



**T.C.
AMASYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ**

**ORTAOKUL ÖĞRENCİLERİNİN SİBER GÜVENLİK
FARKINDALIKLARININ BELİRLENMESİ**

YÜKSEK LİSANS TEZİ

FIRAT YILMAZ

OCAK

FIRAT YILMAZ

**BİLGİSAYAR VE ÖĞRETİM
TEKNOLOJİLERİ EĞİTİMİ
ANABİLİM DALI**

OCAK 2023

**ORTAOKUL ÖĞRENCİLERİNİN SİBER GÜVENLİK
FARKINDALIKLARININ BELİRLENMESİ**

Fırat YILMAZ

YÜKSEK LİSANS TEZİ

Danışman

Dr. Öğretim Üyesi Aslıhan İSTANBULLU

**AMASYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ**

OCAK 2023

Yüksek Lisans Tezi Kabul ve Onay Sayfası

Fırat YILMAZ tarafından hazırlanan “Ortaokul Öğrencilerinin Siber Güvenlik Farkındalıklarının Belirlenmesi” adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ ile Amasya Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalında YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Danışman: Dr. Öğr. Üyesi Aslıhan İSTANBULLU

Bilgisayar Teknolojileri Anabilim Dalı, Amasya Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum.

Başkan : Doç. Dr. Volkan KUKUL

Öğretim Teknolojileri Anabilim Dalı, Amasya Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum.

Üye : Dr. Öğr. Üyesi Şirin KÜÇÜK AVCI

Eğitim Programları ve Öğretimi Dalı, Akdeniz Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum.

Tez Savunma Tarihi: 25/01/2023

Jüri tarafından kabul edilen bu tezin Yüksek Lisans Tezi olması için gerekli şartları yerine getirdiğini onaylıyorum.

.....

Doç. Dr. Ümit YILDIRIM

Fen Bilimleri Enstitüsü Müdürü

ETİK BEYAN

Amasya Üniversitesi Fen Bilimleri Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmada;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmada yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Fırat YILMAZ

25/01/2023

**ORTAOKUL ÖĞRENCİLERİNİN SİBER GÜVENLİK FARKINDALIKLARININ
BELİRLENMESİ
(Yüksek Lisans Tezi)**

Fırat YILMAZ

AMASYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
Ocak 2023

ÖZET

İnsanlar günümüzde teknolojiye her zamankinden daha fazla bağımlı hale gelmiş bulunmaktadır. Toplumun modern gelişmelere ilişkin olumlu algısına rağmen, teknolojinin getirdiği siber güvenlik tehditleri de gerçek bir tehlikedir. Pandemi dönemi bilgi ve iletişim teknolojilerinin kullanımının artmasıyla birlikte siber saldırı sayısı da artmıştır. Yaşı ne olursa olsun tüm kullanıcılar internette zaman geçirirken çeşitli güvenlik risklerine maruz kalmaktadır. Bu risklere en fazla maruz kalan son kullanıcılar ise özellikle küçük yaşta kullanıcılarıdır. Bu nedenle kullanıcıların erken yaşta siber güvenlik farkındalığı kazanması oldukça önemlidir. Küçük yaşta kullanıcıların mevcut siber güvenlik farkındalıklarını analiz etmek için siber güvenlik farkındalığı ölçeğine ihtiyaç duyulmaktadır. Bu ihtiyaç doğrultusunda ortaokul öğrencilerinin siber güvenlik farkındalık düzeylerini belirlemeye yönelik ölçek geliştirmek ve farklı değişkenler açısından siber güvenlik farkındalıklarını incelemek amaçlanmıştır. Araştırma iki aşamadan oluşmaktadır. İlk aşamada ortaokul öğrencilerine yönelik siber güvenlik farkındalığı ölçeği geliştirilmiştir. Ölçek geliştirme sürecinde nicel araştırma yöntemlerinden olan tarama yöntemi kullanılmıştır. Araştırmanın çalışma grubunu 2021-2022 eğitim öğretim yılında Amasya ili Millî Eğitim Bakanlığı'na bağlı ortaokullarda öğrenim gören 1.456 öğrenci oluşturmaktadır. 854 kişiye yönelik yapılan Açıklayıcı Faktör Analizi sonucunda ölçeğin 25 madde ve 4 alt boyuttan (Şifre Güvenliği, Önleyici Tedbirler, Kötü Amaçlı Yazılım Farkındalığı ve Kişisel Gizliliği Koruma) oluştuğu belirlenmiştir. 602 kişi üzerinde yapılan doğrulayıcı faktör analizi sonucunda ise 4 faktörlü yapı doğrulanmıştır. Ölçeğin tamamına ilişkin Cronbach'ın alfa değeri 0,87 olmakla birlikte Şifre Güvenliği Alt Boyutu 0,92, Önleyici Tedbirler Alt Boyutu 0,82, Kötü Amaçlı Yazılım Farkındalığı Alt Boyutu 0,85 ve Kişisel Gizliliği Koruma Alt Boyutu 0,83' tür. Araştırmanın ikinci aşamasında ortaokul öğrencilerinin siber güvenlik farkındalıkları farklı değişkenler açısından incelenmiştir. Araştırmanın çalışma grubunu 2022-2023 eğitim öğretim yılında Amasya ili Millî Eğitim Bakanlığı'na bağlı ortaokullarda öğrenim gören 530 öğrenci oluşturmaktadır. Araştırma modeli olarak betimsel tarama modeli kullanılmıştır. Araştırma sonucu elde edilen veriler üzerinde siber güvenlik farkındalıklarının cinsiyet değişkenine göre incelenmesinde bağımsız t-testi, sınıf düzeylerine ve günlük internet kullanım sürelerine göre incelenmesinde ANOVA testi uygulanmıştır. Önleyici Tedbirler alt boyutunda cinsiyete göre farkların istatistiksel olarak erkek öğrenciler lehine anlamlı bulunmuş, sınıf düzeyinde 8'inci ve 6'ncı sınıflar arasında anlamlı bir fark olduğu tespit edilmiştir.

Sayfa Adedi : 105
Anahtar Kelimeler : Siber güvenlik, Ortaokul, Ölçek
Danışman : Dr. Öğr. Üyesi Aslıhan İSTANBULLU

DETERMINING THE CYBER SECURITY AWARENESS OF SECONDARY STUDENTS A SCALE DEVELOPMENT STUDY

(M. Sc. Thesis)

Fırat YILMAZ

AMASYA UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

January 2023

ABSTRACT

Today, people have become more dependent on technology than ever before. Despite society's positive perception of modern developments, cybersecurity threats brought by technology are also a real danger. With the increase in the use of information and communication technologies during the pandemic period, the number of cyber attacks has also increased. Regardless of age, all users are exposed to various security risks while spending time on the Internet. The end users who are most exposed to these risks are especially young users. For this reason, it is very important for users to gain cybersecurity awareness at an early age. A cyber security awareness scale is needed to analyze the current cyber security awareness of young users. In line with this need, it was aimed to develop a scale to determine the cyber security awareness levels of secondary school students and to examine their cyber security awareness in terms of different variables. The research consists of two stages. In the first stage, a cyber security awareness scale was developed for secondary school students. In the scale development process, the survey method, which is one of the quantitative research methods, was used. The study group of the research consists of 1,456 students studying in secondary schools affiliated to the Ministry of National Education in Amasya in the 2021-2022 academic year. As a result of the Exploratory Factor Analysis conducted for 854 people, it was determined that the scale consisted of 25 items and 4 sub-dimensions (Password Security, Preventive Measures, Malware Awareness and Protection of Personal Privacy). As a result of the confirmatory factor analysis performed on 602 people, the 4-factor structure was confirmed. While Cronbach's alpha value for the entire scale is 0.87, Password Security Sub-Dimension is 0.92, Preventive Measures Sub-Dimension is 0.82, Malware Awareness Sub-Dimension is 0.85, and Personal Privacy Protection Sub-Dimension is 0.83. In the second stage of the study, the cyber security awareness of secondary school students was examined in terms of different variables. The study group of the research consists of 530 students studying in secondary schools affiliated to the Ministry of National Education in the province of Amasya in the 2022-2023 academic year. The descriptive survey model was used as the research model. The independent t-test was used to analyze the cyber security awareness according to the gender variable on the data obtained as a result of the research, and the ANOVA test was applied to the analysis according to the class levels and daily internet usage times. In the Preventive Measures sub-dimension, the differences by gender were found to be statistically significant in favor of male students, and a significant difference was found between the 8th and 6th grades at the grade level.

Number of pages : 105

Keywords : Cybersecurity, Middle school, Scale

Supervisor : Asst. Prof. Dr. Aslıhan İSTANBULLU

ÖN SÖZ ve TEŞEKKÜR

Çalışma sürecinin başından itibaren değerli bilgi ve katkılarıyla bana yol gösteren tez danışmanım Dr. Öğr. Üyesi Aslıhan İSTANBULLU' ya teşekkürlerimi sunarım.

Görüş ve önerilerini benimle paylaşan, bilgi ve deneyimlerinden yararlandığım kıymetli mesai arkadaşım Dr. Selma KAYA'ya çok teşekkür ederim.

Bu zorlu süreçte benimle aynı heyecanı paylaşan ve bana olan inançları ile beni her daim cesaretlendiren eşim Dr. Öğr. Üyesi Ece AVULOĞLU YILMAZ ve kızım Deniz Ela YILMAZ' a sevgi ve minnetlerimi sunarım.



İÇİNDEKİLER

Sayfa

ÖZET	iv
ABSTRACT	v
ÖN SÖZ ve TEŞEKKÜR.....	vi
İÇİNDEKİLER	vii
ÇİZELGELER DİZİNİ	x
ŞEKİLLER DİZİNİ.....	xii
SİMGELER VE KISALTMALAR DİZİNİ	xiii
1. GİRİŞ	1
1.1. Problem Durumu	1
1.2. Araştırmanın Amacı.....	6
1.3. Araştırma Soruları	6
1.4. Araştırmanın Önemi	6
1.5. Araştırmanın Sınırlılıkları.....	10
1.6. Araştırma Varsayımları	10
2. KURAMSAL ÇERÇEVE	11
2.1. Siber Uzay	11
2.2. Siber Güvenlik.....	14
2.2.1. Siber güvenlik ile ilgili kavramlar	17
2.2.2. Bilgi güvenliği üçlüsü (CIA).....	18
2.2.3. Parker altılısı (parkerian hexad).....	20
2.3. Siber Saldırı	23
2.3.1. Siber saldırı türleri	24
2.4. Siber Güvenlik Farkındalığı	29
2.5. Çocuklarda Siber Güvenlik Farkındalığı	32
2.5.1. Çocuklara yönelik siber tehditler.....	35

Sayfa

2.5.2. Çocuklara yönelik siber güvenlik farkındalığı çalışmaları.....	36
3. YÖNTEM	41
3.1. Siber Güvenlik Farkındalığı Ölçek Geliştirme Çalışması	41
3.1.1. Araştırma modeli	41
3.1.2. Evren ve örneklem.....	41
3.1.3. Veri toplama araçları.....	46
3.1.4. Verilerin toplanması	49
3.1.5. Verilerin analizi.....	50
3.2. Ölçek Uygulama Çalışması	50
3.2.1. Araştırmanın modeli.....	51
3.2.2. Evren ve örneklem.....	51
3.2.3. Çalışma grubu.....	51
3.2.4. Veri toplama aracı.....	53
3.2.5. Verilerin analizi.....	54
4. BULGULAR.....	56
4.1. SGFÖ Geçerli midir?.....	56
4.1.1 SGFÖ' nün kapsam geçerliği	56
4.1.2. SGFÖ' nün yapı geçerliği.....	56
4.1.3. Açımlayıcı faktör analizi (AFA).....	57
4.1.4. AFA örneklem büyüklüğü	57
4.1.5. AFA kayıp verilerin temizlenmesi	59
4.1.6. Doğrusallık, normallik ve uç değerler.....	59
4.1.7. AFA bulguları.....	61
4.1.8. Doğrulayıcı faktör analizi (DFA)	66
4.1.9. Doğrulayıcı faktör analizi ön deneme uygulama ve veri toplama süreci	66

Sayfa

4.1.10. Modelin betimlenmesi.....	67
4.1.11. Modelin tanımlanması.....	67
4.1.12. Model uyumunun incelenmesi.....	67
4.2. Siber Güvenlik Farkındalığı Ölçeği Güvenirlik Ölçütlerini Karşılammakta mıdır?.....	72
4.2.1. Ölçeğin kullanımı	72
4.3. SGFÖ'nün Uygulanmasına İlişkin Bulgular	73
4.3.1. Cinsiyet değişkenine yönelik bulgular	74
4.3.2. Sınıf düzeyi değişkenine yönelik bulgular	74
4.3.3. İnternet ve bilişim teknolojileri kullanım sürelerine göre Anova testi sonuçları.....	76
5. SONUÇ, TARTIŞMA VE ÖNERİLER.....	78
5.1. Sonuç ve Tartışma	78
5.1.1. Birinci alt probleme ilişkin sonuçlar ve tartışma.....	78
5.1.2. İkinci alt probleme ilişkin sonuçlar ve tartışma.....	79
5.1.3. Üçüncü alt probleme ilişkin sonuçlar ve tartışma	80
5.2. Öneriler	84
5.2.1. Uygulamaya yönelik öneriler	84
5.2.2. Araştırmaya yönelik öneriler.....	84
KAYNAKLAR	85
EKLER	97
ÖZGEÇMİŞ	105

ÇİZELGELER DİZİNİ

Çizelge	Sayfa
Çizelge 2.1. Öğrencilerin siber dünyada karşılaştığı tehlikeler	36
Çizelge 3.1. Amasya ili 5, 6, 7 ve 8'inci sınıf öğrenci sayıları.....	42
Çizelge 3.2. Çalışma grubu okul ve sınıf bilgisi	42
Çizelge 3.3. Çalışma grubu cinsiyet dağılımı	43
Çizelge 3.4. Çalışma grubu teknolojik ürün sahipliği.....	43
Çizelge 3.5. Çalışma grubu teknolojik ürün dağılımı	44
Çizelge 3.6. Çalışma grubu internete erişim yöntemi.....	44
Çizelge 3.7. Çalışma grubu günlük internet kullanım süreleri	45
Çizelge 3.8. Çalışma grubu internet kullanım alanları	45
Çizelge 3.9. Ölçek geliştirme aşamaları	47
Çizelge 3.10. Çalışma grubu demografik özellikler	52
Çizelge 3.11. SGFÖ'nün güvenilirlik değerleri.....	53
Çizelge 3.12. Basıklık ve çarpıklık değerleri.....	54
Çizelge 3.13. Uygulanan parametrik testler çizelgesi.....	54
Çizelge 4.1. AFA örneklem büyüklüğü	58
Çizelge 4.2. KMO Referans Aralıkları	58
Çizelge 4.3. KMO ölçüm değerleri.....	59
Çizelge 4.4. Basıklık ve çarpıklık değerleri.....	59
Çizelge 4.5. Madde-ölçek korelasyon katsayısı analiz sonuçları	61
Çizelge 4.6. Faktör analizi sonuçları (döndürülmüş temel bileşenler analizi sonuçları)	64
Çizelge 4.7. Ölçek boyutları ve açıklanan varyans değerleri.....	65
Çizelge 4.8. Siber güvenlik ölçeğini oluşturan faktörler arasındaki korelasyon katsayısı ..	65
Çizelge 4.9. DFA sonuçları.....	68
Çizelge 4.10. DFA için uyum indeksleri	70

Çizelge	Sayfa
Çizelge 4.11. Siber güvenlik farkındalığı ölçeğinde yer alan maddelere ait t değerleri.....	70
Çizelge 4.12. SGFÖ güvenirlik katsayısı değerleri	72
Çizelge 4.13. Ölçek puan hesaplama tablosu.....	73
Çizelge 4.14. SGFÖ toplam puan yorum çizelgesi.....	73
Çizelge 4.15. Cinsiyet değişkenine göre T testi sonuçları	74
Çizelge 4.16. SGFÖ sınıf düzeyi değişkenine göre Anova testi sonuçları	75
Çizelge 4.17. Sınıf değişkenine göre kişisel gizliliği koruma faktörü Tukey testi sonuçları	76
Çizelge 4.18. İnternet ve bilişim teknolojileri kullanma sürelerine göre Anova testi sonuçları.....	77

ŞEKİLLER DİZİNİ

Şekil	Sayfa
Şekil 1.1. 2011-2021 yılları arasında internet erişim imkânı ve bireylerde internet kullanımı.....	2
Şekil 1.2. 2004-2021 yılları arasında bilgisayar güvenliği, internet güvenliği, bilgi güvenliği ve siber güvenlik terimlerinin ne sıklıkla arandığına dair grafik.	2
Şekil 2.1. Genel siber uzay mekanları	14
Şekil 2.2. CIA üçlemesi	19
Şekil 2.3. Parker altılısı	21
Şekil 3.1. Ölçek geliştirme aşamaları.	46
Şekil 4.1. Normal dağılım grafiği	60
Şekil 4.2. Genel ortalama Zscore uç değerleri.....	60
Şekil 4.3. Faktör saçılım grafiği.....	63
Şekil 4.4. Birinci düzey doğrulayıcı faktör analizi	69
Şekil 4.5. İkinci düzey doğrulayıcı faktör analizi	71

SİMGELER VE KISALTMALAR DİZİNİ

Bu çalışmada kullanılmış bazı simgeler ve kısaltmalar, yanda açıklamaları verilmek üzere aşağıda listelenmiştir.

Kısaltmalar	Açıklama
SG	Siber güvenlik
MEB	Millî eğitim bakanlığı
YÖK	Yüksek öğrenim kurumu
PST	Physical-social-thinking spaces (Fiziksel, sosyal ve düşünme Alanı)
ABD	Amerika birleşik devletleri
MITM	Man-in-the-middle attacks (Ortadaki adam saldırısı)
SGFÖ	Siber güvenlik farkındalık ölçeği
IOT	Internet of things (Nesnelerin interneti)
BGD	Bilgi güvenliği derneği
TBD	Türkiye bilişim derneği
CPS	Cyber-physical systems (Siber fiziksel sistem)
PC	Personal computer (Kişisel bilgisayar)
DDOS	Distributed denial of service (Dağıtık hizmet reddi saldırıları)

1. GİRİŞ

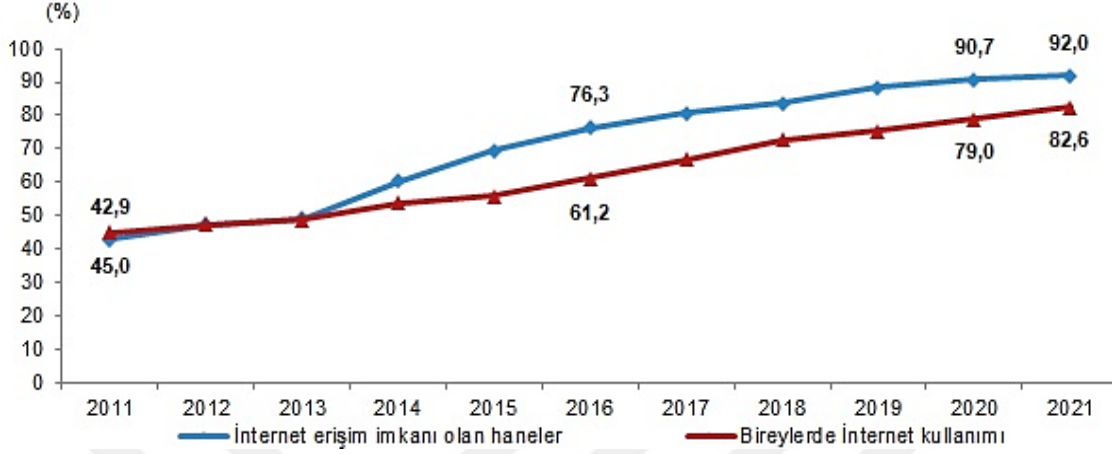
Bu bölümde problem durumu, araştırmanın amacı, araştırma sorular, araştırmanın önemi, araştırmanın sınırlılıkları ve araştırma varsayımları açıklanmıştır.

1.1. Problem Durumu

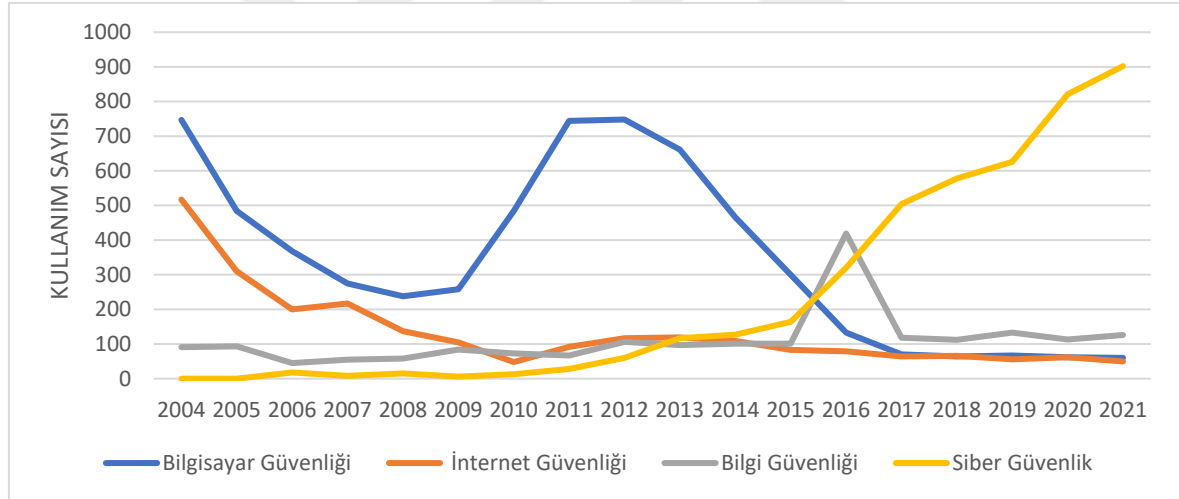
Son 20 yıl içinde nesnelerin interneti (Internet of Things), bulut sistemleri, yapay zekâ vb. teknolojiler sayesinde gün içinde kullandığımız cihazlar (mutfak aletleri, arabalar, termostatlar, saatler vb.) gömülü sistemler aracılığıyla internete bağlanabilmektedir. Bu sayede insanlar, süreçler ve cihazlar arasında dijital verinin üretilmesi, işlenmesi, kaydedilmesi, depolanması ve dağıtılması sağlanmaktadır. Dijital veri biçimleri günümüz dünyasında benzeri görülmemiş bir ölçekte üretilmekte ve işlenmektedir (Selwyn, 2015). Cihazların birbirleriyle haberleşmeleri ve verilerin dijital olarak işlenmesi son kullanıcılar için kolaylık sağlasa da ağa bağlı cihazların sayısının artması ve cihazlar arasında daha fazla dijital veri paylaşılması, verilerin çalınması, değiştirilmesi ya da paylaşılması olasılığını da artırmaktadır. İnternette yapılan her işlemin ardında zamanla biriken bir veri izi bıraktığı dikkate alındığında, siber güvenlik tehdidinin ne kadar büyük olduğu da ortaya çıkmaktadır. Bu nedenle ağların ve dijital verilerin korunmasına ihtiyaç duyulmaktadır. Ülkemizde elektronik cihaz ve internet kullanımı günden güne artış göstermiştir. Özellikle Covid salgını sonrasında acil uzaktan eğitime geçiş sağlanarak hemen hemen her yaştan çok sayıda öğrenci internete bağlanmıştır (UNESCO, 2020). Sağlık, ticaret, turizm vb. birçok alanda çalışan kurumlar, kuruluşlar, şirketler evden çalışma uygulamasına geçmiş ve bu durumda internet ve elektronik cihaz kullanımını artırmıştır. Şekil 1’ de sunulan Türkiye İstatistik Kurumunun (TÜİK) 2021 yılı verilerine göre internet erişimi olan hane sayısı 2011 yılında %45 iken on yılda %47 artışla %92 seviyesine ulaşmıştır. Bireylerde internet kullanımı 2011 yılında %42,9 iken yaklaşık %40 artış göstererek 2021 yılında %82,6 seviyesine ulaşmıştır.

Elektronik cihaz ve internet kullanımı günlük hayatımızı kolaylaştırır da verilerimizin güvenliği açısından ciddi riskler oluşturmaktadır. Kullanıcıların internet ortamında karşılaştıkları ihlal ve riskler yıllara ve değişen teknoloji nedeniyle farklı tanımlamalarda bulunulmuştur. 2004-2010 yılları arasında yaşanan bu ihlaller bilgi güvenliği ve bilgisayar güvenliği kavramları kullanılmış, 2016 yılında Siber Güvenlik (Cyber Security) kavramının

kullanımıyla birlikte diğer kavramların kullanımında azalma görülmüştür. 2021 yılı itibariyle alana hâkim kavram siber güvenlik olmuştur (İstanbulu, 2023).



Şekil 1.1. 2011-2021 yılları arasında internet erişim imkânı ve bireylerde internet kullanımı



Şekil 1.2. 2004-2021 yılları arasında bilgisayar güvenliği, internet güvenliği, bilgi güvenliği ve siber güvenlik terimlerinin ne sıklıkla arandığına dair grafik.

2004 ve 2010 yıllarında en sık “Information Security (Bilgi Güvenliği)” ve “Computer Security (Bilgisayar Güvenliği)” kelimelerinin kullanıldığı görülmektedir. 2016 yılında “Cyber Security (Siber Güvenlik)” kelime kullanımında artışla birlikte “Information Security (Bilgi Güvenliği)” kullanımında azalma olduğu, yine de en fazla kullanılan kelimeler olduğu görülmektedir. 2021 yılının sonunda ise “cyber security (siber güvenlik)” kelime kullarımdaki ciddi artışla birlikte, en sık kullanılan kelime olduğu görülmektedir. Bu nedenle bu çalışmada siber güvenlik kavramı tercih edilmiştir.

