existing local literature, this scale allows for differentiation between responses of 'suspicion' (paranoia) and 'concrete anxiety' (fear) to cyber threats. The factor structure specified in the original study (Mason et al., 2014) was reshaped in this study according to the dynamics of the local sample. In general, it is seen that the Turkish form of the Cyber-Paranoia and Fear Scale is usable, and the results of the analysis support this situation. In this study, the Cyber-Paranoia and Fear Scale was adapted for academicians. In future studies, it will be useful to analyze the validity and reliability of the Cyber-Paranoia and Fear Scale in sample groups consisting of employees from different sectors.

References

Ahmad, T. (2020). *Corona virus (COVID-19) pandemic and work from home: Challenges of cybercrimes and cybersecurity*. Social Science Research Network. https://doi.org/10.2139/ssrn.3568830

Akdemir, N. (2020). Examining the impact of fear of cybercrime on internet users' behavioral adaptations, privacy calculus and security intentions. *International Journal of Eurasia Social Sciences, 11*(40), 606–648. https://doi.org/10.35826/ijoess.2737

Akdeniz, B., & Doğan, A. (2024). Cyberbullying: Definition, prevalence, effects, risk and protective factors. *Current Approaches in Psychiatry, 16*(3), 425–438. https://doi.org/10.18863/pgy.1325195

Arpaci, I., Abdeljawad, T., Baloğlu, M., Kesici, Ş., & Mahariq, I. (2020). Mediating effect of internet addiction on the relationship between individualism and cyberbullying: Cross-Sectional questionnaire study. *Journal of Medical Internet Research, 22*(5), e16210. https://doi.org/10.2196/16210

Apter, E. (2006). On oneworldedness: Or paranoia as a world system. *American Literary History, 18*(2), 365–389. https://doi.org/10.1093/alh/ajj022

Barnes, J., Cote, J., Cudeck, R., & Malthouse, E. (2001). Factor analysis: Checking assumptions of normality before conducting factor analysis. *Journal of Consumer Psychology, 10*(1–2), 79–81. https://doi.org/10.2307/1480486

Bennetts, A., Stopa, L., & Newman-Taylor, K. (2022). What can experimental studies tell us about paranoia and anxiety? A systematic review with implications for theory and clinical practice. *Psychological, Social and Integrative Approaches, 14*(2), 162–175. https://doi.org/10.1080/17522439.2021.1909112

Bhave, D. P., Teo, L. H., & Dalal, R. S. (2020). Privacy at work: A review and a research agenda for a contested terrain. *Journal of Management, 46*(1), 127–164. https://doi.org/10.1177/0149206319878254

Brown, T. A. (2015). *Confirmatory factor analysis for applied research* (2nd ed.). Guilford Press.

Dikmen, M., & Tuncer, M. (2017). Scholar's perceptions and struggle methods against cyberbullying. *Dicle University Journal of Ziya Gökalp Faculty of Education, 31*, 675–686. https://doi.org/10.14582/DUZGEF.1806

Fabrigar, L. R., & Wegener, D. T. (2011). *Exploratory factor analysis.* Oxford University Press.

Freeman, D., & Freeman, J. (2008). *Paranoia: The 21st century fear.* Oxford University Press.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39–50. https://doi.org/10.2307/3151312

Gençöz, T. (1998). Fear: Causes, consequences and ways to deal with. *Crisis Journal, 6*(2), 9–16. https://doi.org/10.1501/Kriz_0000000068

Hofstede, G. (2001). *Culture's consequences: Comparing values, behaviors, institutions, and organizations across nations* (2nd ed.). Sage.

Jolliffe, I. T., & Cadima, J. (2016). Principal component analysis: a review and recent developments. *Philos Trans A Math Phys Eng Sci. 374*(2065), 20150202. https://doi.org/10.1098/rsta.2015.0202

Kaya, A. Y., & Ata, F. (2022). New media and digital paranoia: Extreme skepticism in digital communication. In H. Aker ,& M. Aiken (Eds.), *Handbook of research on cyberchondria, health literacy, and the role of media in society's perception of medical information* (pp. 330–343). IGI Global. https://doi.org/10.4018/978-1-7998-8674-7.ch020

Kayış, A. (2010). Reliability analysis. In Ş. Kalaycı (Ed.), *SPSS applied multivariate statistical techniques* (pp. 404–419). Asil Publishing.

Keles, B., McCrae, N., & Grealish, A. (2020). A systematic review: The influence of social media on depression, anxiety and psychological distress in adolescents. *International Journal of Adolescence and Youth, 25*(1), 79-93. https://doi.org/10.1080/02673843.2019.1590851

Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth. *Psychological Bulletin, 140*(4), 1073–1137. https://doi.org/10.1037/a0035618

Lam, L. W. (2012). Impact of competitiveness on salespeople's commitment and performance. *Journal of Business Research, 65*(9), 1328–1334. https://doi.org/10.1016/j.jbusres.2011.10.026

Laplante, P., & DeFranco, J. (2010). Another ode to paranoia. *IT Professional, 12*(3), 57–59. https://doi.org/10.1109/MITP.2010.82

MacManus, S. A., Caruson, K., & McPhee, B. D. (2013). Cybersecurity at the local government level: Balancing demands for transparency and privacy rights. *Journal of Urban Affairs, 35*(4), 451–470. https://doi.org/10.1111/j.1467-9906.2012.00640.x

Mason, O. J., Stevenson, C., & Freedman, F. (2014). Ever-present threats from information technology: The cyber-paranoia and fear scale. *Frontiers in Psychology, 5*, 1298. https://doi.org/10.3389/fpsyg.2014.01298

Nicholas, D., Rodríguez-Bravo, B., Watkinson, A., Boukacem-Zeghmouri, C., Herman, E., Xu, J., Abrizah, A., & Świgoń, M. (2017). Early career researchers and their publishing and authorship practices. *Learned Publishing, 30*(3), 205–217. https://doi.org/10.1002/leap.1102

Polst, S., Kelbert, P., Feth, D. (2019). Company Privacy Dashboards: Employee Needs and Requirements. In: Moallem, A. (eds) HCI for Cybersecurity, Privacy and Trust. HCII 2019. Lecture Notes in Computer Science, vol 11594. Springer, Cham. https://doi.org/10.1007/978-3-030-22351-9_29

Rajmohan, S. (2016). Hyper vigilance and paranoia: Problematizing self on social media. *Literary Endeavour, 7*(1), 43–49.

Rilho, A. M. V. (2019). *Nothing to hide, nothing to fear: The moderating effect of fear on AI empowered technology intention of use* [Master's thesis, University Institute of Lisbon]. ISCTE Repository. https://repositorio.iscte-iul.pt/handle/10071/19489

Schuett, R. (2020, September 4). *Fear and Freud in politics: Critical notes on Mearsheimer's structural realism.* E-International Relations. https://www.e-ir.info/2020/09/04/fear-and-freud-in-politics-critical-notes-on-mearsheimers-structural-realism/

Shahid, M. (2021). *The effect of perceptions about internet privacy concerns on cyber paranoia and cyber fear* [Unpublished master's thesis], Forman Christian College.

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, 8*(2), 23–74. https://doi.org/10.23668/psycharchives.12784

Statham, V., Emerson, L. M., & Rowse, G. (2019). A systematic review of self-report measures of paranoia. *Psychological Assessment, 31*(2), 139–158. https://doi.org/10.1037/pas0000645

Şahin, M. (2019). Fear, anxiety and anxiety disorders. *Eurasian Journal of Researches in Social and Economics (EJRSE), 6*(10), 117–135.

Veliz, C. (2021). Privacy and digital ethics after the pandemic. *Nature Electronics. 4*(1), 10-11. https://doi.org/10.1038/s41928-020-00536-y

Wright, M. F. (2016). Cybervictims' emotional responses, attributions, and coping strategies for cyber victimization: A qualitative approach. *Safer Communities, 15*(3), 160–169. https://doi.org/10.1108/SC-03-2016-0006

Zimaitis, I., Degutis, M., & Urbonavicius, S. (2020). Social media use and paranoia: Factors that matter in online shopping. *Sustainability, 12*(3), 1–10. https://doi.org/10.3390/su12030904

Zorlu, F., & Ünübol, H. (2018). The multidimensional orientation toward dying and death inventory: Validity and reliability in a Turkey sample. *Anatolian Journal of Psychiatry, 19*(2), 39–46. https://doi.org/10.5455/apd.300390

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Public Affairs.

Addition

Siber Paranoya ve Korku Ölçeği	Kesinlikle Katılmıyorum	Biraz Katılmıyorum	Biraz Katılıyorum	Kesinlikle Katılıyorum
1. Bilgisayar kullanımının artması çocukların beyinlerini olumsuz yönde etkiliyor.				
2. Küresel internetin korkunç sonuçlar doğurarak yakın zamanda çökeceğini düşünüyorum.				
3. Bilgilerimin başkalarının eline geçmemesi için kişisel konularda mümkün olduğunca internet kullanmaktan kaçınırım.				
4. Sosyal medya hesaplarımın (Facebook, instagram, vb) iznim olmadan başkaları tarafından düzenlemesinden endişe duyuyorum.				
5. Cep telefonları/baz istasyonlarının yaydığı elektromanyetik dalgaların etkilerinden endişe duyuyorum.				
6. Teröristler interneti kullanarak halka yönelik terör saldırı planları için yeni yollar bulurlar.				
7. Ödeme kartları (kredi kartı, alışveriş kartı, vb.) görevlilerin seyahatlerimi ve alışverişlerimi izlemesine olanak tanır.				
8. Müşteriler hakkında veri depolayan şirketler, özel bilgilerimin çalınmasına karşı çok savunmasızdır.				
9. İnsanların teknoloji kullanımlarından kaynaklanan tehditler konusunda yeterince endişe duymadığını düşünüyorum.				
10. İnsanların akıllı telefonlar aracılığıyla hareketlerinin izlenebileceği konusunda endişe duymaları gerektiğini düşünüyorum.				
11. Kapalı devre televizyon kameraları (CCTV), insanları izlemek için yasadışı olarak kullanılır.				