Literatürde siber güvenlik kavramına karşılık çevrimiçi güvenlik, internet güvenliği gibi terimler kullanılmakta internet ortamındaki güvenlik endişelerini belirtmek için birbirlerinin yerine kullanılmaktadır (Quayyum, Cruzes ve Jaccheri, 2021). Siber güvenlik, internet güvenliği, bilgi güvenliği ve bilgisayar güvenliği ile ilişkilendirilen genel bir terimdir. Ancak kapsamı, uygulamayı ve doğru kullanımını anlamak önemlidir. Siber güvenlik, birçok kişi tarafından yanlış anlaşıldığı gibi, bilgisayarların sadece internet üzerindeki güvenliğini sağlamakla sınırlı değildir (Singer ve Friedman, 2014). Siber güvenlik, donanım, yazılım, veri ve bilgilerin her türlü ihlalden korunması olarak tanımlanabilir. Siber güvenlik, veri koruma ve bilgi güvenliğinin uygulanması için kurum ve kuruluşlar için en yüksek önceliği, bireyler için ise gizlilik, erişim kontrolü ve güvenlik olarak tanımlanabilir (Tirumala, Sathu ve Naidu, 2015; Toch ve diğerleri, 2018). Şu anda, siber güvenliğin kapsamı, bireyleri siber zorbalığa karşı korumaya ve gelişmiş makine öğrenimi teknikleri kullanarak siber savaşı tanımlamaya yönelik olarak genişletilmiştir (Blanke, Nielsen ve Wrozek, 2022; Tirumala, Valluri ve Babu, 2019).

Dünyada siber güvenliğin sağlanmasına yönelik gerek devlet gerekse özel sektör tarafından ayrılan yüksek bütçe ve geliştirilen güvenlik önlemlerine rağmen siber saldırıların sayısı her geçen yıl artmaktadır. Donanım ve yazılım alanına yönelik güvenlik teknolojilerindeki gelişmeler sıradan kullanıcılar kaynaklı siber güvenlik ihlallerinin önüne geçilmesine imkân tanımamaktadır. Yapılan araştırmalar sonucu çoğu güvenlik ihlallerinin sıradan kullanıcılar olduğu tespit edilmiştir (Tuğal, Almaz ve Sevi, 2021). Sistemler donanım ve yazılımsal olarak güvenli olsa da siber saldırılara neden olan ihlallerin büyük bir kısmı "Son Kullanıcı Hatası" nedeniyle ortaya çıkmaktadır (Cooke, 2020). Yaşanan güvenlik açıklarının %80' ini son kullanıcı hataları oluştururken siber güvenlik faaliyetleri sistem araçları ve teknolojiyi geliştirmek üzerine olmuştur. Hükümetler ve şirketler teknolojik olarak en güvenilir siber savunma teknolojilerine sahip olsa dahi, son kullanıcı hatası, kişisel siber güvenlik bilgisi ve farkındalık eksikliği nedeniyle birçok kayıp yaşanmasının önüne geçememektedirler. Dolayısıyla kullanıcıların gizlilik ve güvenlik risklerini ve kendilerini siber saldırılardan nasıl koruyacaklarını anlamaları modern yaşamda temel bir ihtiyaçtır.

Son kullanıcılar elektronik cihazları kullanabilen her yaştan insanı kapsamaktadır. Son kullanıcılar arasından en tecrübesiz ve tehlikelere en açık olan grubun çocuklar olduğunu söylemek mümkündür. Günümüzde çocukların çeşitli sosyal ağ sitelerini kullanarak, çevrimiçi bilgisayar oyunları oynayarak, evde eğitim yazılımlarını ve diğer çevrimiçi

uygulamaları kullanarak başkalarıyla iletişim kurması yaygınlaşmıştır (Lobe, Velicu, Staksrud, Chaudron ve Di Goia, 2021; Kristjánsson, Gardner, ve Chiribella 2021). Bu sayede dünyaya ilişkin anlayışlarını internet ortamında geliştirebilir ancak kişisel verilerin yayınlanmasıyla bağlantılı riskleri belirleyecek ve zararların sonuçlarını değerlendirecek dijital okuryazarlığa sahip olmayabilirler (Dempsey, Sim, Cassidy, ve Ta, 2022). Yaşları göz önüne alındığında, internet ve dijital sistemleri kullanmanın fırsatlarını ve risklerini değerlendirmeleri zordur, hatta hayatlarının giderek daha fazla kısmı dijital olarak kaydedildiğinden bu durum onların mahremiyetleri ve güvenlikleri üzerinde uzun vadeli etkiler yaratabileceğinin farkına varamayabilirler (Hourcade 2008). Çocukların bu süreçleri nasıl algıladıkları ve dijital veri üretiminin doğasında bulunan gizlilik risklerine ilişkin görüşleri literatürde sınırlıdır (Süss, Lampert ve Trültzsch-Wijnen 2018). Çocuklar söz konusu olduğunda, siber güvenlik, onları etkileyebilecek tüm çevrimiçi risklerle ve çocukların çeşitli siber güvenlik riskleri hakkında sahip oldukları farkındalık da dâhil olmak üzere onları ve aileleri desteklemek için alınan önlemlerle ilgilidir (Quayyum ve diğerleri 2021).

Siber güvenlik farkındalığı, “internet kullanıcılarını çeşitli siber tehditlere ve bilgisayarların ve verilerin bu tehditlere karşı savunmasızlığına karşı duyarlı olmaları için eğiten bir metodoloji” olarak tanımlanmaktadır (Abd Rahim, Hamid, Kiah, Shamshirband ve Furnell, 2015). Shaw, Chen, Harris ve Huang (2009) siber güvenlik farkındalığını “kullanıcıların bilgi güvenliğinin önemini, kuruluşun verilerini ve ağ sistemlerini güvende tutmak için yeterli düzeyde bilgi kontrolü uygulama sorumluluklarını anlama derecesi” olarak tanımlamıştır. Yukarıdaki tanımlara dayanarak, siber güvenlik farkındalığının iki temel amacı vardır: son kullanıcıları siber güvenlik riskleri hakkında uyarmak ve siber güvenlik risklerini anlamalarını, internet kullanımı sırasında güvenliği benimsemeye yeterince adanmak için geliştirmektir. Son kullanıcıdan kaynaklı hataların veya güvenlik açıklarının azaltılması, güvenliğin kişisel veya kurumsal düzeyde iyileştirilmesinde kilit bir faktördür (Giannakas, Papasalouros, Kambourakis ve Gritzalis, 2019). Bu nedenle siber güvenlik hakkında kullanıcı farkındalığının artması gereklidir.

Ülkemizde siber güvenlik ile ilgili olarak Millî Eğitim Bakanlığı (MEB) ve Yüksek Öğretim Kurumuna (YÖK) bazı müfredatlarında yer vermelerine rağmen yeterli düzeyde olmadığı düşünülmektedir (Tavlaş, 2021). MEB müfredatı incelendiğinde Bilişim Teknolojileri ve Yazılım Dersi Öğretim Programında “Etik ve Güvenlik” başlığı altında, beşinci sınıf

düzeyinde Bilişim Teknolojileri ve Yazılım Dersi Öğretim Programında “Etik ve Güvenlik” konusu altında bahsedilmekte, altıncı sınıf düzeyinde “Etik Değerler”, “Dijital Vatandaşlık” ve “Gizlilik ve Güvenlik” konu başlıkları altında incelenmektedir. Ortaokul düzeyinde siber güvenlik konularını içeren Bilişim Teknolojileri Yazılım dersi MEB Talim ve Terbiye Kurulu Başkanlığının (TTKB) 23/12/2021 tarihli ve 49 sayılı kararı doğrultusunda 5’inci ve 6’ıncı sınıflarda haftada sadece 2 saat işlenmektedir. Ortaöğretim seviyesinde Bilgisayar Bilimi Dersi Öğretim Programında “Etik, Güvenlik, Toplum” konusu olarak yer almaktadır. Bilgisayar Bilimi Dersi TTKB’nin 19.01.2018 tarih ve 23 sayılı karar ile kabul edilen öğretim programı uygulanmakta okul türlerine göre farklılık göstermekle birlikte haftada 2 saat işlenmektedir. YÖK’ e bağlı eğitim kurumlarında lisans ve ön lisans düzeyinde yeterli siber güvenlik eğitimleri verilmese de yüksek lisans ve doktora seviyesinde siber güvenliğe yönelik eğitimler bulunmaktadır. Üniversiteler arasında “Siber Güvenlik” ve “Bilgi Güvenliği” isimleri taşıyan yüksek lisans ve doktora programları bulunmaktadır (Önaçan ve Atan, 2016). Bunun haricinde siber güvenlik eğitimi veren çeşitli kurum ve kuruluşlar vardır. Bilgi Güvenliği Derneği (BGD), Türkiye Bilişim Derneği (TBD) sivil toplum kuruluşları (STK) ya da özel kuruluşlar tarafından da verilen bu eğitimler kullanıcılarda bu farkındalığın oluşturulması ve toplumun geneline yayılması için en önemli destek sağlar. Ancak son kullanıcıların (özellikle çocukların) siber güvenliğin öneminin farkında olmaları ve bu eğitimlere katılması mümkün gözükmemektedir. Bu nedenler siber güvenlik alanında farkındalık ve eğitim çalışmalarına ilkokuldan itibaren başlanılmalı ve eğitim sisteminin her kademesindeki ilgili ders müfredatı ile ilişkilendirilerek gelecek nesillerde “Siber Vatandaş” bilinci oluşturulmalıdır (Ünver, 2012).

Alanyazın incelendiğinde son kullanıcıların siber güvenlik ile ilgili olarak bilgilerini, farkındalıklarını ya da tutumlarını ölçebilecek ölçme araçları geliştirilmesine yönelik çalışmalar yapıldığı görülmektedir. Tekerek .A ve Tekerek .M, (2013) Lise öğrencilerinin bilgi güvenliği farkındalığını ölçmek amacıyla “Bilgi ve Bilgisayar Güvenliği Farkındalık Ölçeği” ni geliştirmiştir. Keser ve Güldüren (2015) tarafından yükseköğretim kurumlarında çalışan öğretim elamanlarına yönelik Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ), Güldüren, Çetinkaya ve Keser (2016) “Ortaöğretim Öğrencilerine Yönelik Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ)”, Güldüren, Çetinkaya ve Keser (2017). Öğretmenler İçin Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ), Aslay, Handan ve Üstün (2019) tarafından üniversite öğrencileri, çalışan ve akademisyenlere yönelik “Kişisel Bilişim Güvenliği Tutum Ölçeği” geliştirilmiştir. Siber güvenlik, bilgi güvenliği ve benzeri alanlarda yapılan çalışmaların

Ortaöğretim (Lise düzeyi) itibariyle başladığı ancak pandemi nedeniyle bilişim ve teknolojik aletlerin kullanımının arttığı temel eğitim düzeyinde (İlkokul, Ortaokul) yeterli araştırmanın yapılmadığını göstermektedir. Dolayısıyla literatürde temel eğitim düzeyindeki kullanıcıların siber güvenlik farkındalığını ölçebilen bir ölçme aracına ihtiyaç olduğu düşünülmektedir. Çalışma bu ihtiyaç göz önüne alınarak şekillenmiştir.

1.2. Araştırmanın Amacı

Bu çalışmanın amacı ortaokul öğrencilerinin siber güvenlik farkındalıklarını ölçmek amacıyla geçerli ve güvenilir bir ölçek geliştirmektir. Ayrıca, geliştirilen siber güvenlik ölçeği kullanarak öğrencilerin farklı değişkenler açısından siber güvenlik farkındalıklarını incelemektir.

1.3. Araştırma Soruları

- 1- Siber güvenlik farkındalığı ölçeği geçerlik ölçütlerini karşılamakta mıdır?
- 2- Siber güvenlik farkındalığı ölçeği güvenirlik ölçütlerini karşılamakta mıdır?
- 3- Ortaokul öğrencilerinin siber güvenlik farkındalıkları toplam puan ve alt boyutlarda;
 - a) Cinsiyet değişkenine göre farklılaşmakta mıdır?
 - b) Sınıf düzeyi değişkenine göre farklılaşmakta mıdır?
 - c) İnternet ve bilişim teknolojileri kullanma sürelerine göre farklılaşmakta mıdır?

1.4. Araştırmanın Önemi

Nesnelerin İnterneti (IOT), bulut bilişim ve diğer gelişen teknolojilerin sürekli gelişmesiyle birlikte, hayatın her alanında bilgi kaynaklarının tam olarak paylaşıldığı ve eş zamanlı olarak kullanıldığı çeşitli Siber-Fiziksel Sistemler (Cyber-Physical Systems-CPS) kurulmuştur. Bir yandan bu kaynaklar, ulusal güç, ulaşım, finans, enerji ve diğer önemli ve etkili alanların etkin işleyişini destekleyen tüm ülke ve kuruluşların kilit stratejik alt yapıları haline gelmiştir. Öte yandan, bu kaynaklar insanların üretim ve yaşam biçimlerini derinden etkiler ve değiştirmektedir (Aydeger, Saputro ve Akkaya, 2019; Clements, Yang, Sharma, Hu ve Lao, 2021). Bu gelişmelere bağlı olarak büyüyen bilgi kaynakları ve hizmetlerden yararlanan küresel siber uzayın güvenlik tehditleri de her geçen gün katlanarak artış göstermeye devam ediyor. Yeni siber tehditler küresel olarak yayılırken, çeşitli siber

güvenlik ihlalleri de sıklıkla meydana gelmektedir. Büyük güvenlik olayları (örneğin, Wanna Cry fidye yazılımı virüsü, eBay veri ihlali), siber güvenliğin yıllar içinde ciddi zorluklarla karşı karşıya olduğunu defalarca göstermiştir (Liu, Peng ve Su, 2014).

Etkin olmayan siber güvenlik önlemleri, dünyadaki bilgi toplumlarının gelişimi ve istikrarı için ciddi tehditler ve riskler oluşturmaktadır (Kianpour, Kowalski ve Øverby, 2022). Tüm toplumu etkileyen bir tehdidin bireysel düzeyde de geri döndürülemez sonuçlara sebebiyet vereceği aşikârdır. Bilginin kâğıt veya kitaplarda yer almaması ve dijitalleşmesi sonucu izinsiz erişimlerin engellenmesi, mahremiyetin korunması daha da zorlaşmaktadır. PC virüsleri, bilgi kesintileri, Dağıtılmış Hizmet Reddi (DDoS) ve çok sayıda başka saldırı vektörü dâhil olmak üzere ağ saldırılarına ek olarak PC’ nize, lisanslı ürünlere yetkisiz erişim sağlamaya veya hassas bilgileri toplamak amacıyla saldırılar düzenlenmektedir. En başta kabul edilmesi gereken gerçeklik, her gün dünya genelinde devasa bir günlük çevrim içi tehdidi olduğudur. Bu bilgisayar suçlarıyla mücadele için idareler ve kuruluşlar aracılığıyla çeşitli adımlar atılmaktadır. Siber güvenlik çoğu için önemli bir konu olsa da henüz genel nüfus katılımcılarından yeterli ilgi görmemiştir (Alghamdie, 2021).

Siber güvenlik, elektronik verileri ve bilgisayar sistemlerini koruyan tüm süreçlerin ve teknolojinin toplanması için kullanılan kümülatif bir terimdir. Tanımın rolü, kelimenin tam anlamıyla ne anlama geldiğini açıklamaktır, ancak sanal dünyada siber güvenliğin önemine gereken dikkati toplayamamaktadır. Siber güvenlik, her birey, küçük ve orta ölçekli şirket ve hükümet için hayati bir rol oynamaktadır (Al-Ghamdi, 2021). Siber suçlular günümüzde esas olarak sistem kullanıcılarını hedef aldığından, siber güvenlikle ilgili olarak insan eylemlerine odaklanılmaktadır. Daha önce siber suçlular, kullanıcıların kullandığı sistemlere odaklanmıştı. Ancak en büyük sorun teknolojinin güvenliği değil, bilgi sistemleri kullanıcılarının riskli davranışlarıdır (Öğütçü, Testik ve Chouseinoglou, 2016).

Pandemi önlemleri neticesinde alınan kısıtlama kararlarının da etkisiyle internet kullanımındaki artış, yalnızca teknik personellerin değil, her yaştan kullanıcıların siber güvenlik farkındalığına sahip olması gerekliliğini ortaya koymaktadır. Alanyazında ağırlıkla siber güvenliğinden mesul teknik personelin siber güvenlik eğitiminin değil, aynı zamanda internet güvenliği farkındalık eğitimlerinin ve diğer farkındalık kampanyalarının herkes için zorunluluk haline geldiği belirtilmektedir. Son kullanıcıların siber güvenlik zincirindeki en zayıf halka olduğu ve yaptıkları hatalar sebebiyle ortaya çıkan siber güvenlik ihlallerinin

önüne geçilmesi için siber güvenlik hakkında farkındalık yaratılması gereklidir (Vaczi, Toth-Laufer ve Szadeczky 2020).

Çocuklar tarafından dijital teknolojinin kullanımı son yıllarda önemli ölçüde artmıştır (Holloway, Green ve Livingstone 2013). Özellikle COVID-19 salgını ve sonrasında ortaya çıkan karantina, okulların kapanması vb. durumlar çocukları arkadaşlarıyla iletişim kurmanın birincil yolu olarak internete yönlendirmiştir. (Lobe ve diğerleri, 2020; Kristjánsson ve diğerleri, 2021). Siber güvenlik her yaştan insanı etkileyen bir konu olmasına rağmen dur ancak işin içinde çocuklar olduğunda güvenlik endişeleri daha da önemli ve dikkat edilmesi gereken bir hususa dönüşmektedir. Yaşları göz önüne alındığında, internet ve dijital sistemleri kullanmanın fırsatlarını ve risklerini değerlendirmeleri zordur, hatta hayatlarının giderek daha fazla kısmı dijital olarak kaydedilmekte ve bu durum onların mahremiyetleri ve güvenlikleri üzerinde potansiyel olarak uzun vadeli etkiler yaratmaktadır (Hourcade, 2015).

Siber güvenlik çocuklar söz konusu olduğunda, onları etkileyebilecek tüm çevrimiçi riskler, çocukların farkındalıkları da dâhil olmak üzere onları ve ailelerini desteklemek için alınan önlemlerle ilgilidir (Quayyum ve diğerleri, 2021). Çocuklar tarafından dijital teknolojinin kullanımı son yıllarda nemli ölçüde artmıştır (Holloway ve diğerleri, 2013; Hourcade, 2015). İnternet birçok fırsat sunarken çeşitli riskler de taşımaktadır. Çocuklar, özellikle internette özel verileri başkalarıyla paylaştıklarında sunulan kontrollerin olmaması nedeniyle tehlike altında olabilirler. Günümüzde 12 yaşın altındaki çocuklar giderek daha fazla çevrimiçi oyun oynamak, YouTube izlemek ve sosyal medya platformlarını keşfetmek için zaman harcamaktadırlar (Ofcom, 2016)Bunu yaparken, farkında olmadan arkalarında dijital ayak izlerini bırakırlar ve yalnızca ticari kuruluşların değil kötü niyetli insanlarda çocukların çevrimiçi etkinliklerine ilişkin içgörü kazanmasını kolaylaştırırlar. Ticari taraflar veya siber saldırganlar, çocuklar sosyal ağ sitelerine katıldıklarında, çevrimiçi formları doldurduklarında, internete bağlı akıllı oyuncakları ve diğer araçları doldurduklarında cihazlarına yüklenen çerezler aracılığıyla çocukların çevrimiçi verilerini toplayabilirler ve bu sadece çocukların kullanıcıların kendilerini ifşa etmesi yoluyla gerçekleşmektedir (McReynolds, Hubbard, Lau, Saraf ve Cakmak, 2017). Çocuklar dünyaya ilişkin anlayışlarını internet ortamında geliştirmekte, kişisel verilerin yayınlanmasıyla bağlantılı riskleri belirleyecek ve zararların sonuçlarını değerlendirecek dijital okuryazarlığa sahip olmayabilirler (Dempsey, Sim, Cassidy ve Ta, 2022).

Sosyal medyanın ve diğer ağ bağlantılı teknolojilerin yaygın olarak benimsenmesi ve çocukların çevrimiçi olduklarında karşılaştıkları tehditlerin artmasıyla çocukların güvenliği hızla büyüyen bir sorun haline geldi (Staksrud, Livingstone, ve Haddon 2007;Quayyum ve diğerleri, 2021). Çocukların İnternet kullanımıyla karşılaştıkları tehditlerin genellikle içerik tehditlerini ve iletişim tehditlerini içerdiği görülmektedir. İçerik tehditleri arasında spam, hedefli e-postalar/reklamlar, pornografi, şiddet içeren içerik, anoreksiya yanlısı içerik ve uyuşturucuyla ilgili içerik bulunurken, temas tehditleri arasında çocuk tacizi, cinsel içerikli mesajlaşma, siber zorbalık, siber takip ve gizlilik kaybı yer alır (Magkos, Kleisiari, Chanas ve Giannakouris-Salalidis, 2014). Boyd ve Hargittai (2013) bu sınıflandırmayı, yasadışı dosya paylaşımı veya başkalarına zorbalık gibi çocuğun meşgul olması gibi davranış tehditlerini içerecek şekilde genişletmiştir. Magkos ve diğerleri (2014), özellikle bilgisayarlar ve İnternet kullanımıyla ilgili tehditleri, yani bilgi güvenliği tehditlerini de içerecek şekilde genişletmiş, kötü amaçlı yazılım, kimlik avı, veri hırsızlığı/kaybı, parola çalma/kırma ve İnternet bağımlılığı gibi tehlikeleri de dâhil etmiştir.

İnternet ve çevrimiçi teknolojilerin hızla benimsenmesi endüstriye, araştırmacılara, politika yapıcılara ve hükümetlere internet kullanımının risklerini tanıma ve risklerle ilişkili zararın en aza indirilmesini sağlamak için stratejiler ve araçlar, yani aracılık mekanizmaları geliştirme görevi sunar (Donoso, Verdoodt, Van Mechelen, ve Jasmontaite, 2016). Çevrimiçi ortamda güvende olmak için, çocukların çevrimiçi fırsatlar ve riskler, çevrimiçi zarar ve tehditlerin nasıl yönetileceği konusunda eğitime ihtiyaçları vardır. İnterneti güvenli, saygılı ve sorumlu bir şekilde kullanmaları için yetkilendirilmeleri gerekir. Okullar, çevrimiçi güvenliği teşvik etme ve öğretmede hayati bir rol oynamaktadır (Polanin ve diğerleri, 2021);(Patterson, Ryckman, ve Guerra 2022). Konunun önemi, çocukların zaten çevrimiçi risklere maruz kaldığı gerçeğiyle birleştiğinde, okullarında uygun bir siber güvenlik müfredatı zorunlu hale getirilmelidir. Daha genç yaşta öğretmek, muhtemelen tamamen yetenekli yetişkinlerle sonuçlanacaktır. Konunun önemi, çocukların zaten çevrimiçi risklere maruz kaldığı gerçeğiyle birleştiğinde, okullarında uygun bir siber güvenlik müfredatı zorunlu hale getirilmelidir (Witsenboer, Sijtsma, ve Scheele 2022).

Bu tespitler ışığında dünyada ve ülkemizde giderek daha büyük bir sorun haline gelen çevrimiçi ortamlarda çocukların güvenliğini nasıl sağlayacağız sorusunu cevaplayabilmemiz için çocukların (öğrencilerin) siber güvenlik farkındalıklarının ne düzeyde olduğunun

belirlenmesi gerekmektedir. Alanyazında siber güvenlik farkındalığı ile ilgili incelenen ölçek geliştirme çalışmalarında genellikle erişkinler, öğretmenler, akademisyenler, belirli meslek gruplarına yönelik geliştirilen siber güvenlik farkındalığı ölçekleri olarak görülmektedir. Bu anlamda temel eğitim (ortaokul öğrencileri) düzeyindeki öğrencilere ait siber güvenlik farkındalıkları durumları bu çalışmayla ortaya koyulacaktır. Bu yönleriyle, bu araştırma, araştırmacılara ve velilere yol gösterici olacaktır. Ayrıca ortaokul öğrencilerine yönelik siber güvenlik farkındalık ile alanyazına katkı sağlanacağı ve daha sonra yapılacak araştırmalara da yol gösterebileceği düşünülmektedir.

1.5. Araştırmanın Sınırlılıkları

Araştırmanın çalışma grubu Amasya ilinden kolay ulaşılabilir örnekleme yöntemi ile seçilmiş olan ortaokullardaki 5., 6., 7. ve 8. sınıf öğrencileri ile sınırlıdır.

Geliştirilen ölçek için toplanan veriler 2021-2022 eğitim-öğretim yılı güz dönemi, araştırma problemleri için toplanan veriler 2022-2023 bahar dönemi ile sınırlıdır.

1.6. Araştırma Varsayımları

- 1- Araştırmada, öğrencilerin demografik bilgi formu ve ölçek maddelerini samimiyetle, tarafsız ve doğru bir şekilde doldurmuş oldukları varsayılmaktadır.
- 2- Araştırmada, örneklemin evreni temsil ettiği varsayılmaktadır.
- 3- Araştırmada, kullanılmış olan ölçek taslağının araştırmanın amacına hizmet ettiği varsayılmaktadır.

2. KURAMSAL ÇERÇEVE

Araştırmanın bu bölümünde Siber Uzay, Siber Güvenlik, Siber Güvenlik Farkındalığı ile ilgili kuramsal bilgilere ve bu konular ile ilgili alan yazındaki çalışmalara yer verilmiştir.

2.1. Siber Uzay

Siber uzay denilince aklımıza bilgisayar, ağ, internet, veri ve bilgi, donanım ve yazılım, iletişim gibi bazı ilgili kelimeler gelmektedir. Yaygın kullanılan bir mecaz olarak siber uzay terimi, bir dereceye kadar, İnternet kavramını ifade etmek ve bilgisayar ağından türetilen çeşitli kavramları işaret etmektedir. Çeşitli bilgisayar altyapıları ve bilgisayar ağları içinde var olan kavramsal ve cisimsiz bir alandır. Öte yandan, insanların etkileşimde bulunabileceği sanal bir ortam olarak kavramsallaştırılan bilgisayar teknolojilerine ilişkin genel bir terminolojidir. Siber uzay teriminin çeşitli sözlüklerde, resmi hükümet kaynaklarında ve literatürde tutarsız bir şekilde anlaşılması şaşırtıcı değildir. Şu anda, bilgi ve bilgisayar teknolojisinin hızlı gelişimi olarak, “siber uzay” terimi, şüphesiz günlük yaşamımızda, işimizde ve çalışmalarımızda giderek daha fazla yer işgal etmeye başlayacaktır.

Başlangıçta, siber uzay terimi ilk olarak 1960'ların sonunda Ussing ve Hoff'un “duyusal alanlar” fikrini temsil etmek için yaptığı sanat eserlerinde, insanları algılayabilen ve adapte olabilen fiziksel bir oda olarak ortaya çıktı. 1980’lerde, terim Gibson tarafından bilim kurgu “Burning Chrome” ve “Neuromancer” adlı eserlerinde kullanılmıştır (Gibson 2017). “İnsan sistemindeki her bilgisayarın bankalarından soyutlanmış verilerin grafik bir temsili” olarak tanımlanan terim ilk kullanıldığı zamandan itibaren, konsepti belirgin bir şekilde bilgisayarlar tarafından yaratılan dijital dünyanın eş anlamlısı olarak tanımlanmış ve aktif olarak kullanılmaya başlanmıştır. Şimdiye kadar, siber uzay terimi, bilgisayar teknolojileri ve ağın küreselleşmesi ile ilgili olarak bilim adamları, araştırmacılar, profesyoneller, hobiler ve bilgisayar korsanları tarafından çeşitli akademik ve teknoloji çalışmalarında yaygın olarak kullanılmıştır (Ning, Ye, Bouras, Wei ve Daneshmand, 2018).

Siber uzay terimi ülkemizin en üst siber güvenlik belgesi olan 2020-2023 Ulusal Siber Güvenlik Stratejisi belgesinde “Doğrudan ya da dolaylı olarak internete, elektronik haberleşme ve bilgisayar ağlarına bağlı olan tüm sistem ve hizmetler “(Ulusal Siber

Güvenlik Belgesi, 2020) olarak tanımlanmış ve çalışmaya kaynaklık edecek tanım olarak kabul edilmiştir.

Mevcut tanımlar incelendiğinde birbirine benzer özellikler bir grup altında toplanabilmektedir. Özetle, geniş tanım yelpazesi en fazla dört yönden oluşmaktadır. Bunlar;

1. Aynı zamanda siber uzayın temel bileşeni olan ağ sistemi;
2. Veriler ve/veya bilgiler ve bunların depolanması, işlenmesi, erişimi, iletimi, değişimi ve paylaşımı;
3. İnsan-makine etkileşimleri;
4. Zaman boyutu.

Özünde, bu tanımların ortaya koyduğu en önemli fikir, siber uzayın geleneksel PST'ye (physical-social-thinking spaces=fiziksel-sosyal- düşünme alanı) dayanan yapay bir alan olduğu, aynı zamanda PST'den bağımsız olarak kendi kendini düzenleyen bir alan olduğudur. Ayrıca, bir insan siber uzayın bir katılımcısı veya bir bileşeni olarak onunla etkileşime girebilir. Sonuç olarak, geleneksel anlamda siber uzay, küresel olarak birbirine bağlı bilgisayar ağlarına ve tüm ilgili altyapılara ve unsurlara dayanan dijital, sanal, soyut ve zamandan bağımsız metaforik alanı ifade eder (Ning ve diğerleri 2018).

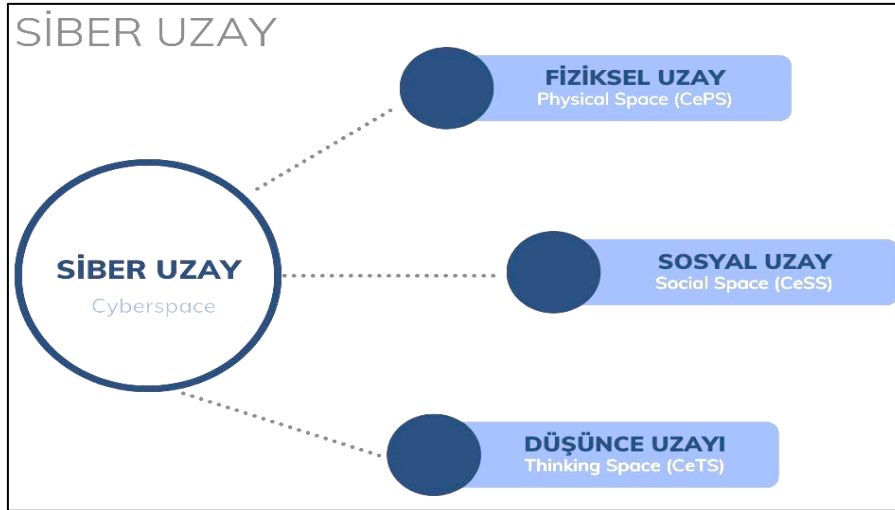
Etki alanı olarak siber uzay insan yapımıdır ve belirli amaçları desteklemek için inşa edilmiştir (Waldrop 2008). Tasarımcılar, erişim kolaylığı, kullanılabilirlik, birlikte çalışabilirlik, genişletilebilirlik ve yenilikçiliğe prim veriyor. Güvenlik ve hesap verebilirlik, özellikle sistemin başlangıcında küçük güvenilir kullanıcılar çevresi arasında daha düşük önceliklerdi. Bu erken tasarım özellikleri, özellikle yeniliği ve gelişmiş işlevselliği yönlendiren pazar teşvikleri, güvenlik veya ağ esnekliğinde karşılaştırmalı olarak hızlı ilerlemeler üretmeyebileceğinden, günümüzde yaygın güvenlik açıklarının devam eden varlığının sebeplerinin anlaşılmasına yardımcı olur. Siber uzayın ayırt edici ve kurucu bir özelliği, hiçbir merkezi varlığın bu yeni alanı oluşturan tüm ağlar üzerinde kontrol uygulamamasıdır (Mayer, Martino, Mazurier ve Tzvetkova, 2014).

Siber uzay dinamikdir. Fiziki arazinin aksine yapısı bile çok hızlı değişebilmektedir. Bu fikri daha iyi aydınlatmak için, Kuzey Atlantik Antlaşması Örgütü (North Atlantic Treaty Organization-NATO) Siber Kooperatif Savunma Mükemmeliyet Merkezi'nden iki analist, siber uzayı "zamana bağlı birbirine bağlı bilgi sistemleri ve bu sistemlerle etkileşime giren

insan kullanıcılar" olarak tanımladı. Bu tanım, siber uzayın “küresel olarak birbirine bağlı donanım, yazılım ve veri ağlarından” ve bunlarla etkileşime giren insanlardan oluştuğu fikrini yakalama avantajına sahiptir. Bununla birlikte, burada en alakalı olanı, yazarların "kullanıcıların, düğümlerin ve bağlantıların görünüp kaybolabileceğini ve bilginin bazen çok hızlı bir şekilde dönüştürülebileceğini" vurgulayan "zamana bağlı" terimini tanıtmasıdır (Ottis ve Lorents 2010).

Siber uzay barındırdığı mimari ve teknolojiler nedeniyle hızlıdır. Bu hızın çeşitli tezahürleri vardır. Hız, neredeyse anında gerçekleşebilen siber uzaydaki olayların özelliğidir. Örnek vermek gerekirse, Ocak 2003'te internette çoğalan Slammer solucanıdır. Yayılmaya başladıktan 10 dakika sonra savunmasız ev kullanıcılarının yüzde 90'ından fazlasının cihazlarına bulaştı. Finans, ulaşım ve devlet kurumlarında önemli aksamalara neden oldu (Moore ve diğerleri, 2003) Bu savunmasız ana bilgisayarlar, dünya çapında geniş çapta dağılmış en az 75.000 makineyi içeriyordu.

Siber uzaya ulaşmak günümüz teknolojik imkânları sayesinde çok kolaydır. Cep telefonu veya bilgisayar olmayanlar bile bir internet kafede zaman satın alarak siber uzaya girebilirler. Buradaki en önemli karşıtlık muhtemelen siber uzay ve uzay arasındadır. Uzaya erişimle ilgili kaynaklar ve teknoloji gereksinimleri nedeniyle, uzaydaki aktörler genellikle ulusal hükümetler ve nispeten az sayıda özel kuruluşla sınırlıdır. Bazıları için siber uzay, her şeyden önce iletişimin gerçekleştiği ve fikirlerin değiş tokuş edildiği bir ortam olabilir. Diğerlerine göre siber uzay, birincil faaliyetlerin temel hizmetlerin sağlanması, değeri artırma veya servet depolamak olduğu ticari bir alandır. Siber uzay aynı zamanda, bazılarının kullanılması için sanal dünyayı terk etmeden nesnelerin aktarıldığı bir yer olabilir. Siber uzayda kullanılan mekanlar Şekil 2.1.'de sunulmuştur. Siber uzayı düşünmenin dördüncü bir yolu, ülkelerin kendi ulusal çıkarlarını rekabette ve kendi çıkarlarını takip eden diğer devletlerle çatışmada ilerletmeye çalıştıkları bir devletlerarası etkileşim alanı olarak düşünmektir. Elbette, siber uzay, bu alandaki faaliyetleri yönetmesi gereken uygun normlar, düzenlemeler ve yasalar hakkında çalışma yapılmasına neden olan bu durumlardır (Nielsen, 2012).



Şekil 2.1. Genel siber uzay mekanları (Ning, Ye, Bouras, Wei ve Daneshmand, 2018)

2.2. Siber Güvenlik

Teknolojideki değişiklikler, siber güvenliğin sorun boyutlarını yaratmış ve değiştirmiştir. Ev bilgisayarları çoğaldıkça ve internete erişim tüketiciler için erişilebilir hale geldikçe, yasa dışı etkileşimler ve işlemler için potansiyel de artmıştır. Uzak bilgisayar erişim teknolojisinin ortaya çıkışı, yalnızca ev bilgisayarları için değil, internete doğrudan bağlı bilgisayarlara kontrolünde olan alt yapı ve hükümet sistemleri için de yetkisiz erişim ve denetim sorununa neden olmuştur. Bu teknolojinin küresel ölçekte yaygınlaşması, herhangi bir ülke için dış politika endişeleri yaratmaktadır. Elektronik tıbbi kayıtlar, sağlık hizmetleri endüstrisine ağlarının ve verilerinin güvenliğini ve güvenliğini izleme konusunda sorumluluğu artırmaktadır. Çevrim içi alışveriş, bankacılık ve diğer finansal işlemleri kolaylaştıran teknolojiler, benzer şekilde bu sektörleri siber güvenlikle ilgilendiriyor. Bu alanların her biri, siber güvenliği sağlamak için çalışmalarını sürdürürken ve sistemleri bozmak için tasarlanmış teknolojilerde hızlı değişikliklere tabidir (Lewallen, 2021).

Siber güvenlik (SG) için genel olarak üzerinde mutabık kalınan bir tanım yapılması her zamankinden daha zor görünüyor. Bu, yalnızca çeşitli amaçlara, bağlamlara ve statülere sahip resmi metinlerde bulunan sayısız (ve bazen birbiriyle çelişen) tanımlarda değil, aynı zamanda tam olarak bu sorunu ele almayı amaçlayan ve son yıllarda sayısı hızla artan akademik çalışmalara da yansımaktadır (Papakonstantinou, 2022). Tüm akademisyenlerin üzerinde uzlaştığı net bir gerçek veya operasyonel tanımı yoktur. Ancak Uluslararası Telekomünikasyon Birliği (International Telecommunication Union-ITU) siber güvenliği

“araçların, politikaların, güvenlik kavramlarının, güvenlik önlemlerinin toplamıdır. Yönergeler, risk yönetimi yaklaşımları, eylemler, eğitim, en iyi uygulamalar, siber ortamı ve organizasyonu ve kullanıcı varlıklarını korumak için kullanılabilecek güvenceler ve teknolojiler. SG, siber ortamdaki ilgili güvenlik risklerine karşı kuruluşun ve kullanıcı varlıklarının güvenlik özelliklerinin elde edilmesini ve sürdürülmesini sağlamak için çaba gösterir.” olarak tanımlar (ITU, 2021).

SG’nin diğer bir tanımına Oxford Üniversitesi yayınlarında rastlıyoruz. Elektronik verilerin suça veya yetkisiz kullanımına karşı korunma durumu veya bunun için alınan tedbirler. (Oxford University Press, 2014). Amerika Birleşik Devletleri Güvenlik Kurumu (United States Department of Homeland Security-DHS) SG’yi bilgi ve iletişim sistemlerinin ve içerdiği bilgilerin hasar, yetkisiz kullanım veya değişiklik veya istismardan korunduğu ve/veya bunlara karşı korunduğu faaliyet veya süreç, yetenek veya yetenek veya durum olarak tanımlamış (DHS, 2014), Lewis (2006) ise, siber güvenlik, bilgisayar ağlarının ve içerdikleri bilgilerin sızma ve kötü niyetli hasar veya kesintilerden korunmasını gerektirir demiştir. Amoroso (2006), siber güvenlik, yazılımlara, bilgisayarlara ve ağlara yönelik kötü niyetli saldırı riskini azaltmayı içerir. Buna, izinsiz girişleri tespit etmek, virüsleri durdurmak, kötü niyetli erişimi engellemek, kimlik doğrulamasını uygulamak, şifreli iletişimlerini etkinleştirmek ve daha fazlası için kullanılan araçlar dâhildir şeklinde tanımlamıştır.

İnternet kullanıcılarına yönelik riskleri tanımlamak için farklı terimler kullanılmaktadır. SG, internet güvenliği, çevrimiçi güvenlik vb. terimler literatürde birbirinin yerine kullanılmaktadır (Quayyum ve diğerleri 2021). SG, internet güvenliği, bilgi güvenliği ve bilgisayar güvenliği ile ilişkilendirilen genel bir terimdir. Ancak kapsamı, uygulamayı ve doğru kullanımını anlamak önemlidir. Birçok kişi tarafından yanlış anlaşıldığı gibi, SG bilgisayarların internet üzerindeki güvenliğini sağlamakla sınırlı değildir (Singer ve Friedman, 2014). Siber güvenlik, çevrimiçi bir sistemde (internet) bulunan donanım, yazılım, veri ve bilgilerin her türlü ihlalden korunması olarak da tanımlanmakta ve kapsamı, elektronik cihaz ve ekipmanların (ev dâhil) yetkisiz kullanım, yanıltıcılar ve saptırmalara karşı güvence altına alınmasıyla genişletilmiştir. SG, veri koruma ve bilgi güvenliğinin uygulanması için organizasyon için en yüksek öncelik, bireyler için ise gizlilik ve erişim kontrolü ve güvenlik olarak tanımlanabilir (Tirumala ve diğerleri, 2015; Toch, ve diğerleri, 2018). Şu anda, SG’nin kapsamı, bireyleri siber zorbalığa karşı korumaya ve gelişmiş

makine öğrenimi teknikleri kullanarak siber savaşı tanımlamaya yönelik olarak genişletilmiştir (Blanke ve diğerleri, 2022; Tirumala ve diğerleri 2019). Ayrıca SG yerine güvenlik kültürü, bilgi güvenliği kültürü ve son zamanlarda siber güvenlik kültürü gibi birçok terim kullanılmaktadır. SG genellikle daha genel olarak bilgi güvenliği ile eş anlamlı olarak kullanılsa da iki terimin doğası tartışmalı bir şekilde farklıdır. Örneğin, Von Solms ve Van Niekerk (2013) siber güvenliği, daha kapsamlı olarak kabul edilebilecek insan ve organizasyon varlıkları başta olmak üzere ek bir dizi varlığı koruma amacı olarak tanımlamaktadır. Bu nedenle, bu geniş yönlerin korunmasına ilişkin ortak değerler, inançlar ve beklenen davranışların dikkate alındığı görülebilir (Da Veiga 2016; Ioannou, Stavrou, ve Bada 2019). Bahsedilen tanımlar incelendiğinde SG'nin çok boyutluluğunu yakalayan kısa ve evrensel olarak kabul edilebilir bir tanımının olmaması, karmaşık siber güvenlik zorluklarını çözmek için birlikte hareket etmesi gereken disiplinleri ayırırken siber güvenliğin ağırlıklı olarak teknik görüşünü güçlendirerek teknolojik ve bilimsel ilerlemeleri engellemektedir (Craig, Diakun-Thibault ve Purse 2014).

SG tanımları literatür haricinde hükümetlerin siber güvenlik politikaları, Avrupa Birliği (AB), NATO ve benzeri örgütlerin strateji belgelerinde de yer almaktadır. Dijital çağda, modern toplumlar küresel olarak birbirine bağlıdır ve giderek bilgi ve iletişim teknolojilerine (BİT) ve dijital altyapıya bağımlıdır. Bununla birlikte, bu karşılıklı bağlantı, aynı zamanda, ulusal, bölgesel ve uluslararası düzeylerde yönetilmesi gereken, ortaya çıkan tehditlere karşı karşılıklı bağımlılıklar ve güvenlik açıkları da yaratır. Siber güvenliğin geliştirilmesi ve kritik bilgi altyapılarının korunması, özellikle dijital ekonomi ve bilgi toplumuna yönelik küresel harekette her ulusun güvenliği ve ekonomik refahı için esastır. Ulusal düzeyde siber güvenlik, hükümet yetkilileri, özel sektör ve sivil toplum tarafından önleme, hazırlık, müdahale ve olay kurtarma için koordineli eylem gerektiren ortak bir sorumluluktur. Bunun sorunsuz bir şekilde işlemesi ve güvenli, emniyetli ve esnek bir dijital alan sağlamak için çok paydaşlı bir yaklaşımla geliştirilmesi, uygulanması ve yürütülmesi gereken kapsamlı bir çerçeve veya strateji gereklidir. Bu çerçeve genellikle Ulusal Siber Güvenlik Stratejisi (National Cyber Security Strategy-NCSS) olarak adlandırılır ve herhangi bir ülkenin sosyo-ekonomik güvenliği için kritik bir unsurdur. Ülkemiz Ulaştırma ve Altyapı Bakanlığı koordinesinde 2013-2014, 2016-2019 ve 2020-2023 yıllarını kapsayan üç adet Siber Güvenlik Eylem Planı yayımlamıştır. Siber Güvenlik Eylem Planı belgesinde SG, "Siber uzayı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilginin/verinin gizliliği, bütünlüğü ve erişilebilirliğinin güvence altına alınmasını,

saldırıların ve siber olayların tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber olay öncesi durumlarına geri döndürülmesini kapsayan faaliyetler bütünü.” olarak tanımlanmıştır (Ulusal Siber Güvenlik Belgesi, 2020).

Gelişen tehditler ve siber güvenlik farkındalığı eksikliği, hükümetleri, araştırmacıları ve vatandaşları, bir devletin siber dirençli olduğu konusuna dair kesin bir sonuca ulaştıramamaktadır. Ancak bir ülkenin siber güvenlik düzeyinin, siber tehditleri önlemeye hazırlığının ve siber olayları ve siber uzaydaki suç faaliyetlerini yönetmeye hazır olup olmadığının bilinmesi o ülkenin ihtiyaç analizinin önemli bir unsurudur. Ülkelerin SG alanında ne kadar başarılı oldukları sürekli izlenmelidir. Estonya hükümeti tarafından hazırlanan Küresel Siber Güvenlik Endeksi (Global Cybersecurity Index-GCI), ülkelerin siber güvenliğe olan bağlılığını küresel düzeyde ölçen, konunun önemi ve farklı boyutları hakkında farkındalık yaratmak için güvenilir bir referanstır. Bu ölçütlere göre değerlendirilen 160 ülke içinde 2022 yılında Türkiye 58. sırada yer almaktadır (NCSI, 2022).

2.2.1. Siber güvenlik ile ilgili kavramlar

Bilgi Güvenliği: Bilişim sistemlerinin ve bilgilerin izinsiz kullanımını, yetkisiz kişilerce erişilmesini ve ifşa edilmesini, silinmesini, değiştirilmesini ve zarar görmesini, engellemek, bu sistem ve bilgilere yetkili kişiler ve işlemlerin ihtiyaç duyulan zamanda ve kalitede erişebilmesini sağlamak için yürütülen faaliyetler bütünüdür (Ulusal Siber Güvenlik Belgesi, 2020).

Bilişim Sistemleri: Siber ortamda bilgi ve iletişimin sağlandığı, bilgisayar ve internet ağı yardımıyla bilgi ve iletişim teknolojileri kullanılarak gerçekleştirilen bütün işlemlerdir (Ulusal Siber Olaylara Müdahale Merkezi, 2014).

Erişim Kontrolü: Bilgiye erişimin denetlenmesi, bilgi sistemlerine yetkisiz erişimin engellenmesi, yetkisiz kullanıcı erişimine izin verilmemesi, hizmetlerin korunması, yetkisiz işlemlerin tespit edilmesi ve uzaktan çalışma ortamlarında bilgi güvenliğinin sağlanmasıdır (Ulusal Siber Olaylara Müdahale Merkezi, 2014).

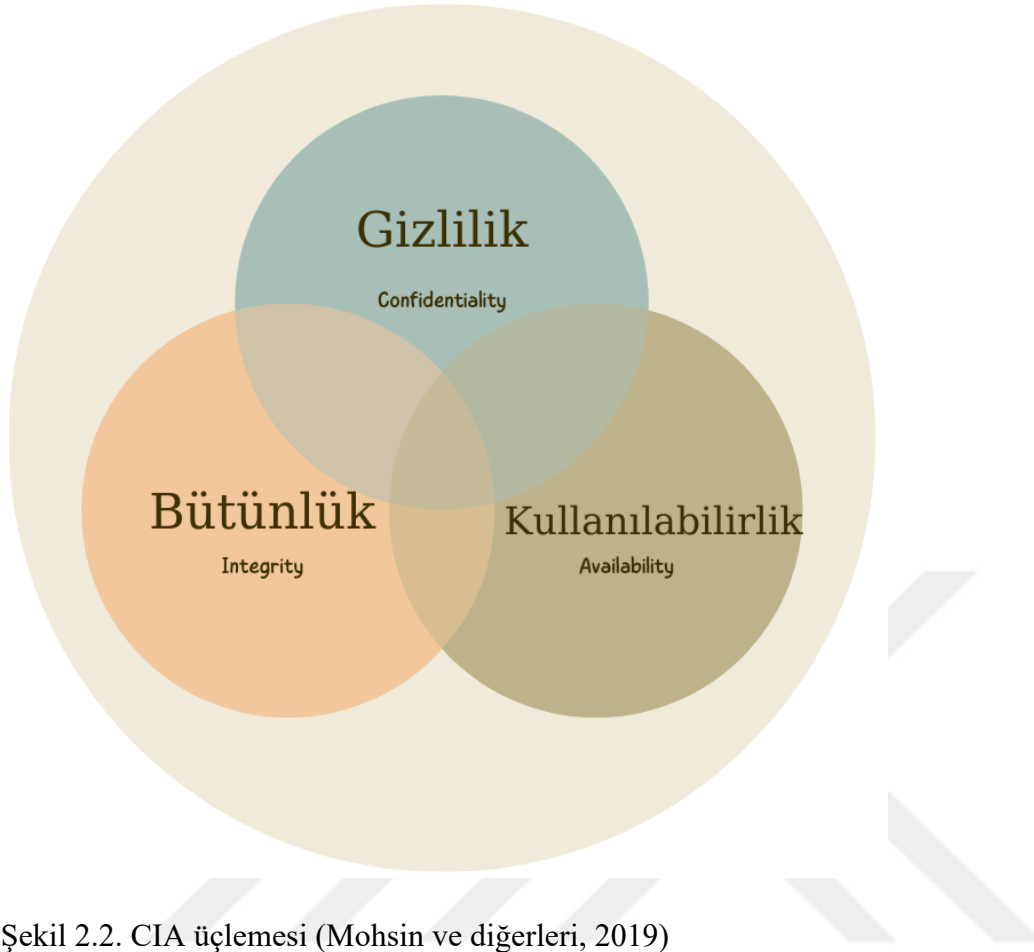
Siber Saldırı: Siber uzaydaki bilişim ve endüstriyel kontrol sistemlerinin veya bu sistemler tarafından işlenen bilginin/verinin gizliliği, bütünlüğü veya erişilebilirliğini ortadan kaldırmak amacıyla, siber uzayın herhangi bir yerindeki kişi ve/veya bilişim sistemleri tarafından kasıtlı olarak yapılan işlemler (Ulusal Siber Güvenlik Belgesi, 2020).

Siber Suç: Bir bilişim sisteminin güvenliğini ve buna bağlı verileri ve kullanıcılarını hedef alan ve bilişim sistemi kullanılarak işlenen suçlardır. Siber suçu diğer suçlardan ayıran özelliği bir bilişim sistemi olmadan işlenememesidir. Bu suç türü bilgisayar ve internetle işlenen suçlar olarak da adlandırılmaktadır (Ulusal Siber Güvenlik Belgesi, 2020).

Siber varlık: Siber ortamlarda bulunan, araçlar, işlemler, dokümanlar, planlar, veriler veya bilgilerdir. Bu bir bilgisayar, sunucu veya bir ağ cihazı olabileceği gibi kişisel, kurumsal veya ulusal veriler de olabilir. İnternete bağlı televizyon, cihaz, sistem veya araç olabileceği gibi veri tabanı, veri merkezi, veri kayıt sistemi veya kullanılan yazılımlar, donanımlar ve süreçler siber ortamdaki varlıklardır (USOM, 2014).

2.2.2. Bilgi güvenliği üçlüsü (CIA)

CIA üçlüsü (Confidentiality-Gizlilik, Availability-Erişilebilirlik-Kullanılabilirlik, Integrity-Bütünlük), doksanlı yıllardan itibaren Güvenlik hedeflerini ifade etmek ve güvenlik gereksinimlerini ifade etmenin çok amaçlı, standart bir yolu olarak ortaya çıkmıştır. Daha sonra, genellikle ek güvenlik özelliklerini içerecek veya belirli alanları ele alacak şekilde genişletilmiştir (Shoufan ve Damiani, 2017). Canbek ve Sağıroğlu (2006) bilgi güvenliğinin temel unsurları olarak gizlilik (confidentiality), bütünlük (integrity), kullanılabilirlik (availability) yanı sıra kimlik doğrulama (authentication) ve inkâr edememe (non-repudiation) olarak belirtmişlerdir. Bunun dışında sorumluluk (accountability), erişim denetimi (Access control), güvenilirlik (reliability) ve emniyet (safety) etkenleri de bilgi güvenliğini destekleyen unsurlar olarak belirtilmiştir. Bu alt boyutların tam anlamıyla sağlanması ile oluşturulan bir sisteme bilgi güvenliğinin tamamıyla sağlanabileceği düşünülmektedir.



Şekil 2.2. CIA üçlemesi (Mohsin ve diğerleri, 2019)

Gizlilik: 'Gizlilik' terimi, Latince “confidere” fiilinden türetilmiştir. "tam güvene veya güvene sahip olmak" anlamına gelir. Gizlilik, kökleri yukarıdan aşağıya bir otoriteyi sürdürme ve bilgiye erişimi olanlar üzerinde, bilmesi gereken bir şey üzerinde kontrol sağlamaya yönelik askeri zihniyete dayanan bilgi güvenliğinin birincil ilkesidir. Camp (1999), gizliliğin, verilerin ve bu tür veriler tarafından temsil edilen bilgilerin, kullanımının yalnızca yetkili kişiler tarafından yetkilendirilmiş amaçlarla sınırlandırılacak şekilde korunması gerektiği fikrini ifade ettiğini öne sürer. Kısaca Bilginin/verinin yetkisiz kişiler, varlıklar ya da süreçler tarafından erişilememesi, kullanılamaması, depolanmaması, başka bir ortama kaydedilmemesi veya ifşa edilmemesi özelliğidir (Ulusal Siber Güvenlik Belgesi, 2020).

Bütünlük: Etimolojik açıdan bakıldığında, 'bütünlük' kelimesi 'sağlamlık', 'bütünlük' anlamına gelir ve Latince “tangere” kelimesinden türetilmiş ve 'dokunmak' anlamına gelir. Olumsuz ön eki özel bir gücü belirtir ve bu nedenle 'bütünlük' kelimesinin anlamı 'dokunulmaz' kelimesinin belirli çağrışımlarıyla ilişkilendirilebilir, bu da etik bütünlük

kavramıyla ilgilidir. Bilgi güvenliği ve denetimi mesleğinde etik, çeşitli mesleki uygulama standartları ve niteliklerinin içeriğinde öngörülen, yaygın olarak kabul edilen ilke ve değerlere bağlılığı içerir. “Uygun olmayan bilgi değişikliği veya imhasının” önlenmesi olarak tanımlar ve özellikle bilginin gerçekliğini ve reddedilmemesini içerir (von Solms ve van Niekerk 2013). Kısaca bütünlük “Bilginin/verinin doğruluğunu ve tamlığını koruma özelliği” dir (Ulusal Siber Güvenlik Belgesi, 2020).

Kullanılabilirlik (Erişilebilirlik): 'Kullanılabilirlik' kelimesi Latince kökenli olup “valere” den gelir ve “değerli olmak” anlamına gelir. Bilgi güvenliğinde kullanılabilirlik terimi, “bilgiye zamanında ve güvenilir erişim ve bilgi kullanımı” anlamına gelir (United States Code, 2006). Bu, bu belgenin önceki alt bölümünde bahsedilen ve kimlik yönetimi altındaki bir sonraki alt bölümde ele alınacak olan erişim yönlerinin yanı sıra sistemlerin kullanılabilirliği ile ilgili yönleri içerir. Ulusal Siber Güvenlik Belgesi (2020)’de ise terim “erişilebilirlik” olarak kullanılmış ve “Bilginin/verinin yetkili bir varlık tarafından talep edildiğinde erişilebilir ve kullanılabilir olma özelliği.” olarak tanımlanmıştır. Kullanılabilirlik mühendisliği perspektifinden, bir sistem etkili ve verimli olduğunda kullanılabilir olarak kabul edilir ve kullanıcıları genellikle belirli bir ortamdaki belirli görevlerin performansından memnun kalır (Weir ve diğerleri, 2009).

2.2.3. Parker altılısı (parkerian hexad)

Çok uzun bir süre, bir güvenlik tasarımının CIA üçlüsünün tüm bileşenlerini karşılaması durumunda, bilgileri olabildiğince güvende olduğu düşünülüyordu. Ancak bu düşünce tarzı, son yıllarda çeşitli nedenlerle değişti. Verileri saklama şeklimizde, nerede sakladığımızda, nasıl ilettiğimizde ve nasıl güvenceye aldığımızda çok şey değişti. Ayrıca, bilgi çoğaldıkça ve dünya çapında daha yaygın olarak paylaşıldıkça, veri güvenliğinin sağlanması ve mahremiyetin korunması zorlaşmaktadır (Cukier, 2010).

Parkerian altılısı, daha kapsamlı ve eksiksiz bir güvenlik modeli oluşturmak için CIA üçlüsüne eklenen bir dizi bileşenin ifadesidir. Bilgi güvenliğinin nasıl anlaşıldığını ve uygulandığını değiştirmeyi amaçlar. Parkerian Hexad' in altı atomik ögesi gizlilik, bütünlük, kullanılabilirlik, özgünlük, sahiplik veya kontrol ve faydadır. Günümüzün bilgi varlıklarının güvenliğini artırmak için CIA modelinin boşluklarını doldurmayı amaçlamaktadır. Altıgen sadece altı bileşeni sembolize etmekle kalmaz, aynı zamanda mecazi olarak her bir bileşenin

mükemmel bir şekilde birbirine uyduğunu ve kapsamlı bilgi güvenliği bulmacasını çözdüğünü gösterir (Pender-Bey, 2019).



Şekil 2.3. Parker altılısı (Pender-Bey, 2019)

Gizlilik: Gizlilik, muhtemelen hem CIA modelinin hem de Parkerian Hexad'ın en önemli unsurudur. Bilginin yetkisiz kişilere, kuruluşlara veya süreçlere sunulmaması veya ifşa edilmemesi özelliğini ifade eder (Steichen, 2012). Verileriniz gizli değilse, güvenli değildir. Her kuruluş, yalnızca belirli kişilerin erişmesine izin verilmesi gereken bir tür hassas bilgiye sahiptir. Bu bilgilerin ifşa edilmesi durumunda şirket ve/veya müşterileri üzerinde zararlı etkileri olabilir.

Günümüzde hassas verilerin gizliliğini korumak için kullanılabilecek çok sayıda yöntem, teknoloji ve teknik bulunmaktadır. Kuruluşa bağlı olarak, bazı yöntemler gereksiz kabul edilebilir ve/veya kullanıcıların günlük sorumluluklarını yerine getirmelerini yasaklayabilir. Her kuruluş, kendisi için en uygun yöntemin hangisi olduğunu bulmalıdır (Pender-Bey, 2019).

Sahiplik/Kontrol: Sahip olma/kontrol bileşeni, Parker'ın CIA modeline yaptığı eklemelerden biridir. Gizli verilerin, gizliliği fiilen ihlal etmeden veya ihlal etmeden yetkisiz bir kişi veya tarafça ele geçirilebileceği ve kontrol edilebileceği fikrine karşı koruma sağlamak için eklenmiştir. Parker bu bileşeni şu şekilde tanımlar: “kişinin kontrolü altına alma veya kontrolüne alma veya emrinde tutma durumu; velayetten farklı olarak, mülkiyetin kendisine ait olan kişi tarafından fiili fiziksel kontrolü; sahip olunan veya kontrol edilen bir şey.” (Parker, 2010). Bu bileşen aynı zamanda sahip olunan ve kopyası yazılı olan kamuya açık verilerin korunmasını da ele alır. Makaleler, kitaplar, haber yayınları, bilimsel dergiler vb., teknik olarak herkesin görebileceği şekilde mevcut olsalar bile korunmalıdır. Sahiplik/Kontrol hayati önem taşır çünkü gizliliğin hem önemli olduğu hem de var olmadığı ihlalleri kapsar.

Bütünlük: Bütünlük CIA üçlüsünün orijinal bir bileşenidir. Verilerin yetkisiz veya istenmeyen bir şekilde değiştirilmesini önleme yeteneği olarak tanımlanmaktadır. Bu tanım, yalnızca yetkisiz taraflar veya izinsiz girişlerle sınırlı değildir. Bu tanım, bilgi varlıklarına yetkili erişimi olan kişileri de kapsar. Çalışanların veri bütünlüğüne yönelik en büyük tehditlerden biri olduğu bilinen bir gerçektir. Çalışanlar bazen yanlışlıkla dosyaları siler, yanlış veriler girer, yanlış dosyaya kaydeder, yanlış dosyaları düzenler vb. Dosya bozulması başka bir endişe kaynağıdır. Bilgi aktarılırken, saklanırken veya virüsler tarafından dosya bozulması meydana gelebilir (Andress, 2014). Bütünlüğü korumak için, yalnızca verilerde yetkisiz ve/veya istenmeyen değişiklikleri engellemek için önlemlerin alınması gerekmez, Veri doğrulama ve doğrulama kontrolleri, yedekleme gerçekleştirme ve sürdürme ve karma oluşturma gibi veri bütünlüğünü korumanın ve sağlamanın birkaç yolu vardır.

Özgünlük: Özgünlük Parker'ın CIA modeline yaptığı eklemelerden bir diğeridir. Bir mesajın, işlemin veya diğer bilgi alışverişinin, geldiğini iddia ettiği kaynaktan geldiğine dair güvence anlamına gelir. Orijinallik, kimlik kanıtını içerir (Clemmer, 2010). Web üzerinden gerçekleştirilen işlemlere bağlı olarak iletişim kurduğunuz ve veri paylaştığınız anahtardır. İnternet, vergilerimizi ödemek, banka havalesi yapmak, alışveriş yapmak ve faturaları ödemek gibi evlerimizden hemen hemen her şeyi yapabilme olanağını sağladı. Bu faydalar ve diğer pek çok özellik nedeniyle, müşterilere ziyaret ettikleri sitenin meşru ve iletişimin güvenli olduğunu bilme güvenini vermek için teknolojiler geliştirilmiştir (Pender-Bey, 2019).

Kullanılabilirlik: Kullanılabilirlik, orijinal CIA modelinin son bileşenidir. Kullanılabilirlik, gerektiğinde kaynaklara sahip olma yeteneği olarak da tanımlanır. Tanımlanması daha basit bileşenlerden biridir, ancak ironik bir şekilde, korunması en zor olanlardan biridir. Günümüzde güvenlik uzmanları, ağları ve kaynaklarını güvence altına almakla görevlendirilirken, aynı zamanda kullanılabilirliği sürdürmek zorundadırlar. Günümüz teknolojik gelişmeleri ışığında tam güvenliği gerçekten sağlamanın tek yolu, sunucunun fişini çekmektir. Ancak gerek şirketler gerekse bireysel kullanıcıların önemli verileri bu şekilde işlevsiz olur. Yapılması gereken doğru kullanılabilirlik ve güvenlik dengesine ulaşmaktır (Pender-Bey, 2019).

Faydalılık: Faydalılık basitçe verilerin kullanılabilirliğini ifade eder. Bu, Parker altılısının son temel bileşenidir. Veri söz konusu olduğunda çok gözden kaçan bir konseptte odaklanır. Veriler, altı PH bileşeninden (gizlilik, bütünlük, kullanılabilirlik, özgünlük, sahiplik/kontrol) beşini karşılayabilir, ancak yararlı bir durumda mı? Fayda genellikle kullanılabilirlikle karıştırılır veya varsayılır, ancak ikisi farklıdır (Parker, 2010).

2.3. Siber Saldırı

Siber Saldırı ile ilgili birçok tanım bulunmaktadır. Hathaway ve diğerleri, (2012) “Politik veya ulusal güvenlik amacıyla bir bilgisayar ağının işlevlerini baltalamak için yapılan her türlü eylem. ”, Owens, Fulton, Jones ve Carlisle (2019) “Düşman bilgisayar sistemlerini veya ağlarını veya bu sistemlerde veya ağlarda bulunan veya bu ağlardan geçen bilgi ve/veya programları değiştirmek, bozmak, aldatmak, kalitesini düşürmek veya yok etmek için -belki de uzun bir süre boyunca- kasıtlı eylemlerin kullanılması. ”, Roscini ve Trust (2014) “ (a) propaganda veya aldatma ve/veya (b) hedeflenen bilgisayarın, bilgisayar sisteminin veya ağın ve (varsa) ilgili bilgisayar tarafından işletilen fiziksel altyapının işleyişini kısmen veya tamamen bozmak ve/veya (c) bilgisayara, bilgisayar sistemine veya ağa harici olarak fiziksel zarar vermek. ”, Uma ve Padmavathi (2013), “Yetkisiz veya güvenli bilgilere erişmek, casusluk yapmak, ağları devre dışı bırakmak ve hem veri hem de para çalmak amacıyla siber uzayın istismarı. ”, Staff (2010), “Bilgisayar veya ilgili ağları veya sistemleri kullanan ve bir rakibin kritik siber sistemlerini, varlıklarını veya işlevlerini bozmayı ve/veya yok etmeyi amaçlayan düşmanca bir eylem. ”, Waxman (2011), "Bilgisayar sistemlerini veya ağlarını veya üzerlerindeki bilgi veya programları değiştirme, bozma veya yok etme çabaları. " olarak tanımlanmıştır. Çalışmanın temelini oluşturan Ulusal Siber Güvenlik Belgesinde

(2020) “Siber uzaydaki bilişim ve endüstriyel kontrol sistemlerinin veya bu sistemler tarafından işlenen bilginin/verinin gizliliği, bütünlüğü veya erişilebilirliğini ortadan kaldırmak amacıyla, siber uzayın herhangi bir yerindeki kişi ve/veya bilişim sistemleri tarafından kasıtlı olarak yapılan işlemler.” olarak tanımlanmaktadır.

2.3.1. Siber saldırı türleri

Günümüzde dünyada gerçekleşen birçok siber saldırı çeşidi vardır. Çeşitli siber saldırı türlerini bilirsek, ağ ve sistemlerimizi bunlara karşı korumamız kolaylaşır. En önemli siber saldırı yöntemleri aşağıda sıralanmıştır:

1. DDOS (Hizmet Reddi Saldırısı)
2. Kimlik Avı
3. Kimlik Avı (Sosyal Mühendislik)
4. Man-in-the-middle attacks (Ortadaki Adam Saldırısı)
5. Mantıksal Bomba,
6. Oltalama (Phising)
7. Packet Sniffer (Koklayıcı),
8. Solucan,
9. Truva atı,
10. Virüs.

DDOS (Hizmet Reddi Saldırısı): Yetkili kullanıcıların sisteme erişimi veya tam tersi şekilde sistemin yetkili kullanıcılara erişimlerinin engellenmesidir. Bu tehlikeli bir elektronik saldırı formu olarak kabul edilir (Al Hayani ve Ilhan 2020). Saldırgan bir noktadan hedef bilgisayarları çeşitli mesajlara daldırmaya ve yasal veri akışını engellemeye başlar. Bu, herhangi bir sistemin interneti kullanmasını veya diğer sistemlerle iletişim kurmasını engeller (Panimalar, Pai, ve Khan 2018). Yaygın Hizmet Reddi adı verilen başka bir yöntemde, tek bir kaynaktan saldırı başlatmak yerine, aynı anda çok sayıda dağıtılmış sistemden saldırıyorlar. Bu genellikle solucanlar kullanılarak ve hedefe saldırmak için birden fazla bilgisayarda çoğaltılarak yapılır. Farklı beceri seviyelerine sahip ağlardaki güvenlik açıklarını algılayabilen ve girebilen kötüye kullanım araçları halka açıktır. Bu saldırı, birçok bilgisayarı kontrol etmeye ve aralarında botnet olarak bilinen robotik ağlar oluşturmaya yönelik bir bilgisayar programı ile başlar. Bu botnet' ler, bilgisayar korsanları

tarafından bir hizmet reddi saldırısı gerçekleştirmek için kullanılır. Kontrol edilen ağlar, kurbanın bilgisayar sistemini birkaç mesaj ve istekle doldurur. Bu temel hizmetlerin kesintiye uğramasına ve askıya alınmasına neden olur (Madeti ve Singh 2017; Panimalar vd. 2018). Dağıtılmış bir hizmet reddi saldırısı, sistem kaynaklarını tüketen bir saldırıyı ifade eder, ancak bu, saldırgan tarafından kötü niyetli programlara bulaşmış, zombi adı verilen çok sayıda ana makine tarafından gerçekleştirilir. Zombiler genellikle paketlerini kurban makinesine yönlendirir ve bu nedenle hizmet reddine neden olur. Hizmet reddinin ve dağıtılmış hizmet reddinin farklı biçimleri arasında smurf saldırısı, botnet' ler, teardrop saldırısı ve ping-of-death saldırısı bulunur.

Kimlik Avı: Genellikle toplum mühendisliğine dayanan bir yöntemdir. Kötü niyetli kişiler, kurbanlarını, kötü niyetli programlar içeren bir bağlantı açmaya motive eder ve bu nedenle, mağdurun ilgisini çekebilecek konuları içeren mesajlar göndererek veya kurbanın adını veya kötü amaçlı yazılımı kullanarak cihazlarına bulaşır. Mağdur bir mesajı açtığı anda, kötü niyetli kişi e-postalar, kişisel mesajlar ve hatta sosyal medya sitelerine yüklenen ve artık bu tür tehditlere ve saldırılara karşı savunmasız hale gelen uygulamalar aracılığıyla korsanlık sürecine başlar (Alhayani, Abbas, Khutar ve Mohammed. 2021).

Man-in-the-middle attacks (Ortakdaki adam saldırısı-MITM): Bu, bilgisayar korsanının gönderici ve alıcı arasındaki bir iletişim iletim kanalına girmesiyle meydana gelen bir saldırıyı ifade eder. Bu tür saldırılar, oturumun ele geçirilmesine, gizlice dinlenmesine ve hatta meşru kullanıcılar arasında iletilen bilgilerin değiştirilmesine neden olur. Oturum kaçırmaya, bilgisayar korsanlarının iki güvenilir istemci ve ağ sunucusu arasındaki oturumu devraldığı bir MITM saldırı biçimini ifade eder. Bu saldırıda, ağ sunucusu oturuma devam ederken saldırgan bilgisayar güvenilen istemcinin IP adresini değiştirecektir. Dolayısıyla meşru kullanıcılar, doğru kişiyle iletişim kurduklarına inanmaya devam edeceklerdir. Bir ortakdaki adam saldırısının bir biçimi olan IP sahtekarlığı, saldırgan tarafından herhangi bir sistemi bilinen ve güvenilen varlıkla iletişim halinde olduğuna ikna etmek için kullanılır ve böylece saldırgana sisteme erişme yeteneği sağlar. Ardından saldırgan, hedeflenen ana bilgisayara kendi IP kaynak adresiyle değil, bilinen ve güvenilen ana bilgisayarın IP adresiyle paketleri kolayca gönderir(Zhu, Ji ve Liu, 2014; Mohsin ve diğerleri. 2019;) . Sonunda, hedef ana bilgisayar bu paketi kabul edebilir ve buna göre hareket edebilir. Bir MITM saldırısı biçimi olarak yeniden oynatma, saldırganın iletişim kanalını ele geçirmesi

ve eski mesajları kullanması ile gerçekleşir. Daha sonra kendilerini meşru katılımcılar olarak taklit ederek onları daha sonra göndermeye çalışır.

Mantıksal Bomba: Bir programcının belirli bir olay olması durumunda programın otomatik olarak yıkıcı bir faaliyet gerçekleştirdiği bir programa kod girdiği başka bir saldırı türüdür (Fratantonio ve diğerleri, 2016).

Olta (Phishing): Kimlik avcılığı tarafından kullanılan bir stratejidir. Bu stratejiler, taklit saldırı, ileri saldırı ve açılır saldırı olarak üç gruba ayrılır. Kimlik avcılığı, saldırıyı taklit ederek kurbanlarını, meşru bir kuruluştan gelen resmi bir e-postayı taklit eden e-posta yoluyla kişisel bilgilerini açıklamaları için cezbeder. İleriye dönük saldırı ve açılır pencere saldırıları, kimlik avcısının bir proxy web sitesi (ileriye yönelik saldırı) veya bir açılır pencere (açılır pencere) aracılığıyla kurbanın kişisel bilgilerini ele geçirdiği ve aldığı ortadaki adam (MITM) yöntemlerinin kullanımını içerir (Mohammad, Thabtah, ve McCluskey 2015).

Packet Sniffer(Koklayıcı): Yönlendirilmiş bilgileri gizlice dinleyen ve veri akışındaki her paketi inceleyerek şifreler gibi belirli bilgileri arayan bir programdır (Tomer, Lade, Kumar ve Patel, 2013).

Solucan (Worm): Solucan, bir bilgisayardan diğerine bulaşırken sadece kendisini bilgisayarın işletim sistemine veya bulaştığı bilgisayara bağlamaz. Aynı zamanda bir geçiş programı olan bir virüsten farklıdır. Kendisini girdiği herhangi bir bilgisayarın işletim sistemine ilişitir ve virüslü bilgisayardaki dosyaları kullanan diğer herhangi bir bilgisayara bulaşabilir. Başka bir deyişle solucan, kendi imkânlarıyla bir bilgisayar sistemine bulaşabilen ve onu otomatik bir şekilde kullanarak başka bir sisteme bulaşabilen bir yazılım bileşenidir. Bu döngü daha sonra tekrarlanır ve solucan bulaşmış konakların popülasyonu katlanarak artar (Yu, Boyer, Chellappan ve Xuan, 2005).

Truva Atı: Truva atı tehlikeli kodu gizler ve genellikle kullanıcının çalıştırmak istediği yararlı bir program gibi görünür (Das Purba, Chu, ve Al-Shaer 2020). Ayrıca, bir virüs, yaygın olarak uygulanabilir programlar olan sistem dosyalarını, bu dosyalara bir kopyasını ekleyerek bozar. Bu sürümler, virüslü dosyaları belleğe yükleyerek çalışır ve virüsün diğer dosyalara bulaşmasına izin verir. Solucanların aksine, virüslerin yayılması için insan

müdahalesi gerekir. Öte yandan solucan, ağdaki bir bilgisayardan diğerine kopyalayarak kendini yenileyen otonom bir sistem programıdır (Aziz ve Amtul 2019).

Botnet: Kötü amaçlı yazılımları dağıtmak, saldırıları koordine etmek ve istenmeyen postaları göndermek ve mesajları çalmak için kullanılan virüslü uzaktan kontrol sistemlerinden oluşan bir ağıdır. Botnet'ler genellikle hedef bilgisayara gizlice yüklenir ve yetkisiz kullanıcının kötü niyetli hedeflerine ulaşmak için hedef sistemi uzaktan kontrol etmesine izin verir. Botnet'lere elektronik askerler de denir (Kharlamova, Hashemi, ve Træholt 2021).

Virüs: Bilgisayar virüsleri, kendilerini çoğaltabilen ve kablolu veya kablosuz ağlar aracılığıyla yayılabilen kötü amaçlı kodlar veya programlardır (Yang, Yang, Zhu ve Wen, 2013). Virüsler, diğer programlara bağlanan ve kendini çoğaltarak sisteme bulaşan ve bu nedenle kullanıcı yetkilendirmesini virüse daha açık hale getiren ve kötü amaçlı programları yayarak tüm sistemi veya ağı sömürebilecek bir programdır. Bu programlar verilere, disklere, dosya silme ve şifrelemeye bulaşmak için çok büyük işlemler gerçekleştirebilir (Raja ve diğerleri. 2022). Farklı virüs kategorileri arasında ön yükleme sektörü, yerleşik, çok parçalı, çok biçimli, üzerine yazma, web komut dosyası oluşturma, tarayıcı korsanı, e-posta virüsü ve diğer birkaçı bulunur. Bilgisayar ağının kullanıcılar tarafından farklı şekillerde kullanımı her geçen gün arttığından, kötü amaçlı yazılımlardan arınmış bir ağ sağlanması gerekmektedir (MadhuSudanan ve Geetha 2020).

SG kapsamında basit güvenlik uygulamalarının uygulanmasına ihtiyaç vardır. Bunlar şu şekilde sıralanabilir (Stewart ve Jürjens 2017).

1. Teknik önlemlerin alınması: Bu tür önlemler, elektronik saldırılara yardımcı olan ters izleme teknolojilerinin geliştirilmesi ve sistemlere yerleştirilmesidir. Böylece saldırıları başlangıç aşamalarında hızlı bir şekilde algılayarak gerekli önlemlerin alınmasına ve ağda bulunan bilgilerin yedeklenmesine yardımcı olacaktır. Haberleşme, altyapı veya internet ağları olsun, orijinal verilerin kaybolması durumunda veri yedeklemesine ihtiyaç vardır. Ağ güvenliği yapısının gözden geçirilmesi ve çevresel güvenlik anlayışının benimsenmesi, siber güvenlik davranışına bireysel davranışlardan bağımsız olarak tüm unsurların dâhil edilmesine yardımcı olur.

2. Siber İttifak Sağlanması: Geleneksel ittifakın kapsamının genişletilmesi, bazı ülkelerin siyasi anlaşmalarını imzalarken siber güvenliğin sağlanmasından sorumlu işlevler arasında yer almasına ihtiyaç vardır. Bunlar NATO ittifakını da içermektedir.
3. Siber yeteneklerin geliştirilmesi: Ülkelerin, özellikle daha akıllı teknolojilerin yaratılmasına yardımcı olacak çocuklar arasında insan unsuruna yatırım yapmasına ihtiyaç vardır. Ayrıca teknoloji şirketlerinin çocukları bilgilendirmesi, veri gizliliği ve bilgi güvenliği alanında yenilikleri ve yetenekleri teşvik etmesi ve ardından onlar için bu tür yarışmalar düzenlemesi gerekmektedir. Bu onların temel unsurları keşfetmelerine ve yeteneklerinin benimsenmesine yardımcı olacaktır.
4. Toplum bilincinin sağlanması: Hükümetler, siber uzayın tehditlerine ilişkin programlarda ve mevcut teknolojilerden nasıl yararlanacaklarını ve tehditlerinden nasıl kurtulacaklarını anlamalarına yardımcı olan çeşitli teknolojik uygulamalar hakkında toplumla ilgili üye farkındalığını değiş tokuş etmelidir ve bu, aşağıdakiler arasındaki bir ortaklık yoluyla sağlanır.
5. Siber güvenlik sigortasına yatırım yapılması: Siber suçluların çoğu, güvenliklerinin en bilinçli şirketlerinin bile hala saldırıya uğrama riskleriyle karşı karşıya kalması için oluşturulmuş güvenlik savunma hatlarını ihlal etmenin karmaşık yollarını bulmaya çalışır. Bu nedenle şirketler siber saldırı sonucu uğrayabileceği veya üçüncü şahıslar tarafından yöneltilebilecek tazminat taleplerini karşılayabilmek için güvenlik sigortalarına yatırım yapmaktadırlar.
6. Verilerin şifrelenmesi ve yedeklenmesi: Siber suçtan etkili bir şekilde kendini koruma, iki unsura ihtiyaç duyan bir stratejidir. Özel verilere veya bilgilere erişimi reddetmek ve bu verileri izinsiz erişecek saldırgan için işe yaramaz hale getirmektir. Bu, her zaman kurumsal veriler şifrelenerek yapılır.

Ülkemizde siber güvenlik eğitimleri MEB ve YÖK' e bağlı akademik kurumların müfredatlarında yer almasına rağmen yeterli düzeyde değildir. Bilgi Güvenliği Derneği

(BGD), Türkiye Bilişim Derneği (TBD) sivil toplum kuruluşları (STK) ya da özel organizasyonlar tarafından da verilen bu eğitimler kullanıcılarda bu farkındalığın oluşturulması ve toplumun geneline yayılması için en önemli etkidir. Siber güvenlik alanında farkındalık ve eğitim çalışmaları ilkokuldan itibaren verilmeli ve eğitim sisteminin her kademesinde ilgili ders müfredatı ile ilişkilendirilmelidir. Gelecek nesillerde “Siber Vatandaş” bilinci oluşturulmalıdır(Ünver, 2012). Siber saldırıları ve riskleri azaltmak için siber güvenlik farkındalığının artırılması gerekmektedir (Kaur ve Ramkumar, 2022).

2.4. Siber Güvenlik Farkındalığı

Grabosky, (2016) “siber suçların önlenmesi ve kontrolü için en önemli stratejilerden birinin, özel kişi ve kurumların karşı karşıya olduğu riskler ve bunların en iyi şekilde nasıl en aza indirilebileceği konusunda kamu bilincini artırmak olduğunu” belirtmektedir. Kullanıcının kötü amaçlı olayları algılama şekli, bir ağ olayını yorumlamalarına yardımcı olan bilgi havuzlarına bağlıdır. Daha sonra, bir olaya yol açan çeşitli nitelikler arasında var olan bağlantıları anlayabilir ve belirli bir ağ etkinliğine göre onu yargılayabilirler(Al-Ghamdi, 2021).

Saldırganlar, yazılım ve donanımdaki güvenlik açıklarından yararlanarak siber uzayda yer alan bilgilere izinsiz erişebilmektedirler. Virüslü e-postaları açmaları veya bilgisayarlarına kötü amaçlı yazılım bulaştıran bozuk web sitelerini ziyaret etmeleri için kullanıcıları manipüle etmektedirler. Parolalarını sık sık değiştirmeyen, antivirüs korumasını düzenli olarak güncellemeyen ve yalnızca korumalı kablosuz ağları kullanmak gibi temel siber güvenlik uygulamalarını takip etmeyen kişiler saldırganların birincil hedefleridir. Çok sayıda güvenlik ihlali, bilgi eksikliği veya güvenli olmayan davranışlardan kaynaklanmaktadır. Kullanıcıların siber güvenlik bilgisi, gelişen internet teknolojileri, kullanıcı davranışlarındaki değişiklikler ve uzaktan iletişimin yaygın uygulamasını destekleyen bankacılık, sosyal ağ ve bilgi ekonomisi gibi çevrim içi hizmetlerin yaygın kullanımı ile başa çıkmak için önemlidir (Thomson ve von Solms, 1998; Whitson, 2009).

Alanyazın incelendiğinde siber güvenlik farkındalığına (SGF) dair birçok tanım karşımıza çıkmaktadır. Abd Rahim ve diğerleri (2015) SGF’yi “İnternet kullanıcılarını çeşitli siber tehditlere ve bilgisayarların ve verilerin bu tehditlere karşı savunmasızlığına karşı duyarlı olmaları için eğiten bir metodoloji” olarak tanımlamıştır. Shaw ve diğerleri (2009) ise

“kullanıcıların bilgi güvenliğinin önemi ve kuruluşa ait dataları ve ağ yapılarını güvende tutmak için yeterli düzeyde bilgi sahipliği, uygulama sorumluluklarını anlama derecesi” olarak tanımladı. Siber hijyen olarak da SGF, bilimsel literatürde ve politika yapıcılar tarafından sıklıkla dile getirilmektedir. Ancak akademik araştırmalarda bu terimin ortak bir tanımı yoktur. SG, “çevrimiçi tüketicilerin kişisel bilgilerinin ve işverenlerinin internet özellikli cihazlarındaki bilgilerinin güvenliğini ve bütünlüğünü bir siber saldırıda ele geçirilmekten korumak için benimsemeleri gereken siber güvenlik uygulamaları” ile ilgilidir (Vishwanath ve diğerleri, 2020).

Bu tanımlara dayanarak, siber güvenlik bilincinin iki temel amacı vardır: internet kullanıcılarını siber güvenlik riskleri hakkında uyarmak ve internet kullanıcılarının siber güvenlik risklerini anlamalarını sağlamak. SGF, insan kaynaklı hataların veya güvenlik açıklarının azaltılması, güvenliğin kişisel veya kurumsal düzeyde iyileştirilmesinde kilit bir faktördür (Giannakas, Papasalouros, Kamburakis ve Gritzalis, 2019). İnsan kaynaklı hataların veya güvenlik açıklarının azaltılması, için siber güvenlik ve gizlilik sorunları hakkında kullanıcı farkındalığı artırılmalıdır.

Fielding (2020), kurumlar için hayati önem taşıyan SG' yi sağlamak için gerekli olanları şu şekilde açıklamıştır: “Kuruluşların yapabileceği şey, tüm çalışanların karşılaştıkları risklerin ve ciddi veri kaybı ve hizmet kesintilerinin işverenleri üzerindeki etkilerinin farkında olduğu, güvenlik öncelikli bir kültür oluşturmaya yardımcı olmaktır” SG eğitimi ve farkındalığı artırma faaliyetleri SG'yi sağlamanın ilk adımıdır. Eğitim programları, geçici çalışanlar, yükleniciler, yarı zamanlı çalışanlar ve üst düzey yöneticiler dâhil olmak üzere tüm çalışanlara odaklanmalıdır. Her şey doğru türde bir program oluşturmakla ilgilidir. Gerçek dünya senaryolarını içeren simülasyon alıştırma çalışmalarının, özellikle kısa, 15 dakikalık aralıklarla- az ve sık sık- iletilirse, istenen etkiye sahip olma olasılığı yüksektir. Egzersizleri kendileri yapmak kadar önemli olan, bireylere performansları ve nerede iyileştirmelerin yapılması gerektiği konusunda geri bildirimde bulunmaktır. İnsanlara her şeyin neden olduğu gibi olması gerektiğini açıklamak ve neleri farklı yapmaları gerektiği konusunda onları eğitmek önemlidir. Unutulmaması gereken, bu belirsiz "yetiştirme" kavramıyla ilgili değildir. Farkındalık ile davranışları değiştirmektir. Bu, herhangi bir programın değerlendirilmesi gereken özelliğidir.

Dikkat edilmesi gereken en önemli husus insanların SG bilgi düzeyi ve farkındalığının her bireyde farklı olması ve bu farkın nedenlerinin tespit edilmesidir. Kullanıcıları ve güvenlik davranışlarını etkileyen faktörleri daha iyi anlamaya çalışan önemli miktarda araştırma vardır. Bazı araştırmacılar, zayıf güvenlik uygulamaları, kimlik avı veya sosyal mühendislik gibi siber suçların kurbanı olma konusundaki artan duyarlılıkla ilişkili insan özelliklerinde farklılıklar tespit etmiş olsa da bu alandaki çalışmalar hala (Egelman ve Peer 2015). Kullanıcıların bireysel farklılıklarının siber güvenlik davranış niyetlerini nasıl etkilediğini anlamak, araştırmacıların, güvenlik uzmanlarının ve kuruluşların zayıf veya potansiyel olarak tehlikeli güvenlik uygulamalarına daha duyarlı kullanıcıları belirlemesine yardımcı olmak için kritik öneme sahiptir. Bu tür içgörüler, uygulayıcıların hedeflenen eğitim çabalarını geliştirmelerine ve topluluklarında genel siber güvenlik için en büyük zorluğu oluşturan kullanıcılara hitap etmeye odaklanmalarına yardımcı olabilir (Gratian, Bandi, Cukier, Dykstra ve Ginther, 2018).

Egelman ve Peer (2015) tarafından önerilen dört ana kullanıcı güvenlik davranışı kategorisine odaklanmak kullanıcıları sınıflandırmaya ve onların SGF davranışlarını incelemek için uygun bir yöntemdir. Bu güvenlik davranışları cihaz güvenliği, parola oluşturma, proaktif farkındalık ve güncellemedir. Cihaz Güvenliği, cihazları kilitlemek, otomatik cihaz veya ekran kilitlemeyi ayarlamak ve cihazları gözetimsiz bırakmadan önce manuel olarak güvenceye almak için PIN'lerin ve şifrelerin kullanılması anlamına gelir. Parola oluşturma, güçlü parolalar seçmeyi ve parolaları farklı hesaplar arasında yeniden kullanmamayı ifade eder. Proaktif farkındalık web sitelerinde veya e-posta mesajlarında URL çubuğu veya diğer tarayıcı göstergeleri gibi bağlamsal ipuçlarına dikkat etmeyi, web sitelerine bilgi gönderirken dikkatli olmayı ve güvenlik olaylarını bildirirken proaktif olmayı ifade eder. Son olarak güncelleme, kullanıcıların sürekli olarak güvenlik yamalarını ne ölçüde uyguladıklarını veya yazılımlarını başka bir şekilde güncel tuttuklarını ölçer (Gratian ve diğerleri, 2018).

SGF' de bireysel farklılıklar, insanlar arasında değişen çok çeşitli değişkenleri kapsayabilir (Egelman ve Peer, 2015). "Demografik Faktörler, Kişilik Özellikleri, Risk Alma Tercihleri ve Karar Verme Stilleri" dört ana bireysel farklılık olarak kategorize edilmiştir. Demografi, bir insan popülasyonundaki bir dizi özelliği kapsar. Yaş farkı ve cinsiyet farkı bu demografiye örnek verilebilir. Kullanıcıların uyumluluk, vicdanlılık, nevrotiklik, açıklık ve dışa dönüklük gibi kişilik özellikleri, cihaz güvenliği, parola oluşturma, proaktif farkındalık

ve güncelleme konusundaki güvenlik davranışı niyetleriyle ilişkili olacağına dair çalışmalar mevcuttur. Kişilik özellikleri, büyük ölçüde kimlik avına yatkınlık bağlamında incelenmiştir. Halevi, Lewis, ve Memon (2013), yüksek nevrotiklik ve kimlik avı duyarlılığı olan kadınlar arasında bir ilişki ve açıklık ile zayıf mahremiyet ayarları arasında bir ilişki buldu. Pattinson (2012) yüksek açıklık ve dışa dönüklüğün, düşük kimlik avı duyarlılığıyla ilişkili olduğunu bulmuştur. Risk alma, risk tutumunun bir ölçüsüdür ve literatürde çeşitli riskli davranış biçimleriyle ilgili olarak incelenen karar vermeyi şekillendirmektedir. Güvenlik davranışlarıyla ilgili olarak incelenen risk alma tercihlerinin etik, finansal, sağlık/güvenlik, eğlence ve sosyal risk alma olmak üzere beş boyutu vardır (Egelman ve Peer, 2015). Karar verme stili, bir karar verme durumunda bireyin sergilediği tepki örüntüsüdür (Thunholm, 2004). Karar verme stilleri rasyonel, kaçınma, bağımlı, sezgisel ve spontan karar verme olmak üzere beş geniş kategoriye ayrılır. Rasyonel, karar verirken mantık kullanmayı ifade eder; kaçınma, karar vermeyi geciktirmeyi ifade eder; bağımlı, karar verme yardımı için başkalarına güvenmeyi ifade eder; sezgisel, içgüdülere dayalı karar vermeyi ifade eder; son olarak, kendiliğinden, hızlı karar vermeyi ifade eder (Scott ve Bruce, 1995). Egelman ve Peer (2015), hem bağımlı karar verme hem de anlık karar vermenin iyi güvenlik davranışlarıyla ters orantılı olduğunu bulmuşlardır.

Siber tehditler her yaşta kullanıcıyı tehdit ederken çocuklar siber uzaya ve siber tehditlere önceki nesillere göre daha fazla maruz kalmaktadır (Snyman ve diğerleri. 2021). COVID-19 salgını sırasında okulların kapanması ve derslerin çevrimiçi verilmesi, çocukları siber saldırılara ve kötü amaçlı yazılımlara eğilimli hale getirmiştir (Yuliana 2022). Bu nedenle, çocuklar arasında siber güvenlik farkındalığı kritik öneme sahiptir. Sonuç olarak, sayıları hızla artan siber saldırılara karşı savunma yapabilmek için sıradan insanların siber güvenlik farkındalık düzeylerinin önemli ölçüde artırılması gerektiği açıktır (Alzubaidi 2021).

2.5. Çocuklarda Siber Güvenlik Farkındalığı

Çocuklar, tehditlerin çeşitli yönlerine karşı en savunmasız olduğu kadar en masum olarak kabul edilir. Suç faaliyetleri, sosyal faaliyetler veya dijital faaliyetler olsun, çocuklar her yerde çalışan suçlu beyinler için kolay bir av olarak kabul edilir. Dijital dünyamızda her geçen gün yaşanan gelişmeler sayesinde çocuklar çeşitli akıllı cihazlara ve dijital kaynaklara bağımlı hale gelmektedir. Çocukların sağlık ve esenliği ile ilgili zorluklar dışında, çocuklar

bu teknolojilerin sürekli ve yönetilmeyen kullanımıyla ilgili zorluklara ve risklere karşı daha yatkın ve savunmasız olarak kabul edilir (Siddiqui ve Zeeshan 2020).

Çocuklar, özellikle internette özel verileri başkalarıyla paylaştıklarında sunulan kontrollerin olmaması nedeniyle tehlikeye atılabilir. Günümüzün bağlantılı dünyasında çocukların karşılaştığı tehlikeler ve riskler, yabancı tehlikesi, cinsel iletişim, siber zorbalık ve gelecekte kullanılmak üzere rutin olarak saklanan kişisel verilerin toplanmasına kadar geniş ve (Dempsey ve diğerleri. 2022). Birleşik Krallık'ta 8-11 yaşındakilerin yaklaşık %18'i endişe verici veya kötü olduğunu düşündükleri çevrim içi içerik gördüklerini bildirmişlerdir (Bentley ve diğerleri. 2020). Gizlilik riskleri konusunda farkındalık eksikliği nedeniyle, çevrim içi gizlilik tehditleri söz konusu olduğunda çocuklar genellikle yetişkinlerden daha savunmasız olarak görülüyor (Livingstone, Stoilova, ve Nandagiri 2019).

“Dijital ortam, çocukların şiddete maruz kaldığı ve/veya kendilerine veya başkalarına zarar vermekten etkilenebilecekleri durumları kolaylaştırarak, çocuklara yönelik şiddet uygulamak için yeni yollar açabilir. Pandemi gibi krizler, çocukların bu koşullarda sanal platformlarda daha fazla zaman harcadıkları göz önüne alındığında, çevrim içi zarar riskinin artmasına neden olabilir.” (Birleşmiş Milletler, 2021). Birleşmiş Milletlere üye olan ve Türkiye dâhil 196 ülke tarafından imzalanan çocuk hakları sözleşmesi uyarınca sözleşmeye taraf devletler çocukları dijital ortamdaki şiddetten korumak için yasal ve idari önlemler almalıdır. Bu önlemler, çocukları kendi ülkelerinde kabul edilen ve ortaya çıkan her tür şiddet riskinden koruyan sağlam yasal, düzenleyici ve kurumsal çerçevelerin düzenli olarak gözden geçirilmesi, güncellenmesi ve uygulanması da dâhildir. Bu tür riskler arasında fiziksel veya zihinsel şiddet, yaralanma veya istismar, ihmal veya kötü muamele, cinsel sömürü ve istismar dâhil olmak üzere sömürü ve istismar, çocuk kaçakçılığı, cinsiyete dayalı şiddet, siber saldırganlık, siber saldırılar ve bilgi savaşı yer alır. Taraf Devletler, çocukların gelişen yeteneklerine uygun olarak güvenlik ve koruyucu önlemler almalıdır (Birleşmiş Milletler, 2021).

Çocuklar, akranları ve aileleri de dahil olmak üzere insanlarla etkileşim kurmak için günlük yaşamlarında teknolojiyi giderek daha fazla kullandıklarından, çocukların interneti kullanırken karşılaşacakları riskleri yönetmelerine yardımcı olacak stratejiler geliştirilmelidir (Lobe ve diğerleri, 2020; Smahel ve diğerleri, 2020). Akıllı oyuncaklar ve giyilebilir aktivite izleyiciler gibi çocukların kullandığı akıllı teknolojiler ve diğer dijital

cihazlar, sensörler ve yapay zekâ aracılığıyla fiziksel ve dijital dünyalara aracılık eder ve çocukların kişisel dijital verilerinin toplanmasına katkıda bulunur. Ancak, çocukların bu süreçleri nasıl algıladıklarına ve dijital veri üretiminin doğasında bulunan gizlilik risklerine ilişkin görüşleri literatürde sınırlıdır (Trueltzsch-Wijnen ve diğerleri, 2018).

Çocuklar sadece teknoloji konusunda bilgili değil, aynı zamanda teknolojiyi kullanma konusunda da yetkindirler. Aslında, çocuklarına sınavlarda, doğum günü hediyelerinde vb. mükemmellik için ödül olarak alet veren ebeveynler de bulunmaktadır. Böyle bir durum küçük çocukları interneti sınırsız veya izleme olmadan bağımsız olarak keşfederken teknoloji aracılığıyla istismara karşı savunmasız hale getirir. İnternetin faydalarından yararlanırken, çocukların artık daha erken yaşlarda internet erişimine sahip olması nedeniyle, ebeveynlerin veya çocukların siber zorbalık gibi potansiyel risklerin farkında olması ve güvenlik önlemleri alması önemlidir (Ab Hamid, Yunos, ve Ahmad 2018). Çocukların internet kullanımı, önemli toplumsal, pazar ve teknolojik yeniliklere yanıt olarak hızla değişmektedir. Sık sık çevrim içi video, müzik, oyun, mesajlaşma ve arama yapmalarından da anlaşılabileceği gibi, internet kullanımları genel olarak olumludur. Üç ila dört yaşındaki çocukların ebeveynleri, çocuklarının YouTube'da çizgi film, mini film, animasyon veya şarkı izleme olasılığının yüksek olduğunu bildiriyor. Daha büyük çocuklar daha fazla müzik videosu, vlogger, YouTube kişilikleri ve komik videolar izledikleri için, çocukların büyüdükçe izledikleri içerikler de farklılaşmaktadır (Ofcom 2016).

Genç kullanıcıların siber güvenlik konusunda eğitilmeleri zorlu bir süreçtir. Alan yazın incelendiğinde mevcut siber güvenlik farkındalık eğitim modüllerinin genç kullanıcılara kişisel verilerin korunmasına ilişkin bilgi aktarılmasındaki etkinliğini araştırmak için birçok çalışma yapılmıştır (Erol ve diğerleri, 2015; Alotaibi ve diğerleri 2016). Siber güvenlik farkındalığını değerlendirirken kullanıcıları kategorilere ayırmak, doğru siber güvenlik mesajının doğru kitlelere iletilmesini sağlamak için gereklidir. Bu nedenle, özellikle çocuklar açısından, onları tek bir birim olarak incelemeye hala yeterli önem verilmemektedir. Değerlendirme kapsamı olarak çocuklar, bu tür siber tehdide daha fazla maruz kaldıkları ve sadece kendilerine değil ailelerine de zarar verecekleri için kimlik hırsızlığı ile mücadeleye yardımcı olmayı amaçlamaktadır. Belirlenen bu boşluk, çocukların geri bildirimleri ve kişisel verilerin korunmasına ilişkin anlayışları açısından değerlendirmenin etkili bir yolunun planlanmasında iyi olabilecek, kaçırılmış bir fırsat olarak görülebilir (Rahim, Hamid, Kiah, Shamshirband ve Furnell, 2015).

Çocuklarının internette ne yaptığı hakkında çok az bilgiye sahip olan ebeveyn sayısının fazla olması, siber güvenlik tehditleri konusundaki farkındalığın hala düşük olduğunun bir göstergesidir. Bu daha çok, ebeveynlerinin teknolojik olarak zorlandığını fark eden çocukların anlayışsız bakışları aracılığıyla bariz bir dezavantaj olarak görülüyor (Byrne, Katz, Lee, Linz ve McIlrath, 2014). Çocukları ekran başındayken, her 10 ebeveyninden sadece 4'ü çocuklarının internette hangi içeriklerle ilgilendiğini biliyor. Çoğu durumda, ebeveynler, çocuklarının izinsiz erişimlerinin ve uygunsuz çevrim içi sitelere maruz kalmalarının farkında değiller ve bu da çocukları siber güvenlik tehdidine maruz bırakmaktadır (Ahmad ve diğerleri, 2018). Çocukların maruz kaldığı tehlikeler incelendiğinde atılması gereken adımlar için bir yol haritası oluşturulabilecektir.

2.5.1. Çocuklara yönelik siber tehditler

Çocuklar sosyal, fiziksel ve duygusal esenliği üzerinde kısa ve uzun vadeli etkisi olabilecek siber uzayla bağlantılı bir dizi siber risk ve tehdit vardır (Byron, 2008). Alanyazın incelendiğinde Valcke, Wever, Keer ve Schellens, (2011), çocukların karşılaşılabileceği çevrim içi riskleri tartışmış ve çocuklara yönelik çevrim içi riskleri üç temel risk türüne ayırmıştır. Birincisi içerik riskleri ve içerik örneği çevrim içi yanlış bilgi riskleridir. İkincisi, siber zorbalık ve mahremiyet riskleri gibi temas riskleridir. Üçüncüsü, kişisel verilerin toplanması gibi ticari risklerdir. Öte yandan Livingstone, Giovanna, Mascheroni ve Staksrud (2015), çevrim içi riskleri içerik riskleri, iletişim riskleri ve davranış riskleri olarak sınıflandırarak farklı çevrim içi risk türlerini inceledikleri araştırmalarında çocuk ne kadar küçükse, takip etme, tımar etme ve zorbalık gibi çevrim içi risklere maruz kalma şansının o kadar yüksek olduğunu belirtmişlerdir.

Slavtcheva-Petkova, Nash, ve Bulger (2015) çocukların interneti kullanırken karşılaşılabilecekleri risklerin çok büyük olduğunu, çok ciddi olarak sınıflandırılan bu risklerden bazılarının diğer risklere göre küçük bir yüzde olabileceğini, diğer risklere göre de ciddi olduğunu ifade etmiş ve riskleri inceleyen araştırma makalelerini incelerken, bahsedilen ana çevrimiçi risklerin pornografi, siber zorbalık, cinsel mesaj gönderme ve alma, kimlik hırsızlığı ve kimlik avı olduğunu belirtmiştir. Stone'a (2013) göre, okul öğrencileri (çocuklar) için siber riskler Çizelge 2.1.'de gösterildiği gibi üç ana kategoriye ayrılabilir.

Çizelge 2.1. Öğrencilerin siber dünyada karşılaştığı tehlikeler (Stone, 2013)

Bireylerin(Saldırganların) öğrenciye zarar verme niyeti	Öğrencilerin zararlı çevrimiçi etkileşimlere maruz kalması	Öğrenci kendini zararlı bir duruma sokar
•Siber Zorbalık •Trolleme, •Alevlendirme, •Dışlama, •Maskeleye, •Mobbing, •Karalama, •Dolandırma, •Taciz, •Siber tımar, •Kimliğe bürünme, •Şantaj, •Siber gözetleme, •Kimlik hırsızlığı, •Sosyal mühendislik,	•Uygunsuz içerik/materyal, •Dijital itibarın zedelenmesi, •Sosyal platformlar ve sohbet odaları, •Virüsler, kötü amaçlı yazılımlar, çerezler	•Yasa dışı dosya paylaşımı, •İntihal, •Çevrimiçi uygunsuz paylaşım, •Ücretsiz indirme, •Telif hakkı ihlalleri, •Başkalarının materyallerinin etik olmayan gönderileri, • Cinsel mesajlar

Yukarıda bahsedilen çevrim içi riskler incelendiğinde, özellikle çevrim içi risklerin olumsuz etkilerinin boyutunun ve nasıl doğru tepki verebileceklerinin farkında olmayan çocuklarımızın interneti kullanırken karşılaşılabilecekleri tehdidin ne kadar büyük olduğu dikkat çekmektedir (Al Shamsi, 2019). Yukarıdaki konuların yanında öğrencilerin karşılaştıkları ve önlen alınması gereken SG ile ilgili sorunlar şunları içerir: parolaların korunması; gizlilik ayarlarını yönetme, siber görgü kurallarına bağlı kalma, başlangıçta çevrim içi tanıştığınız insanlarla gerçek hayatta tanışmak, yaşa uygunluk ve dijital ayak izi. Okul öğrencileri, etkili farkındalık programları ve eğitim yoluyla kendi siber güvenliklerinin sorumluluğunu almaya teşvik edilmeli ve donatılmalıdır (Kritzing, Bada, ve Nurse, 2017).

2.5.2. Çocuklara yönelik siber güvenlik farkındalığı çalışmaları

Bu bölümde çocuklara yönelik siber güvenlik farkındalığı alanında yurt içi ve yurtdışında yapılan çalışmalar incelenmiştir.

Tekerek A. ve Tekerek M. (2013) ilköğretim ve lise öğrencilerinin bilgi ve bilgisayar farkındalık düzeylerini ortaya çıkarmak amacıyla 2.449 öğrencinin katılımıyla gerçekleştirdikleri çalışmalarında öğrencilerin güvenli şifre kullanımı, çevrimiçi güvenli

iletiřim, kötü amaçlı yazılım incelemesi yapma, belge koruma, kişisel bilgisayar güvenlięi, güvenlik duvarı ve filtreleme yazılımı kullanımı, internet üzerinden arkadaş edinme ve internetin güvenli bir alan mı olduęu konularında farkındalık düzeyleri oldukça düşük olduęu sonucuna ulaşmışlardır. Ek olarak kız öğrencilerin erkek öğrencilere oranla bilgi güvenlięi farkındalıęının yüksek olduęu, öğrenim seviyesi arttıkça yine bilgi güvenlięi farkındalıęının arttığı, yerleşim yerine bakıldığında ise benzer şekilde ilçe merkezinde bulunan öğrencilerin farkındalıęının anlamlı oranda yüksek olduęu tespit edilmiştir.

Karakuş, Çağıltay, Kaşıkçı, Kurşun ve Ogan, (2014) Avrupa Çevrim içi Çocuklar projesine dâhil olan Türkiye ve 23 Avrupa ülkesinden 9-16 yaş aralıęındaki çocuklar ve ebeveynleri ile nitel araştırma gerçekleştirerek çocukların ve ebeveynlerinin İnternet kullanımları, çocukların internetteki faaliyetleri, karşılaştıkları riskler ve ebeveynlerin çocuklarının internet yaşantıları ile ilgili farkındalıkları raporlamışlardır. Çalışma bulgularında ülkemizdeki çocuk ve ebeveynlerin SGF’ de Avrupa ortalamalarının gerisinde kaldıkları, internet kullanımı konusunda kendilerine güvendikleri ancak internet becerileri konusunda yeterli olmadıklarını ortaya koymuştur. Bu sonuçlar karşılaşılabilecekleri riskler karşısında yetersiz kalabileceklerini göstermiştir.

Hacımustafaoğlu, (2019) ortaöğretim öğrencilerinin bilgi güvenlięi farkındalıkları ve siber mağdur olmalarının farklı değişkenlere (cinsiyet, kardeş sayısı, anne ve baba eğitim düzeyi, sınıf düzeyi, günlük internet kullanım süresi ve kişisel bilgisayar, tablet bilgisayar veya akıllı telefon sahibi olma) açısından incelemiştir. Çalışma sonuçları incelendiğinde ortaöğretim öğrencilerinin bilgi güvenlięi farkındalıklarının orta düzeyde olduęu ölçeğin alt faktörlerine ait puanlar incelendiğinde ise kişisel verilerin korunması alt boyutunda farkındalıklarının ortalamanın üstünde, saldırı ve tehditler alt boyutunda farkındalıklarının orta düzeyde, mahremiyet alt boyutunda farkındalıklarının ise ortalamanın üstünde olduęu tespit edilmiştir. Ortaöğretim öğrencilerinin kişisel verilerini ve mahremiyetlerini önemsediklerini ve bunun için önlem aldıkları sonucuna ulaşmıştır.

Gökçearslan, Günbatar ve Sarıtepeci ortaöğretim düzeyinde Bilgi Güvenlięi Farkındalıęı (BGF) düzeylerini ölçmüşlerdir. Çalışma sonucunda BT dersi alan öğrencilerin bilgi güvenlięi farkındalıklarının yüksek olduęu tespit edilmiştir. Derin ve Gençöğlü (2020), ortaokul öğrencilerinin bilgi güvenlięi farkındalık düzeylerini ve teknoloji kullanımlarını; cinsiyet, yaş ve sınıf, internet kullanım süresi ve internet kullanım amacı değişkenlerine göre

farklılaşıp farklılaşmadıklarını belirlemek amacıyla bir çalışma yapmışlardır. Çalışma neticesinde internet kullanım süresi fazla olan öğrencilerin, siber tehditler hakkında bilgi düzeylerinin yüksek olduğu ve interneti sosyal medya platformları amacıyla kullanan öğrencilerin bilgi güvenliği farkındalığı konusunda bilinçlendirilmesi gerektiğini göstermiştir.

Mıhçı, Türker ve Kılıç Çakmak (2019), 7 ortaokuldan 6.839 öğrenci, 749 öğretmen ve 4.916 velinin katıldığı bir çalışma gerçekleştirmiştir. Öğrencilerin internet bağımlılığı, siber zorbalık, çevrimiçi mahremiyet ve siber güvenlik konusunda yüksek düzeyde farkındalığa ve internette, uygunsuz çevrimiçi içerik ve telif hakkı konusunda orta düzeyde farkındalığa sahip olduklarını göstermiştir. Ayrıca, öğrencilerin farkındalık düzeyleri cinsiyet, sınıf düzeyi, internet kullanım süresi ve güvenli ve sorumlu internet kullanımı konusunda eğitim alma isteği açısından önemli ölçüde farklılık göstermiştir. Öğretmenlerin tüm kavramlara ilişkin farkındalıkları orta düzeydedir. Ayrıca ebeveynlerin çocuklarının internet bağımlılığı, internette, çevrimiçi mahremiyet, uygunsuz çevrimiçi içerik, telif hakkı ve siber güvenlik konularında orta düzeyde, siber zorbalık konusunda ise yüksek düzeyde farkındalık sahibi olduklarını düşündükleri belirlenmiştir.

Yurt içinde yapılan çalışmalarda siber güvenlik kavramından çok bilgi güvenliği kavramı üzerinde araştırmaların yapıldığı saptanmıştır. Alanyazın incelendiğinde ortaokul öğrencilerine yönelik Makhabbat ve Gülseçen (2022) tarafından gerçekleştirilen bir çalışmaya rastlanmıştır. Yapılan çalışma Erol ve diğerleri (2015) “Siber Güvenlik Ölçeği” kullanılmıştır. Yapılan çalışmada öğrencilerin siber güvenlik farkındalık durumlarının orta düzeyde olduğu görülmüştür. Öğrencilerin güvenilmeyenden kaçınmakta ve güvenlik için önlem alabildikleri tespit edilmiş olup internet üzerinde gezinirken iz bırakmamaya dikkat ettikleri belirlenmiştir. Alanyazın taraması sonucu ortaokul öğrenci yaş grubuna yönelik özelleşmiş bir ölçek tespit edilmemiştir.

SGF’yi artırmak ve ölçmek amacıyla çocuklara yönelik yurt dışında birçok çalışma gerçekleştirilmiştir. Hamdan ve diğerleri (2013), Birleşik Arap Emirliğinde 13-18 yaş aralığındaki 150 gence odaklanmıştır. Çalışmada amaç, siber güvenlik tehditlerini araştırmak, tespit etmek ve internet tehditlerinden nasıl korunabilecekleri konusunda onlara ve ebeveynlerine destek olabilecek stratejiler önermektir. Mevcut durumu ölçmek amacıyla 10 soruluk bir anket uygulanmıştır. Araştırma sonucu günlük internet kullanım saatleri 5 ve

üstü olan gençlerin daha fazla siber saldırıya maruz kaldıkları ancak daha fazla SGF' ye sahip oldukları, siber suçluların saldırdığı gençlerin sayısını en aza indirilebilmesi için ebeveynler ve gençler arasında farkındalık yaratılması gerektiğini açıkça göstermektedir.

Clemons ve Wilson, (2015), genç internet kullanıcılarının internette gerçekte ne yaptığını değerlendirmiştir. Gençlerden diğer öğrencilerin çevrim içi etkinlikleri hakkında farkındalıkları istendi. Ayrıca, okul e-posta hesaplarının çevrim içi sosyal mühendisliğe ve çeşitli çevrim içi kaynaklardan bilgi bağlantılarına yönelik tutumları ve tercihleri hakkında nitel araştırma gerçekleştirmiştir. Çalışma Amerika Birleşik Devletleri, Arjantin, Brezilya, Şili, Kolombiya, Almanya, Japonya ve Meksika'da çevrim içi olarak gerçekleştirilen veli ve öğrencilerle yapılan anketlere dayanmaktadır. Çalışma sonunda öğrenciler ve diğer genç nüfus arasında, kişisel mahremiyeti göz ardı etme ve ifade edilen tercihlerle tutarsız davranışlarda bulunma kararlarının neredeyse evrensel olduğu tespit edilmiştir.

Shin ve Kang, (2016), çalışmalarında ergenlerin çevrim içi mahremiyetle ilgili algı ve davranışlarında ebeveyn ve internet faktörlerinin rolünü araştırmıştır. Çalışma kapsamında Singapur'un farklı yerlerinde bulunan dört farklı ortaokuldan 12-18 yaş arası 746 çocuk ile bir anket uygulanmıştır. Ölçeğin alt faktörleri olarak ebeveyn ara buluculuğu, ergenlerin internet deneyimleri, internette geçirdikleri zaman ve çevrim içi iletişim faaliyetlerine katılımları incelenmiştir. Çocukların ebeveynlerine kendilerini açıklamaları, ergenlerin çevrim içi gizlilik endişelerini, kişisel olarak tanımlanabilir bilgileri ifşa etme istekliliğini etkileyebileceği sonucunda ulaşılmıştır.

Velki, Solic, Gorjanac ve Nenadic (2017) yaptığı çalışmada yetişkinler için kullanılan bir siber güvenlik farkındalığı ölçeğinin ortaokul çocuklarına uygun olup olmadığını deneyimlemiştir. Bu amaç kapsamında ölçek 355 öğrenciye uygulanmıştır. Analiz sonucunda e-posta sistemine erişimleri için şifrelerini açıklayan ortaokul öğrencilerinin yüzdesi yetişkinlere göre çok daha yüksek olduğu tespit edilmiştir. Yetişkinlerle karşılaştırıldığında, iletişimde, güvenlik eleştirisi ve yedekleme kalitesinin önemi ile ilgili alt ölçek boyutlarında çocukların yetişkinlerden daha düşük sonuçlar aldığı ortaya çıkmıştır. Ortaokul öğrencileri, kişisel bilgisayar bakımı ve verilerin güvenliğine olan inanç ile ilgili alt ölçeklerde boyutlarda yetişkinlerden daha yüksek puan elde etmiştir. Buna ek olarak, siber mağdur olan öğrencilerin yüzdesi ve siber şiddet uygulama konularında öğrencilerin yetişkinlere oranla daha yüksek bir yüzdesi vardır.

Dempsey, Sim, ve Cassidy (2018), 8 ila 10 yaşları arasındaki 32 çocuğun mahremiyet anlayışlarını ölçmek için bir anket oluşturmuşlardır hazırlamışlardır. Çocuklara sekiz farklı senaryo sunulmuş ve çocukların bilgilerin gizli kalması gerekip gerekmediğine karar vermeleri ve nedenini belirtmeleri istenmiştir. Bu çalışmada çocukların, özellikle çevrim içi güvenlikle ilgili olduğunda, gizlilik konusunda bir anlayışa sahip olduğudur. Ancak çocuklar, verilerinin doğal bir değeri önemi olduğunu, veriler ve hangi verilerin korunması gerektiği konusunu da yanılgılara sahip olduğunu henüz tam olarak anlamadıkları bulgusuna ulaşmışlardır.

Teimouri, Benrazavi, Griffiths ve Hassan (2018) yaşları 9-16 arasında değişen toplam 420 ilkokul ve ortaokul öğrenciyi kapsayan bir çalışma gerçekleştirmiştir. Malezyalı öğrencilerden algılanan çevrim içi güvenliği değerlendiren 12, çevrim içi koruma motivasyonunu değerlendiren 22 ve çevrimiçi risklere maruz kalma ile ilgili 39 sorudan oluşan ölçeği yanıtlamaları istenmiştir. Çalışma sonunda çevrim içi risklere maruz kalmayı ciddiye alan çocukların bu risklere daha az maruz kalmasına rağmen, çocukların çevrim içi risklere karşı algılanan duyarlılıkları ile çevrim içi risklere maruz kalma arasında bir ilişki olmadığını göstermektedir.

Choong, Theofanos, Renaud, ve Prior (2019), çocukların şifre güvenliğinin çok önemli olduğu bir dünyaya daha etkili bir şekilde hazırlanmasına katkı sağlamak, şifre konusundaki bilgi ve deneyimlerini tespit etmek için bir anket geliştirmişlerdir. Çalışmanın veri setinde ABD'nin Midwest bölgesinde bulunan iki okuldan farklı düzeylerde 189 okul öğrenci katılmıştır. Çalışma sonucunda 6-8. sınıf öğrencileri şifreleriyle daha fazla zorluk yaşadıklarını bildirdiler. Ayrıca şifrelerini korumak için daha fazla mücadele ettikleri ortaya çıkmıştır.

3. YÖNTEM

Araştırma iki bölümden oluşmaktadır. İlk bölümde siber güvenlik farkındalığı ölçeği geliştirilmektedir. İkinci bölümde ise bu ölçek kullanılarak ortaokul öğrencilerinin siber güvenlik farkındalık düzeyleri ölçülmüştür. Bu nedenle gerçekleştirilen araştırmanın bu bölümünde araştırmanın modeli, evren ve örneklem, verilerin toplanması, veri toplama araçları ve verilerin çözümlenmesinde kullanılan yöntem ve tekniklerde ayrı ayrı sunulmuştur.

3.1. Siber Güvenlik Farkındalığı Ölçek Geliştirme Çalışması

Gerçekleştirilen araştırmanın bu bölümünde; araştırmanın modeli, evren ve örneklemi, verilerin toplanması, veri toplama araçları ve verilerin çözümlenmesinde kullanılan yöntem ve teknikler yer almaktadır.

3.1.1. Araştırma modeli

Nicel desen olarak ele alınan araştırmada, tarama modeli kullanılmıştır. Tarama modeli, bir konu ya da olay hakkında katılımcı görüş, ilgi, tutum gibi özellikleri belirlemek amacıyla büyük çapta örneklemin kullanıldığı araştırmalar (Büyüköztürk, Kılıç Çakmak, Akgün, Karadeniz ve Demirel, 2018) olup geçmişte ya da halen var olan durumu var olduğu şekliyle betimlemeyi amaçlayan araştırma yaklaşımlarıdır (Karasar, 2000).

3.1.2. Evren ve örneklem

Araştırmanın evrenini Amasya ilindeki tüm ortaokul öğrencileri oluşturmaktadır. Ancak tüm evrene ulaşmak maliyet ve zaman bakımından mümkün olmadığı için örneklem belirlenmiştir. Örneklem Amasya merkezde ortaokul kademesinde 2021-2022 eğitim ve öğretim yılında öğrenim gören 5, 6, 7 ve 8. sınıf öğrencilerinden belirlenmiştir. Amasya ilinde ortaokul kademesinde öğrenim gören öğrenci sayıları aşağıda verilmiştir.

Çizelge 3. 1. Amasya ili 5, 6, 7 ve 8'inci sınıf öğrenci sayıları

İlçeler	5.Sınıf	6.Sınıf	7.Sınıf	8.Sınıf	Genel Toplam
Göynücek	84	91	90	68	333
Gümüşhacıköy	208	204	209	228	849
Hamamözü	34	25	31	26	116
Merkez	2008	1884	1935	1956	7.783
Merzifon	997	955	1022	948	3.922
Suluova	649	608	608	633	2.498
Taşova	313	312	300	317	1.242
Genel Toplam	4.293	4.079	4.195	4.176	16.743

Çizelge 3.1’ de görüldüğü üzere Amasya ilinde 4.293 5. sınıf, 4.079 6.sınıf, 4.195 7. sınıf, 4.176 8. sınıf olmak üzere toplam 16.743 ortaokul öğrencisi bulunmaktadır. Bu öğrencilerden amaçlı örnekleme yöntemi ile çalışma grubu belirlenmiştir. Amaçlı örnekleme geniş katılımcıların katılımıyla oluşan zengin bilgi kümesinde araştırılan durumların derinlemesine çalışılmasına olanak vermektedir (Büyüköztürk ve diğerleri, 2009; Patton, 2002). Ölçek geliştirme aşamasının çalışma grubu için Amasya ilinde ortaokul kademesinde en kalabalık olan iki eğitim kurumu seçilmiştir. Çalışmanın örnekleme açımlayıcı faktör analizi (n=854) ve doğrulayıcı faktör analizi (n=602) aşamalarında değerlendirmek üzere toplam 1.456 ortaokul öğrencisinden oluşmaktadır. Krejcie ve Morgan (1970), 4.000 kişilik bir evrende 351, 4.500 kişilik bir evrende 354 kişinin evreni temsil edebilecek yeterlikte olduğunu belirtmektedir (Akt. Gay; 1996:125). Ayrıca Şencan (2005) ölçek geliştirme çalışmalarında örnekleme büyüklüğünün belirlenmesinde ölçekte yer alan madde sayısının en az 5 katı olması gerektiği belirtilmektedir (Şencan, 2005). Buna göre çalışma grubu sayısının evreni temsil ettiği söylenebilir. Çalışma grubuna ait demografik bilgiler aşağıda sunulmuştur.

Çizelge 3. 2. Çalışma grubu okul ve sınıf bilgisi

Okullar	5.Sınıf	6.Sınıf	7.Sınıf	8.Sınıf	Genel Toplam
B Ortaokulu	202	195	210	195	802
A Ortaokulu	180	151	152	171	654
Genel Toplam	382	346	362	366	1.456

Öğrencilerden 802 kişi B ortaokulunda 654 kişi A ortaokulunda eğitim görmektedir. Öğrencilerin 382 tanesi 5'inci sınıf, 346'sı 6'ncı sınıf, 362'si 7'nci sınıf ve 366'sı 8'inci sınıf düzeyinde öğrenim görmektedir. Çalışma grubunun cinsiyet dağılımı çizelge 3.3' de sunulmuştur.

Çizelge 3. 3. Çalışma grubu cinsiyet dağılımı

Cinsiyet	N	Oran(%)
Erkek	686	46,9
Kız	778	53,1
Toplam	1464	100

Çizelge 3.3' te görüldüğü üzere çalışma grubunda 686 erkek (%46,9) ve 778 kız (%53,1) öğrenci bulunmaktadır. Bu öğrencilerin teknolojik ürüne (cep telefonu, dizüstü bilgisayar, masaüstü bilgisayar, tablet bilgisayar) sahip olma durumu çizelge 3.4 de sunulmuştur.

Çizelge 3. 4. Çalışma grubu teknolojik ürün sahipliği

Teknolojik Alet	N	Oran(%)
Var	1.455	99,4
Yok	9	0,6
Toplam	1464	100

Çizelge 3.4' de görüldüğü üzere 1.464 öğrenciden 1.455'i (%99,4) teknolojik alete sahipken sadece 9 tanesinin herhangi bir teknolojik aleti bulunmamaktadır. Bu oran tüm örneklemin %0,6'sına denk gelmektedir. Katılımcıların sahip olduğu teknolojik ürünlerin dağılımı çizelge 3.5' de görülmektedir.

Çizelge 3. 5. Çalışma grubu teknolojik ürün dağılımı

Teknolojik Ürün	Var	Oran (%)	Yok	Oran (%)
Cep Telefonu	1.002	68,40	462	31,60
Tablet	723	49,40	741	50,60
Masaüstü Bilgisayar	399	27,30	1.065	72,70
Dizüstü Bilgisayar	547	37,40	917	62,60
Akıllı Saat	343	23,40	1.121	76,60

Çizelge 3.5’ de görüldüğü üzere çalışma grubunda bulunan 1.464 öğrenci 5 ayrı teknolojik ürün kapsamında 3.014 teknolojik ürüne sahiptir. Bunlardan 1002’ sini (%68,40) cep telefonu, 723’ ünü tablet bilgisayar (%49,40), 399’unu masaüstü bilgisayar (%27,30), 547’sini dizüstü bilgisayar (%39,40) ve 343’ünü akıllı saat (%23,40) oluşturmaktadır. çizelge 3.5’e göre öğrenciler tarafından en fazla kullanılan teknolojik cihaz cep telefonu iken en az akıllı saattir. Çalışma grubunun sahip oldukları teknolojik ürünler ile internete bağlanma yöntemleri Çizelge 3.6’ da sunulmuştur.

Çizelge 3. 6. Çalışma grubu internete erişim yöntemi

İnternete Bağlantısı	Var	Var (%)	Yok	Yok (%)
Ev İnterneti	1263	86,30	201	13,70
Mobil Bağlantı	478	13,70	986	86,30
Wi-fi Bağlantı (Dış Ortam)	418	28,60	1046	71,4

Çizelge 3.6’da çalışma grubunda yer alan 1.464 öğrencinin internete bağlanmak için seçtiği yöntemler incelendiğinde 1.263 (%86,30) öğrencinin ev internetine sahip olduğu belirlenmiştir. Çalışma grubunun 478’i (%13,70) mobil bağlantı kullandığını belirtmiştir. Ayrıca 418 (%28,60) öğrencinin cafe, park vb. ortak alanlarda sunulan internet hizmetlerinden de yararlandığı tespit edilmiştir.

Çizelge 3. 7. Çalışma grubu günlük internet kullanım süreleri

Süre	N	Oran (%)
1 Saatten Az	421	28,80
1-3 Saat Arası	739	50,50
3-5 Saat Arası	223	15,20
5 Saatten Fazla	81	5,50
Toplam	1.464	100

Çalışma grubunun interneti günlük kullanım saatleri incelendiğinde 737'si (%50,50) gün içerisinde 1 ila 3 saat arası internet kullanmaktadır. 421'i (%28,80) günlük 1 saatten az çevrimiçi olurken 3-5 saat arası kullananların sayısının 223 (%15,20) olduğu tespit edilmiştir. Çalışma grubunun sadece 81'i (%5,50) 5 saatten fazla çevrimiçi olmaktadır. Katılımcıların interneti kullanım amaçları Çizelge 3.8' de incelenmiştir.

Çizelge 3. 8. Çalışma grubu internet kullanım alanları

İnternete Kullanma Amacı	Evet	Oran (%)	Hayır	Oran (%)
Müzik, Film, Eğlence	1.174	80,20	290	19,80
Oyun, Online Oyun	867	59,20	597	40,80
Sosyal Ağ (Facebook, Twitter, Instagram vb.)	647	44,20	817	55,80
Araştırma-Öğrenme (Ders amaçlı veya Ödev)	1.211	82,70	253	17,30
Haberleşme (e-posta, Whatsapp, Bip, Telegram vb.)	850	58,1%	614	41,90

Çalışma grubunda yer alan 1.464 öğrencinin interneti hangi amaçlarla kullandıkları incelendiğinde 1.211'inin (%82,70) ödev ve araştırma için kullandığı, 1.174'ünün (%80,20) müzik, film, eğlence amacıyla, 867 'sının (%59,20) oyun-online oyun için kullandığını belirtmiştir. 850'si (%58,10) haberleşme amacıyla interneti kullanırken 647'si (%55,80) sosyal ağ ortamları için kullandığını belirtmiştir.

3.1.3. Veri toplama araçları

Araştırmanın amaçlarından bir tanesi Siber Güvenlik Farkındalık Ölçeği (SGFÖ) geliştirmektir. Bu doğrultuda, ölçek geliştirilirken Erkuş (2019) tarafından yapılan çalışmada belirtilen ölçek geliştirme adımları izlenmiştir. Ölçeğin geliştirilme sürecinde yapılan çalışmalar şekil 3.1’ de açıklanmıştır.



Şekil 3.1. Ölçek geliştirme aşamaları (Erkuş, 2019).

Erkuş (2019)’ nin ölçek geliştirme adımları referans alınarak bu çalışma için ölçek geliştirme adımları oluşturulmuş ve Çizelge 3.9’ da bu adımlar özetlenmiştir.

Çizelge 3. 9. Ölçek geliştirme aşamaları

Aşamalar	İşlemler	Açıklamalar
1. Aşama Yapıyı belirleme	Ölçeğin Amacını Belirleme	Ortaokul öğrencilerinin Siber Güvenlik Farkındalık düzeylerini belirlemek için geçerli ve güvenilir bir ölçme aracı geliştirmek.
	Literatür Tarama	Yerli ve yabancı alan yazında Siber Güvenlik Farkındalığı ile ilgili araştırmalar, yapılan lisansüstü tezler incelenmiştir
	Ölçülecek Özelliklerin Tanımlanması	Literatür çalışmasının ardından hangi boyutların ve alt boyutların ele alınacağına ve araştırma için ön koşul niteliğinde olan en temel özelliklerin neler olacağına karar verilmiştir.
	Maddelerin Formatına Karar Verme	Ölçeğin beşli likert türünde olması, olumlu ve olumsuz ifadeler içermesi ve kesinlikle katılıyorum, katılıyorum ne katılıyorum ne katılmıyorum, katılmıyorum, kesinlikle katılmıyorum ifadelerini içermesi kararlaştırılmıştır.
2. Aşama Madde Havuzu Aşaması	Madde Havuzunun Oluşturulması	Ölçek maddelerinin yazım aşamasında ilk olarak siber güvenlik farkındalığı ile literatür incelenerek siber güvenlik ile ilgili yaşanan sorunlar ve gerekli farkındalık davranışları belirlenmiştir. Siber Güvenlik ile alakalı 47 soru ve ölçeğin güvenilirliğini artırmak için A15-Lütfen “Tamamen Katılıyorum”, A34-Lütfen “Kesinlikle Katılmıyorum”, A41-Lütfen “Ne Katılıyorum Ne Katılmıyorum” seçeneğini işaretleyin biçiminde 3 soru eklenmiştir. Madde havuzu toplam 50 soruya ulaşmıştır.
	Maddeler hakkında uzman görüşü alma	Ölçekte belirlenen maddelerin öncelikle siber güvenliği ölçüp ölçmediği ve kullanılan ifadelerin açık, anlaşılabilirlik ve öğrenci seviyesine uygunluğunun değerlendirilmesi amacıyla uzman görüşlerine başvurulmuştur. Alan uzmanlarının görüşleri doğrultusunda 5 soru uygun seviyede olmaması, 2 soru ise Türk Dili Uzmanı görüşleri doğrultusunda çıkarılmıştır. Bu doğrultuda 43 maddelik ölçeğin taslak formuna son hali verilerek pilot uygulamaya hazır hale getirilmiştir.
3. Aşama Uzman Görüşü Alma	Maddelerin Gözden Geçirilmesi, Düzeltmelerin Yapılması	Uzmanlardan alınan görüşler doğrultusunda gerekli düzeltmeler yapılmıştır. Ortaokul kademesindeki her sınıf seviyesinden iki öğrenci seçilerek toplamda 8 öğrenciye uygulama yapılmıştır. Öğrencilerden ölçeğin taslak formunda yer alan maddelerin anlaşılabilirliğine yönelik geri bildirimler alınmıştır.
	Kapsam ve Görünüm Geçerlik Çalışması	Kapsam, görünüm ve geçerlik çalışması kapsamında, son düzenlemelerin yapılmasıyla birlikte 3 maddesi güvenlik amacıyla kullanılan 43 maddelik ölçek uygulamaya hazır hale getirilmiştir.

Çizelge 3.9. Ölçek geliştirme aşamaları (çizelgenin devamı)

Aşamalar	İşlemler	Açıklamalar
4. Aşama Pilot Çalışma	Nihai Uygulama	Ölçeğin nihai uygulamasının gerçekleştirilmesi amacıyla, ortaokul kademesindeki her sınıf seviyesinden toplam 1.516 öğrenciye ölçek uygulanmıştır.
5. Aşama Maddelerin Analizi	Madde Analizleri	Bu aşamada AFA ve DFA yapılmıştır. Şifre Güvenliği 7 madde, Önleyici Tedbirler 7 madde, Kötü Amaçlı Yazılım Farkındalığı 6 madde, Kişisel gizliliği koruma 5 madde olarak belirlenmiştir.
6. Aşama Sonuçların Değerlendirilmesi	Sonuçların Analizi	Dört alt boyut için Cronbach'ın Alfa güvenilirlik katsayıları 0,82 ile 0,92 arasındadır; ölçeğin tamamı için hesaplanan Cronbach'ın Alfa değeri ise 0,87'dir.

Ölçek maddelerinin yazım aşamasında ilk olarak siber güvenlik farkındalığı ile ilgili yapı belirlenmiştir. Yapı belirlenirken ölçeğin amacı netleştirilmiş, literatür taraması yapılmış, özellikler tanımlanmış ve madde formatına karar verilmiştir. Literatür incelenerek siber güvenlik ile ilgili yaşanan sorunlar ve gerekli farkındalık davranışları belirlenmiş ve madde havuzu oluşturulmuştur. Ölçek maddelerinin oluşturulmasında ilk olarak, siber güvenlik farkındalığı hakkında ulusal ve uluslararası literatürde bulunan ölçek geliştirme çalışmaları incelenmiştir. İncelemeler sonucunda yetişkinler, farklı meslek dalları ve çeşitli eğitim kademelerine yönelik siber güvenlik farkındalığına yönelik gerçekleştirilen çalışmaların olduğu görülmüştür (Valli, Martinus ve Johnstone, 2014; Hyla ve Fabisiak, 2020). Araştırmacı tarafından gerçekleştirilen çalışma ortaokul kademesindeki öğrencilere yönelik olduğundan bu kademedeki siber güvenlik farkındalığı çalışmalarının incelenmesine öncelik verilmiştir. Bu aşamada Erol ve diğerleri (2015) tarafından geliştirilmiş olan “Kişisel Siber Güvenliği Sağlama Ölçeği”, Baumann, (2016) tarafından geliştirilen “Bilgisayar Güvenliği Ölçeği”, Alqarni, (2017) tarafından geliştirilen “Bilgisayar Güvenliği Uygulamalarının Benimsenmesini Etkileyen Faktörleri Araştırma” ölçeği, Yılmaz ve diğerleri, (2016) tarafından geliştirilen “Öğretmenlerin Dijital Veri Güvenliği Farkındalığı” ölçeği incelenmiştir. Yapılan incelemeler sonucunda ortaokul öğrencilerinin siber güvenlik farkındalıklarının ölçmek amacıyla 47 maddelik madde havuzu oluşturulmuş toplanan verilerin güvenilirliğini artırmak amacıyla ölçeğin A15-Lütfen “Tamamen Katılıyorum” seçeneğini işaretleyiniz, A34-Lütfen “Kesinlikle Katılmıyorum” seçeneğini işaretleyiniz, A41-Lütfen “Ne Katılıyorum Ne Katılmıyorum” seçeneğini işaretleyin biçiminde 3 soru eklenmiştir. Daha sonra gerekli düzenlemeler yapılarak 5’li Likert türünde ve 50 maddeden oluşan ölçeğin taslak formu hazırlanmıştır.

Ölçekte belirlenen maddelerin öncelikle siber güvenliği ölçüp ölçmediği ve kullanılan ifadelerin açık, anlaşılabilirlik ve öğrenci seviyesine uygunluğunun değerlendirilmesi amacıyla uzman görüşlerine başvurulmuştur. Alan uzmanlarına ölçek formları e-posta yoluyla gönderilmiş ve uzmanlardan ölçekte yer alan ifadelerin, ortaokul öğrencilerinin siber güvenlik farkındalıklarını ve siber güvenlik yeterliklerini ölçme, ifadelerin anlaşılabilirliği ve amaca uygunluğu bakımından değerlendirmeleri istenmiştir. Bu değerlendirmelerde uzmanların ifadelerin anlaşılabilirliğine yönelik geri bildirimleri dikkate alınarak madde havuzunda yer alan 2 madde çıkartılmış, ölçekte yer alan ifadeler ve ölçeğin taslak formu üzerinde gerekli düzenlemeler yapılmıştır. Ayrıca ölçme-değerlendirme uzmanı ve 2 ortaokul öğretmeninden alınan görüş neticesinde havuzda yer alan 5 maddenin öğrenci seviyesine uygun olmadığı ve ölçekten çıkarılması gerektiği ifade edilmiştir. Sonrasında ölçek maddelerinde yer alan ifadeler Türk dili uzmanı tarafından ayrıca incelenmiştir. Alınan geri bildirimlerle ölçeğin taslak formu üzerinde gerekli değişiklikler yapılarak yeniden düzenlenmiştir. Taslak ortaokul kademesindeki her sınıf seviyesinden iki öğrenci seçilerek toplamda 8 öğrenciye uygulanmıştır. Öğrencilerden ölçeğin taslak formunda yer alan maddelerin anlaşılabilirliğine yönelik geri bildirimler alınmıştır. Bu doğrultuda son düzenlemelerin yapılmasıyla birlikte 43 maddelik ölçek uygulamaya hazır hale getirilmiştir. Son olarak pilot uygulama ile veriler toplanmış ve madde analizleri yapılarak sonuçlar analiz edilmiştir. Bu aşama tezin ilerleyen bölümlerinde ayrıntılı olarak sunulmuştur.

3.1.4. Verilerin toplanması

Uygulama için Amasya Üniversitesi Etik Kurul Birimi'nden gerekli izin alınmıştır. İkinci aşamada Amasya İl Milli Eğitim Müdürlüğü'nden merkezde bulunan bağlı resmi ve özel ortaokullarında uygulama yapabilmek için araştırma-uygulama izni alınmıştır. Yapılan görüşmelerde İl Milli Eğitim Müdürlüğü'nden alınan araştırma izin belgesi idarecilere takdim edilerek uygulama için izin alınmıştır. İdarecilere araştırmanın amacıyla ilgili bilgi verilmiş, uygulamanın gönüllülük esasına dayalı olduğu ve uygulama süresinin her öğrenci için ortalama on beş dakika süreceği belirtilmiştir. Uygulama sürecinde okul idarecileri ve rehberlik öğretmeni eşliğinde uygulama yapılacak sınıflar araştırmacıya gezdirilmiş ve ders saatindeki öğretmenler bilgilendirilerek araştırmacının uygulama yapması sağlanmıştır. Araştırmacı tarafından tüm sınıflarda katılımın gönüllülük esasına dayalı olduğu, taslak form üzerine isim yazmamaları gerektiği, uygulamanın nasıl yapılacağı ve araştırmanın amacı ile ilgili olarak araştırma hakkında öğrencilere gerekli bilgilendirmeler yapılmıştır.

Veriler pilot uygulama aşamasında Açımlayıcı Faktör Analizi (AFA) ve Doğrulatoryıcı Faktör Analizi (DFA) olmak üzere iki farklı gruptan toplanmıştır. Faktör analizi için öncelikle örneklem sayısı belirlenmiştir. AFA için 300 kişi “iyi”, 500 kişi “çok iyi” ve 1000 kişi “mükemmel” (Tavşancıl; 2006:51) olarak değerlendirilmektedir. Bu doğrultuda ölçeğin pilot uygulamasında kalabalık olan okullar tercih edilmiştir. AFA için 5. Sınıf (N=135), 6. Sınıf(N=244), 7.sınıf(N=250) ve 8. Sınıfta(N=225) öğrenim gören toplam 872 ortaokul öğrencisinden veri toplanmıştır. Bu uygulama sonrasında ölçek formunda yer alan maddelere %10 ve daha fazla oranda cevap vermeyen 28 katılımcı veri setinden çıkarılmıştır (Tabachnick ve Fidell, 2013). AFA sonucunda alt faktörleri belirlenmiş olan ölçeğe son şekli verilerek DFA için tekrar uygulanmıştır. DFA açımlayıcı faktör analizine katılan öğrencilerden farklı olarak 5. sınıfta öğrenim gören 107 öğrenci, 6. sınıfta öğrenim gören 163 öğrenci, 7. sınıfta öğrenim gören 158 öğrenci ve 8 sınıfta öğrenim gören 168 öğrenci olmak üzere toplam 644 öğrenciye uygulanmıştır. Ölçek formunda yer alan maddelere %10 ve daha fazla oranda cevap vermeyen 48 katılımcı veri setinden çıkarılmıştır.

3.1.5. Verilerin analizi

Veri analizinde ölçek maddeleri arasında ilişki bulunup bulunmadığı tespit edilmek isteniyorsa Açımlayıcı Faktör Analizi (AFA), belirlenen bir ilişki, ortaya çıkan faktörler ve bunların altında toplanmış maddeler varsa Doğrulatoryıcı Faktör Analizi (DFA) yapılması önerilmektedir (Büyüköztürk, 2002; Bandalos ve Finney, 2010; Kline, 2011). Araştırmada “Siber güvenlik farkındalığı ölçeği geçerlik ölçütlerini karşılamakta mıdır?” sorusuna cevap bulmak amacı ile AFA ve “Siber güvenlik farkındalığı ölçeği güvenilirlik ölçütlerini karşılamakta mıdır?” sorusuna cevap bulmak amacı ile DFA gerçekleştirilmiştir. AFA çözümlenmesinde SPSS 22 ve DFA çözümlenmesinde LISREL 8.80 (Linear Structural Relation Statistics Package Program) programı kullanılmıştır. Analizlerin ayrıntıları bulgular bölümünde sunulmuştur.

3.2. Ölçek Uygulama Çalışması

Bu bölümde araştırmanın modeli, evreni ve örneklemini, çalışma grubu, veri toplama aracı ve verilerin nasıl analiz edildiği açıklamıştır.

3.2.1. Araştırmanın modeli

Araştırma modeli olarak betimsel tarama modeli kullanılmıştır. Tarama modelleri geçmişte ya da mevcut olan bir durumu olduğu şekliyle tasvir edilen araştırmalar için uygun bir modeldir (Karasar, 2006). Betimsel tarama, örneklem grubunun geniş olduğu, grubu oluşturan bireylerin bir olgu ve olayla ilgili fikirlerinin, tutumlarının alındığı, olgu ve olayların betimlenmeye çalışıldığı araştırmalardır (Karakaya, 2012:59).

3.2.2. Evren ve örneklem

Araştırmanın evrenini Amasya ilindeki tüm ortaokul öğrencileri oluşturmaktadır. Ancak tüm evrene ulaşmak maliyet ve zaman bakımından mümkün olmadığı için örneklem belirlenmiştir. Nicel araştırmalarda araştırmacılar belirlenen evrenin içerisinden uygulama sürecinde ulaşabilecekleri bir örneklem belirlerler (Cresswell, 2017). Örnekleme yöntemi olarak tabakalı örneklem yöntemi tercih edilmiştir. Bu örneklem türünün seçilme amacı diğer örneklem türlerine göre görece küçük bir örneklem grubu ve düşük maliyetle, araştırma evrenini daha yüksek derecede temsil etme olanağı sağlamaktadır (Neuman ve Robson, 2014). Örneklem belirlenirken Amasya ilinin ortaokul kademesinde en kalabalık olan iki eğitim kurumu seçilmiştir. Bu ortaokullar taşınmalı eğitim kapsamında olmaları sebebiyle köy, belde ve merkezden öğrenciler öğrenim görmektedir.

3.2.3. Çalışma grubu

Araştırmanın evrenini Amasya ilindeki tüm ortaokul öğrencileri oluşturmaktadır. Ancak tüm evrene ulaşmak maliyet ve zaman bakımından mümkün olmadığı için örneklem belirlenmiştir. Nicel araştırmalarda araştırmacılar belirlenen evrenin içerisinden uygulama sürecinde ulaşabilecekleri bir örneklem belirlerler (Cresswell, 2017). Örnekleme yöntemi olarak tabakalı örneklem yöntemi tercih edilmiştir. Bu örneklem türünün seçilme amacı diğer örneklem türlerine göre görece küçük bir örneklem grubu ve düşük maliyetle, araştırma evrenini daha yüksek derecede temsil etme olanağı sağlamaktadır (Neuman ve Robson, 2014). Örneklem belirlenirken Amasya ilinin ortaokul kademesinde en kalabalık olan iki eğitim kurumu seçilmiştir. Bu ortaokullar taşınmalı eğitim kapsamında olmaları sebebiyle köy, belde ve merkezden öğrenciler öğrenim görmektedir.

Çizelge 3. 10. Çalışma grubu demografik özellikler

Özellik	Kategori	Frekans (f)	Yüzde (%)
Okul	A Ortaokulu	350	66,0
	B Ortaokulu	180	34,0
Toplam		530	100
Sınıf	5.Sınıf	204	38,5
	6.Sınıf	89	16,8
	7.Sınıf	89	16,8
	8.Sınıf	148	27,9
Toplam		530	100
Cinsiyet	Kadın	246	46,4
	Erkek	284	53,6
Günlük İnternet Kullanımı	1 Saatten Az	161	30,4
	1-3 Saat Arası	270	50,9
	3-5 Saat Arası	71	13,4
	5 Saatten Fazla	28	5,3
Hiç siber saldırıya maruz kaldınız mı?	Evet	28	5,3
	Hayır	419	79,1
	Fikrim Yok	83	15,7
Ailenizde veya yakın çevrenizde siber saldırıya maruz kalan kişiler var mı?	Evet	232	43,8
	Hayır	201	37,9
	Fikrim Yok	97	18,3
Kişisel siber güvenliğinizi sağlayabilecek bilgi ve becerilere sahip olduğunuzu düşünüyor musunuz?	Evet	381	71,9
	Hayır	79	14,9
	Fikrim Yok	70	13,2

Ölçek uygulama çalışma grubunda yer alan 530 öğrenci sınıf düzeylerine göre incelendiğinde en fazla 5’inci sınıf öğrencileri (%38,50) ardından 8’inci sınıf öğrencileri (%27,90) katılım sağlamıştır. Çalışma grubu cinsiyetlerine göre incelendiğinde 246’sı (%46,40) kadın, 284’ü erkek (%53,60) olduğu belirlenmiştir. Çalışma grubunun günlük internet kullanım süreleri incelendiğinde 270’inin (%50,90) 1-3 saat, 161’inin (%30,40) 1 saatten az, 71’inin 3-5 saat ve 28’inin (%5,30) 5 saatten fazla internette zaman geçirdiği

belirlenmiştir. Siber saldırı maruziyetleri incelendiğinde sadece 28'inin (%5,30) siber saldırıya maruz kaldığı, 83'ü (%15,70) fikrim yok demiştir. 232 öğrenci (%43,80) ailesinde veya yakın çevresinde siber saldırıya maruz kalmış kişiler olduğunu belirtmiştir. Öğrencilerin 381'i (%71,90) kişisel siber güvenliğini sağlayabileceğini düşünmektedir.

3.2.4. Veri toplama aracı

Araştırmada veri toplama aracı olarak araştırmacı tarafından hazırlanan ve çalışmanın ilk bölümünde açıklanan SGFÖ kullanılmıştır. SGFÖ, "Şifre Güvenliği" (7 madde) "Önleyici Tedbirler"(7 madde) "Kötü Amaçlı Yazılım Farkındalığı" (6 madde) ve "Kişisel Gizliliği Koruma"(5 madde) olmak üzere 4 boyut ve 25 maddeden oluşmaktadır. Ölçeğin tamamına ilişkin Cronbach'ın alfa değeri 0,87 olmakla birlikte boyutların Cronbach alfa değeri 0,82-0,92 arasında değişmektedir. Araştırmada kullanılan ölçeklerin güvenirlikleri ve bu çalışmadan elde edilen güvenirlik değerleri çizelge 3.11.' de verilmiştir.

Çizelge 3. 11. SGFÖ'nün güvenirlik değerleri

Ölçek/Alt Boyutlar	Cronbach'ın alfa	Uygulamada Elde Edilen
Şifre Güvenliği Alt Boyutu	0,92	0,89
Önleyici Tedbirler Alt Boyutu	0,82	0,80
Kötü Amaçlı Yazılım Farkındalığı Alt Boyutu	0,85	0,84
Kişisel Gizliliği Koruma Alt Boyutu	0,83	0,83
Siber Güvenlik Farkındalığı Ölçeği	0,87	0,82

Ercan ve Kan (2004)' a göre ölçeğe ait Cronbach alfa referans aralıkları aşağıdaki gibidir:

$0 < \alpha < 0.40$ ise güvenilir değil,

$0.40 < \alpha < 0.60$ ise düşük güvenilirlikte,

$0.60 < \alpha < 0.80$ ise oldukça güvenilir,

$0.80 < \alpha < 1.00$ ise yüksek güvenilirlikte.

Çizelge 3.11.'e göre çalışmadan elde edilen güvenirlik değerlerini "yüksek güvenilir" düzeyinde olduğu görülmektedir.

3.2.5. Verilerin analizi

Verilerin analizinde SPSS 22 kullanılmıştır. Öncelikle veri setinin normalliği incelenmiştir. 534 öğrenciye ait veri setinin normalliği incelendiğinde uç değerler olduğu saptanmıştır. Yapılan Tanımlayıcı İstatistikler (Descriptive statistics) sonucu uç değer olarak görülen 4 öğrenciye ait değer veri setinden çıkartılmıştır. Normallik değerleri için mod, medyan, ortalama ve standart sapma değerlerinin yanı sıra basıklık ve çarpıklık değerleri incelenmiştir.

Çizelge 3. 12. Basıklık ve çarpıklık değerleri

Ölçek ve Alt Faktörleri	Basıklık	Çarpıklık
• Şifre Güvenliği Alt Boyutu	-0,480	0,426
• Önleyici Tedbirler Alt Boyutu	-,0719	-0,06
• Kötü Amaçlı Yazılım Farkındalığı Alt Boyutu	-0,315	-0,561
• Kişisel Gizliliği Koruma Alt Boyutu	-0,428	0,217
Siber Güvenlik Farkındalığı Ölçeği Toplam	-0,394	-0,266

Çizelge 3. 13. Uygulanan parametrik testler çizelgesi

Araştırma Sorusu	Yapılan Analiz
Ortaokul öğrencilerinin siber güvenlik farkındalıkları toplam puan ve alt boyutlarda Cinsiyet değişkenine göre farklılaşmakta mıdır?	Bağımsız Gruplar t-Testi
Ortaokul öğrencilerinin siber güvenlik farkındalıkları toplam puan ve alt boyutlarda Sınıf düzeyi değişkenine göre farklılaşmakta mıdır?	Oneway Anova (Tukey Scheffe)
Ortaokul öğrencilerinin siber güvenlik farkındalıkları toplam puan ve alt boyutlarda İnternet ve bilişim teknolojileri kullanma sürelerine göre farklılaşmakta mıdır?	Oneway Anova (Tukey Scheffe)

Çizelge 3.12.'ye göre ölçeğin genelinin ve alt faktörlerinin çarpıklık değeri -0,561 ile 0,426 arasında, Basıklık değeri ise -0,719 ile -0,315 arasında değiştiği gözlenmiştir. Basıklık ve Çarpıklık değerleri-1.5 ile +1.5 olduğu zaman normal dağılım olduğu kabul edilmektedir

(Tabachnick ve Fidell, 2013). Dolayısıyla veriler normal dağılım sergilemektedir. Bu nedenle araştırmanın alt problemlerinin test edilmesinde çizelge 3.13’de sunulan parametrik testlerden yararlanılmıştır.

Çizelge 3.13.’ de ortaokul öğrencilerinin siber güvenlik farkındalıkları toplam puan ve alt boyutlarda cinsiyet değişkenine göre farklılaşma durumunu analiz etmek amacıyla Bağımsız Gruplar t-Testi, ikiden fazla bağımsız değişkene göre ortalama puanların karşılaştırılmasında ise Varyans Analizi (ANOVA) kullanılmıştır. İlişkilerin belirlenmesinde ise korelasyon ve regresyon analizlerine başvurulmuştur.



4. BULGULAR

Bu bölümde veri analizinden elde edilen bulgular araştırma soruları dikkate alınarak açıklanmıştır.

4.1. SGFÖ Geçerli midir?

SGFÖ' nün geçerli olma durumunu belirlemek amacıyla kapsam geçerliği ve yapı geçerliği incelenmiştir.

4.1.1 SGFÖ' nün kapsam geçerliği

Kapsam geçerliği ölçekte yer alan maddelerden her birinin tek başına ve bütün olarak ölçme amacına ne kadar hizmet ettiği. Kapsam geçerliği için konunun uzmanlarının görüşü alınarak farklı ölçütlere göre değerlendirme yapılması engellenmektedir (Tavşancıl, 2002). Kapsam geçerliği çalışmalarında uzmanlardan alınan geri dönüşler neticesinde 5 soru uygun seviyede olmaması, 2 soru ise Türk Dili Uzmanı görüşleri doğrultusunda çıkarılarak 47 maddelik madde havuzu 40 soruya indirilmiştir.

4.1.2. SGFÖ' nün yapı geçerliği

Doğrudan ölçülemeyen bir özelliği ölçmek amacıyla tasarlanan bir testin ölçme derecesine yapı geçerliliği denir (Alpar, 2012). Ölçülmek istenen yapının ölçeceği düşünülen değişkenlerin oluşturduğu bütünün, öngörülen yapıyı belirleyip belirlemediğinin incelenmesi gereklidir (Alpar, 2016). Birçok araştırmacıya göre yapı geçerliliğini ölçmek için kullanılan en temel istatistiklerden biri de faktör analizidir (Cronbach, 1984; Liao, 2004). Faktör analizi, açıklayıcı faktör analizi (exploratory factor analysis-EFA) ve doğrulayıcı faktör analizi (confirmatory factor analysis-CFA) olmak üzere ikiye ayrılır.

Yapı geçerliliğini test etmek için faktör analizi, iç tutarlılık analizi ve hipotez testleri gibi istatistiksel analiz yöntemleri kullanılmaktadır (Büyüköztürk, 2012). Bu çalışmanın bir parçası olarak, yapı geçerliliğini belirlemek için açıklayıcı faktör analizi (AFA) ve doğrulayıcı faktör analizi (DFA) yapılmıştır.

4.1.3. Açıklayıcı faktör analizi (AFA)

AFA sosyal bilimler alanında gerçekleştirilen çalışmalarda sıklıkla kullanılan ve ölçülmek istenen değişkenler altında yatan gizil değişkenlerin (faktör) tespitinde kullanılan bir istatistik tekniğidir. Büyük miktardaki veri daha az sayıda gruba veya faktöre indirgemek için kullanılan çok değişkenli bir istatistiksel yöntemdir (Güçlü,2019). Ölçek maddelerinin kaç faktör oluşturduğu ve hangi maddelerin hangi faktörleri ölçtüğü kesin olarak belirlenemediği durumlarda kullanılır. İsminden de anlaşıldığı gibi AFA var olan yapıyı açıklamaya yardımcı olur (Hayton, Allen ve Scarpello, 2004). Bir ölçek için hazırlanan madde havuzundaki maddelerin nasıl gruplanacağı alan uzmanı tarafından öngörülse bile var olan yapının tam olarak ne olduğu, kaç gizil değişken (faktör) olduğu ve hangi maddelerin hangi faktörlere yüklendiği istatistiksel bir teknikle belirlenir. Böylece, maddelerden hangilerinin işe yaradığı (varyasyon açıklayıp açıklamadığı) kolaylıkla belirlenebilmektedir. Dolayısıyla, bir ölçek geliştirme işleminde öncelikle var olan gizil yapıyı ortaya koymada kullanılan AFA yöntemi kullanılır (Schumacker ve Lomax, 2004). AFA’ da karşılanması gereken bazı varsayımlar bulunmaktadır.

4.1.4. AFA örneklem büyüklüğü

Örneklem büyüklüğü AFA’da dikkat edilmesi gereken önemli unsurların başında gelmektedir. Gerçekleştirilen analiz sonucunda belli olacak faktör ya da bileşen sayısı üzerinde önemli bir etkiye sahiptir (Zwick ve Velicer, 1986). Örneklem büyüklüğünün fazla olması analiz sonuçlarının güvenilirliğinin artmasına yol açmaktadır. Örneklem büyüklüğü ile ilgili araştırmacılar farklı görüşler ileri sürse de Gorsuch (1974) ve Şencan (2005) madde sayısının 5 katı kadar katılımcının yeterli olacağı belirtilmiştir. Ölçeğin geçerlik ve güvenilirlik çalışmaları kapsamında Amasya ilinde ortaokul düzeyinde eğitim gören 854 öğrenciden toplam 40 soruluk anket aracılığı ile toplanan veriler incelenmiştir. 854 veri ile bu koşul sağlanmış ve madde sayısının 21 katı olması analiz sonuçlarının güvenilirliğini artırmıştır.

Çizelge 4.1. incelendiğinde örneklem 5’inci sınıf (N=135), 6’ncı sınıf (N=244), 7’nci sınıf (N=250) ve 8’inci sınıf (N=225) olmak üzere toplam 854 öğrenciden oluşmaktadır. Uygulama için 854 öğrenciye ulaşılmasının iki yaklaşıma göre de oldukça yeterli olduğu düşünülmektedir.

Çizelge 4. 1. AFA örneklem büyüklüğü

Sınıf	N	%
5	135	15,8
6	244	28,6
7	250	29,3
8	225	26,3
Toplam	854	100,0

Açımlayıcı faktör analizinde ilk olarak verilerin faktör analizine uygunluğunun test edilmesi gerekmektedir. Bu amaçla kullanılabilecek yaklaşımlardan birisi Kaiser-Meyer-Olkin (KMO) örneklem uygunluğu/yeterliği testidir. KMO testi açımlayıcı faktör analizi yapabilmek için örneklem büyüklüğünün yeterliği hakkında bilgi veren bir ölçüttür. Buradaki yeterlik bir sayıyı değil ilişki gücünü ifade etmektedir. Korelasyon matrisinin anlamlılığını gösteren test ise Bartlett Küresellik testidir. Sharma (1996)' ya göre KMO değerleri çizelge 4.2.' de ki gibi yorumlanır.

Çizelge 4. 2. KMO Referans Aralıkları (Sharma, 1996)

KMO Değeri	Değer
Zayıf	<0,5
Orta	0,5-0,6
İyi	0,7-0,8
Çok İyi	0,8-0,9
Mükemmel	0,9 ve Üzeri

KMO değerinin 1'e yakın olması, örneklem yeterliliğinin faktör analizi için o derecede iyi olması anlamına gelmektedir. Verilerin açımlayıcı faktör analizine uygunluğunu değerlendirmek için KMO ve Barlett Küresellik değerleri Çizelge 4.3.' de incelenmiştir.

Bu bağlamda analiz sonucunda çıkan 0,904 değeri örneklem büyüklüğünün çok iyi olduğunu göstermektedir. Barlett's Küresellik Testinde ise verilerin anlamlı olması gerekmektedir. Yapılan test sonucunda anlamlı olduğu ($p<.05$) görülmüştür. Dolayısıyla verilerin faktör analizine uygun olduğuna karar verilmiştir.

Çizelge 4. 3. KMO ölçüm değerleri

Kaiser-Meyer-Olkin KMO Örneklem Yeterliği		,904
Bartlett's Test of Sphericity	Ki-Kare	9791,301
	Sd	300
	p	,000

4.1.5. AFA kayıp verilerin temizlenmesi

AFA kapsamında öncelikle 882 veri bulunan veri seti incelenmiştir. İnceleme sonrasında ölçek formunda yer alan maddelere %10 ve daha fazla oranda cevap vermeyen 28 katılımcı veri setinden çıkarılmış ve 854 katılımcıya ait veriler üzerinde analizler gerçekleştirilmiştir.

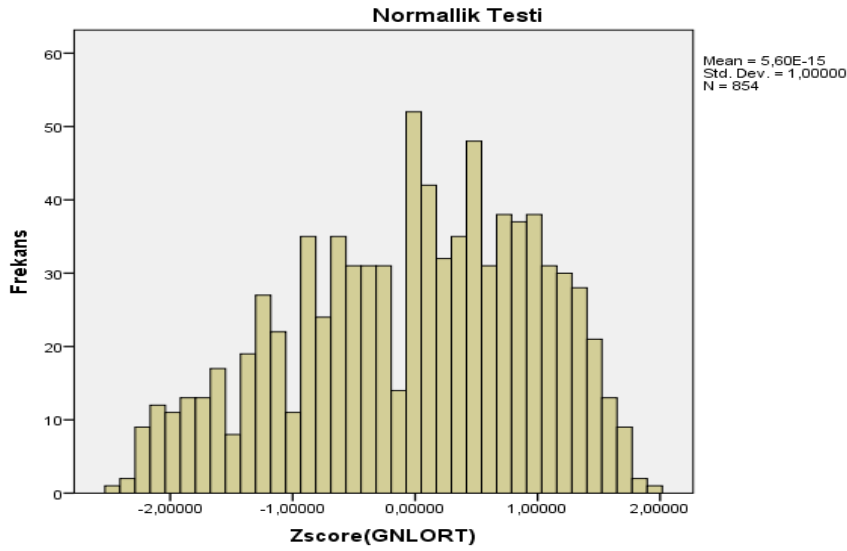
4.1.6. Doğrusallık, normallik ve uç değerler

Faktör analizi kapsamında toplanan değişkenlerin ve bu değişkenlerin tüm doğrusal (lineer) kombinasyonlarının normal dağılım gösterdiği varsayılmaktadır. Toplanan değerlerin dağılım durumu bu varsayımla paralellik gösteriyorsa çözümün değeri artarken normal dağılım ihmal edilirse çözümün değeri azalmaktadır (Tabachnick ve Fidell, 2001). Veriler üzerinden elde edilen Genel Ortalama verileri ile hesaplanan z puanının normallik değerleri için mod, medyan, ortalama ve standart sapma değerlerinin yanı sıra basıklık ve çarpıklık değerleri incelenmiş çizelge 4.4.'de veri setinden elde edilen basıklık ve çarpıklık değerleri paylaşılmıştır. Çarpıklık ve basıklık katsayılarının ± 1 sınırları içinde 0'a yakın olması, çarpıklık ve basıklık katsayılarının kendi standart hatalarına bölünmesi ile hesaplanan çarpıklık ve basıklık indekslerinin ± 2 sınırları içinde 0'a yakın olması, normal dağılımın varlığına kanıt olarak değerlendirilmektedir (Tabachnick ve Fidell, 2013). Verilerin çarpıklık ve basıklık katsayılarının normal dağılıma işaret ettiği anlaşılmıştır. Bu nedenle araştırmanın alt problemlerinin test edilmesinde parametrik fark ve ilişki istatistiklerinden yararlanılmıştır. AFA kapsamında hesaplanan Genel Ortalama değeri üzerinden yapılan normallik testinde örneklem verilerinin normal dağılım gösterdiği tespit edilmiştir.

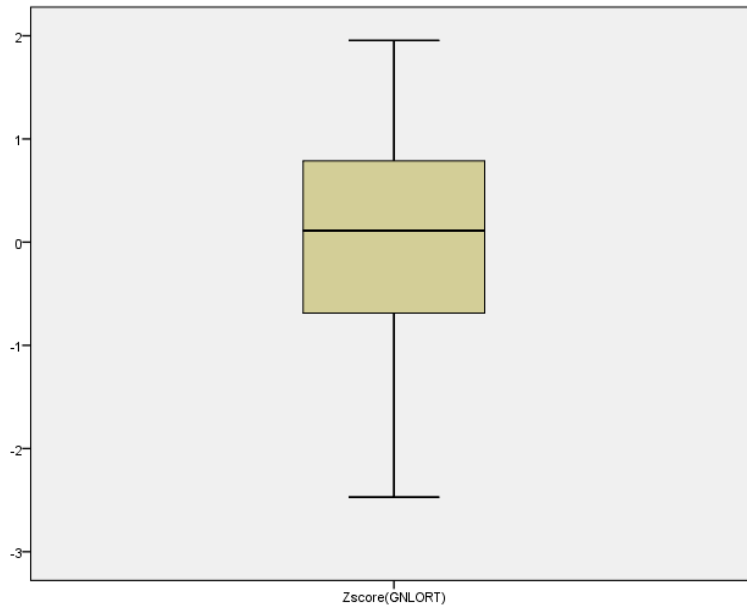
Çizelge 4. 4. Basıklık ve çarpıklık değerleri

	Basıklık	Çarpıklık
Z Puanı	-0,334	-0,753

AFA hesaplama sürecinde diğer tüm çok değişkenli analizlerde olduğu gibi de uç değerler (tek değişkenli veya çok değişkenli) faktör çözümlemeleri sürecinde olumsuz etkiye sahiptir. Bu nedenle AFA öncesinde uç değer analizlerinin yapılması yerinde olacaktır. Veri seti üzerinde yapılan uç değer analizleri sonucu şekil 7’ de paylaşılmış olup herhangi bir uçdeğere rastlanılmamıştır.



Şekil 4. 1. Normal dağılım grafiği



Şekil 4. 2. Genel ortalama Zscore uç değerleri

4.1.7. AFA bulguları

Ölçeğin yapı geçerliliğinde öncelikle madde analizi yapılmıştır. Madde analizi işlemleri, ölçekteki maddelerin, ölçeğin ölçmeyi amaçladığı bir özelliği başka özelliklerle karıştırmadan ölçüp ölçmediğini belirleyerek kendi içinde tutarlı bir ölçek oluşturmak için yapılmaktadır (Tavşancıl; 2006:151). Likert tarafından her bir maddenin ölçme gücünü belirleyebilmek için önerilen yöntemlerden biri olan korelasyona dayalı madde analizi (Akt. Tezbaşaran; 1996:28) uygulanmıştır. Madde ölçek korelasyonunda ise .30 ve daha yüksek olan maddelerin bireyleri iyi derecede ayırt ettiği, .20-.30 arasında kalan maddelerin zorunlu görülmesi durumunda alınabileceği, .20'den düşük maddelerin ise ölçeğe alınmaması gerektiği (Büyüköztürk; 2006:171) ifade edilmektedir. Bu kapsamda ölçeğin toplam puanları ile her bir maddenin puanı arasındaki ilişki için .30 sınır değeri olarak kabul edilmiştir. Madde-Ölçek Korelasyon Katsayısı analizi aşağıda çizelge 4.5.' de verilmiştir.

Çizelge 4. 5. Madde-ölçek korelasyon katsayısı analiz sonuçları

Madde No	r	Madde No	r
M1	0,26	M21	0,22
M2	0,25	M22	0,50*
M3	0,11	M23	0,44*
M4	0,35*	M24	0,45*
M5	0,29	M25	0,48*
M6	0,45*	M26	0,41*
M7	0,05	M27	0,33*
M8	0,23	M28	0,41*
M9	0,33*	M29	0,41*
M10	0,31*	M30	0,41*
M11	0,37*	M31	0,31*
M12	0,34*	M32	0,35*
M13	0,41*	M33	0,21
M14	0,39*	M34	0,41*
M15	0,39*	M35	0,41*
M16	0,40*	M36	0,43*
M17	0,42*	M37	0,38*
M18	0,24	M38	0,29
M19	0,40*	M39	0,51*
M20	0,27	M40	0,50*

Çizelge 4.5.'de yer alan verilere göre; 3 ve 7 numaralı maddelerin korelasyon katsayısı, .20'den düşük olduğu için ölçekten çıkarılmıştır. 1, 2, 5, 8, 18, 20, 21, 33 ve 38 numaralı maddelerin korelasyon katsayısı ise .21 ile .29 arasında değişmektedir. Bu maddeler .30'un üzerinde olmadığı ve güvenilirliği düşürdüğü için çıkarılmıştır. Diğer maddeler sınır değer olarak kabul edilen .30'un üzerinde ve 0,01 düzeyinde anlamlı bulunmuştur. Dolayısıyla 40 maddelik ölçekten 11 madde çıkarılmış ve yapı geçerliliği analizine bireyleri iyi derecede ayırt edileceği düşünülen 29 madde alınmıştır.

Ölçme aracının yapı geçerliği ve çok sayıdaki faktörlerden daha az sayıda yeniden faktör oluşturmak, temel faktörlerin neler olduğunu ve bu faktörlerden her birinin değişkenlerden her birini açıklama derecesini görmek için faktör analizi yapılmış olup (Altunışık ve diğ.; 2005:212) faktör analizi yaklaşımlarından da değişkenler arasındaki ilişkilerden hareketle açıklayıcı (keşfedici, exploratory) yaklaşım kullanılmıştır (Büyüköztürk; 2006:123). Faktör analizinde; faktörlerin kendileriyle yüksek ilişki veren maddeleri bulmak dolayısıyla faktörlerle ilgili yapılacak yorumun daha anlamlı ve açık olması için dik döndürme yöntemlerinden varimax tekniği kullanılmıştır.

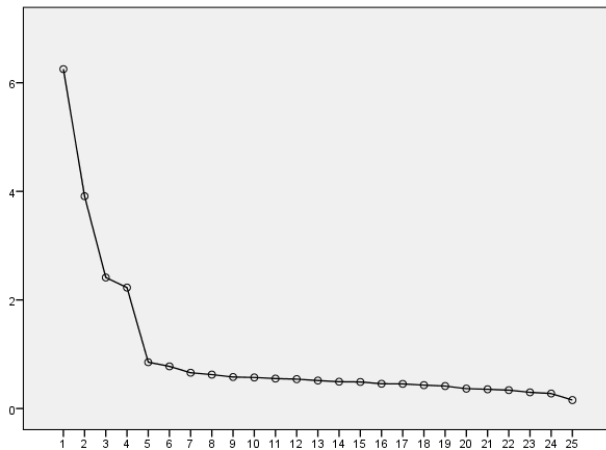
Faktör analizinde madde çıkarılmasında üç ölçüt temel alınmıştır. Bunlar; ortak yük (Communalities) oranı, faktör yük değeri sınırı ve binişik madde bulunmamasıdır. Her bir maddenin ortak varyansı olarak nitelendirilen “ortak yüklerde (Communalities)” 1'e yakın maddelerin seçimi ölçeğin yapısına ve faktörlerin oluşumuna katkıda bulunmaktadır. Bununla birlikte faktör yük değeri .30 sınır değer olarak kabul edilir ve birden fazla faktörde 0,1'den daha az bir farkla yer alan herhangi bir madde, binişik bir madde olarak değerlendirilir ve bu maddeler ölçekten çıkarılır (Büyüköztürk, 2002). Faktör sayısının belirlenmesi işleminde değişkenler arasındaki ilişkileri en yüksek derecede temsil edecek az sayıda faktör belirlenir. Faktör analizinde açıklanan varyans oranlarının tek faktörlüde %30 ve daha fazla olması, çok faktörlülerde bu oranın üzerinde olması uygun görülmektedir (Büyüköztürk; 2006:125).

1. Özdeğerlere (Eigenvalues) Göre Belirleme: Özdeğeri bir ve birden büyük ($\lambda \geq 1$) olan faktörler hesaba katılır. Özdeğeri 1'den küçük olan faktörler hesaba katılmaz. Özdeğer bir faktör tarafından açıklanan toplam varyansı gösterir.

2. Serpilme Diyagramına (ScreePlot) Göre Belirleme: Özdeğerlerin grafiği çizilir. Düşey çizgini yataylaştığı yere kadar olan faktörler çözüme dahil edilir. Diyagramda x eksenini faktörleri, y eksenini özdeğerleri gösterir (Lewis-Beck, 1994).
3. Varyans Oranına Göre Belirleme: Özdeğerlerin açıkladıkları birikimli varyans miktarının toplam varyansı tahmin edici bir düzeye gelene kadar faktörler modele alınır. Analiz sonucunda elde edilen varyans oranları ne kadar büyükse faktör yapısı da o kadar güçlü olur. Genelde %40' üzerinde olması istenir.

Ayrıca; ölçek için yapılan faktör analizi sonucunda oluşan faktörler arasındaki ilişkinin belirlenmesi amacıyla faktörler arasındaki korelasyon katsayısına da bakılmıştır.

Uygulanan faktör analizinde madde seçiminde belirlenen ölçütler kapsamında maddeler seçilmiştir. Ölçekte yer alan dört maddenin (m12,m27,m29 ve m31) ortak varyansa katkısı düşük olup varyansın en düşük %16,6'sını ve en yüksek %27,4'ünü açıklamaktadırlar. Bununla birlikte dört maddenin faktör yük değerlerinin .30'un altında ve birden fazla faktörde yük değerleri olduğu diğer ifade ile faktör yük değerlerinin birbirine yakın oranlarda olduğu (binişik madde) görülmüş her bir madde çıkarıldıktan sonra döndürme yöntemi tekrar edilmiştir. Sonuç olarak uygulanan analiz ile Siber Güvenlik Farkındalığı Ölçeği 25 maddeden oluşmuştur.



Şekil 4. 3. Faktör saçılım grafiği

Şekil 4.3. faktörlere ait saçılım grafiğinde görüldüğü üzere eğim birinci noktadan sonra plato şeklinde hareket etmektedir. Bu noktada faktör sayısı için kesme noktası bir olarak

belirlenmiştir (Çokluk, Şekercioğlu ve Büyüköztürk; 2012). Toplam Varyans Değerleri çizelgesi dikkate alındığında dördüncü ve beşinci faktör arasındaki farkın yüksekliği ve beşinci faktörden sonraki değerlerin birbirine yakınlığı da hesaba katılarak faktör sayısının dört olmasına karar verilmiştir.

Uygulanan analiz sonucunda, yedi maddeden oluşan birinci faktörün yük değerleri 0,878-0,767 arasında değişmekte olup “Şifre Güvenliği” olarak adlandırılmıştır. İkinci faktör, 7 maddeden oluşmuş ve faktör yük değerleri 0,763-0,521 arasındadır. Maddelerin içeriği incelenerek “Önleyici Tedbirler” olarak adlandırmanın uygun olacağına karar verilmiştir. Altı maddeden oluşan maddelerin yük değerleri 0,767-0,698 arasında değişen üçüncü faktörde “Kötü Amaçlı Yazılım Farkındalığı” olarak adlandırılmıştır. Dördüncü faktör ise beş maddeden oluşmaktadır. Beş maddenin yük değerleri 0,832-0,707 arasında değişmektedir. Dördüncü faktör “Kişisel Gizliliği Koruma” olarak isimlendirilmiştir.

Çizelge 4. 6. Faktör analizi sonuçları (döndürülmüş temel bileşenler analizi sonuçları)

Madde	Communalities Ortak Varyansı	Döndürme Sonrası Yük Değeri			
		Faktör 1	Faktör 2	Faktör 3	Faktör 4
M39	,795	,878			
M40	,784	,877			
M6	,718	,841			
M22	,705	,829			
M11	,631	,791			
M36	,603	,767			
M15	,611	,767			
M35	,600		,763		
M26	,565		,743		
M25	,585		,742		
M4	,479		,682		
M28	,465		,657		
M13	,446		,630		
M34	,332		,521		
M32	,604			,767	
M9	,587			,760	
M37	,590			,751	
M24	,633			,748	
M30	,555			,706	
M10	,504			,698	
M17	,701				,832
M19	,593				,767
M16	,607				,761
M14	,553				,724
M23	,555				,707

Çizelge 4. 7. Ölçek boyutları ve açıklanan varyans değerleri

	Faktör 1	Faktör 2	Faktör3	Faktör4	Toplam
Madde Sayısı	7	7	6	5	25
Açıklanan Varyans	19,274	14,077	13,914	11,944	59,209
Güvenirlik Katsayısı	0,92	0,82	0,85	0,83	0,87

Çizelge 4.7.'de görüldüğü üzere birinci faktör toplam varyansın yüzde 19,274'ünü açıklarken ikinci faktör yüzde 14,077'sini üçüncü faktör yüzde 13,914'ünü açıklamaktadır. Dördüncü faktör ise yüzde 11,944 oranında toplam varyansı açıklamaktadır. Dört faktörün birlikte açıkladıkları toplam varyans ise yüzde 59,209'dur.

Çalışmada güvenirlik yaklaşımlarından biri olan ve yaygın olarak kullanılan iç tutarlılık analizlerinden Cronbach Alfa olarak da bilinen, alfa katsayısı yöntemi kullanılmıştır. Kalaycı (2008:405); Alfa katsayısı 0,00-0,40 ise ölçek güvenilir değil; 0,40-0,60 ise ölçeğin güvenirliği düşük; 0,60-0,80 ise ölçek oldukça güvenilir; 0,80-1,00 ise ölçek yüksek derecede güvenilir bir ölçek şeklinde ifade etmektedir.

Yapılan işlem neticesinde 25 maddeden oluşan Siber Güvenlik Ölçeğinin alfa değeri 0,87 olarak hesaplanmıştır. Ölçek maddelerinin birbirleriyle olan tutarlılığını belirlemede bir ölçü olarak kullanılan Cronbach Alfa katsayısının 0.60 ile 0.80 arasında değer alması ölçeğin oldukça güvenilir olduğunu, 0.80 ile 1.00 arasında değer alması ölçeğin yüksek güvenirlikte olduğunu göstermektedir (Uzunsakal ve Yıldız, 2018). Bu kapsamda geliştirilen ölçeğin yüksek düzeyde güvenilir olduğu söylenebilir.

Faktörler arasındaki ilişkinin belirlenmesi için Siber Güvenlik Ölçeği'ni oluşturan faktörler arasındaki korelasyon katsayısı hesaplanmıştır. Faktörler arasındaki korelasyon katsayısı aşağıda çizelge 4.8.'de verilmektedir.

Çizelge 4. 8. Siber güvenlik ölçeğini oluşturan faktörler arasındaki korelasyon katsayısı

Faktörler	1	2	3	4
1	1			
2	,25**	1		
3	,14**	,36**	1	
4	,10**	,26**	,25**	1

Çizelge 4.8.'de faktörler arasındaki korelasyon katsayılarının düşük olduğu görülmektedir. Buna göre, faktörlerin ölçtükleri özellik bakımından birbirinden farklılaştığı söylenebilir.

4.1.8. Doğrulayıcı faktör analizi (DFA)

Doğrulayıcı Faktör Analizi (DFA), katılımcılardan toplanan verinin temelindeki yapıyı değerlendiren açıklayıcı faktör analizinin (AFA) uzantısıdır. AFA kurulan hipoteze yönelik bilgi edinilmesini sağlarken DFA, verilerin içerisinden ortaya çıkan faktörler arasındaki ilişkiyi ve bu ilişkinin büyüklüğünü, faktörlerin birbirlerinden bağımsız olup olmadığını, faktörlerin modeli açıklamakta yeterli olup olmadığını sınamak için kullanılır. DFA'nın öncelikli amacı, tasarlanan faktör modelinin elde edilen veri seti ile ne kadar uyumlu olduğunu belirlemektir. DFA dört temel amaç için kullanılmaktadır. Bunlar, test araçlarının psikometrik değerlendirmesi, yapı geçerliliği, metot etkileri ve ölçüm değişmezliği hesaplamalarıdır.

Faktör analizi sonucunda ölçeğin dört faktörlü bir yapıya sahip olduğu belirlenmiştir. Bu dört boyutlu yapının geçerliğinin test edilmesi için Doğrulayıcı Faktör Analizi (DFA) uygulanmıştır. Doğrulayıcı faktör analizi, belirli değişkenlerin bir kuram temelinde önceden belirlenmiş faktörler üzerinde ağırlıklı olarak yer alacağı şeklindeki bir ön beklentinin sınanmasına dayanır. Bu nedenle analizde yer alacak değişkenler, kuramın sayıltıları doğrultusunda seçilir ve bu değişkenlerin istenilen faktörlerde ne oranda yer aldıklarına bakılır (Çapa, Çakıroğlu ve Sarıkaya, 2005; Deryakulu ve Büyüköztürk, 2005; Özer, 2005).

4.1.9. Doğrulayıcı faktör analizi ön deneme uygulama ve veri toplama süreci

Açımlayıcı Faktör Analizi sonucunda belirlenmiş olan ölçeğe son şekli verilerek Doğrulayıcı Faktör Analizi için tekrar uygulanmıştır. Doğrulayıcı Faktör Analizinin uygulamasında açımlayıcı faktör analizine katılan öğrencilerden farklı olarak 5. sınıfta öğrenim gören 107 öğrenci, 6. sınıfta öğrenim gören 163 öğrenci, 7. sınıfta öğrenim gören 158 öğrenci ve 8. sınıfta öğrenim gören 168 öğrenci olmak üzere toplam 644 öğrenciye uygulanmıştır. Ölçek formunda yer alan maddelere %10 ve daha fazla oranda cevap vermeyen 48 katılımcı veri setinden çıkarılmıştır (Tabachnick ve Fidell, 2013). Elde edilen veriler bilgisayara aktarılmış ve verilerin çözümlenmesinde LISREL 8.80 (Linear Structural Relation Statistics Package Program) programı kullanılmıştır.

4.1.10. Modelin betimlenmesi

Araştırma modeli belirlenirken betimsel araştırmanın tercih edilmesi öz aktarım yoluyla yani verilerin örnekleme yer alan bireylerden elde edilmesi gerekliliğinden yola çıkılmıştır. Yapısal eşitlik modellemesi (YEM) tabanlı analiz programları ile gerçekleştirilen Doğrulayıcı Faktör Analizinde (DFA), regresyon analiz tekniği gibi birinci nesil istatistiksel tekniklere göre faktörler arası ilişkiler, birçok bağımlı ve bağımsız değişkenler arasındaki ilişkilerin modellenebilmesine imkân sunmasının yanı sıra, faktör ağırlıkları, modellerin sınanması ve bir modelin uygunluk derecesi elde edilebilir (Sümer, 2000). DFA’ da son yıllarda ölçek uyarlama ve ölçek geliştirme çalışmalarında sıklıkla kullanıldığı görülmektedir (Çapa, Çakıroğlu ve Sarıkaya, 2005; Deryakulu ve Büyüköztürk, 2005; Özer, 2005). YEM’ in, birçok farklı alanda yoğun olarak kullanılması (Hershberger, 2003), geleneksel yöntemlerden farklı olarak gözlenen değişkenlere ait ölçüm hatalarını dikkate almasından kaynaklanmaktadır (Schumacker ve Lomax, 2004; Stevens, 2009).

4.1.11. Modelin tanımlanması

Model tanımlama YEM’ ler ile ilgili olup belirlenen parametreler doğrultusunda ölçülmek istenen değişkenlerin varyans ve kovaryans dağılımlarının kendine has özellikleridir. DFA’de model tanımlanırken modeldeki faktörler izlenemez ve içsel ölçeklere sahip olmadıkları için her bir modele ait tek bir çözüm bulunmaktadır. Bu nedenle faktörler kendilerine has ölçeklerle ölçülmektedir. (Stevens, 2001: 429). Model tanımlanması oluşturulduktan sonra; faktör yükleri, faktör korelasyonu ve ölçüm hata varyansı tahmin edilecektir.

4.1.12. Model uyumunun incelenmesi

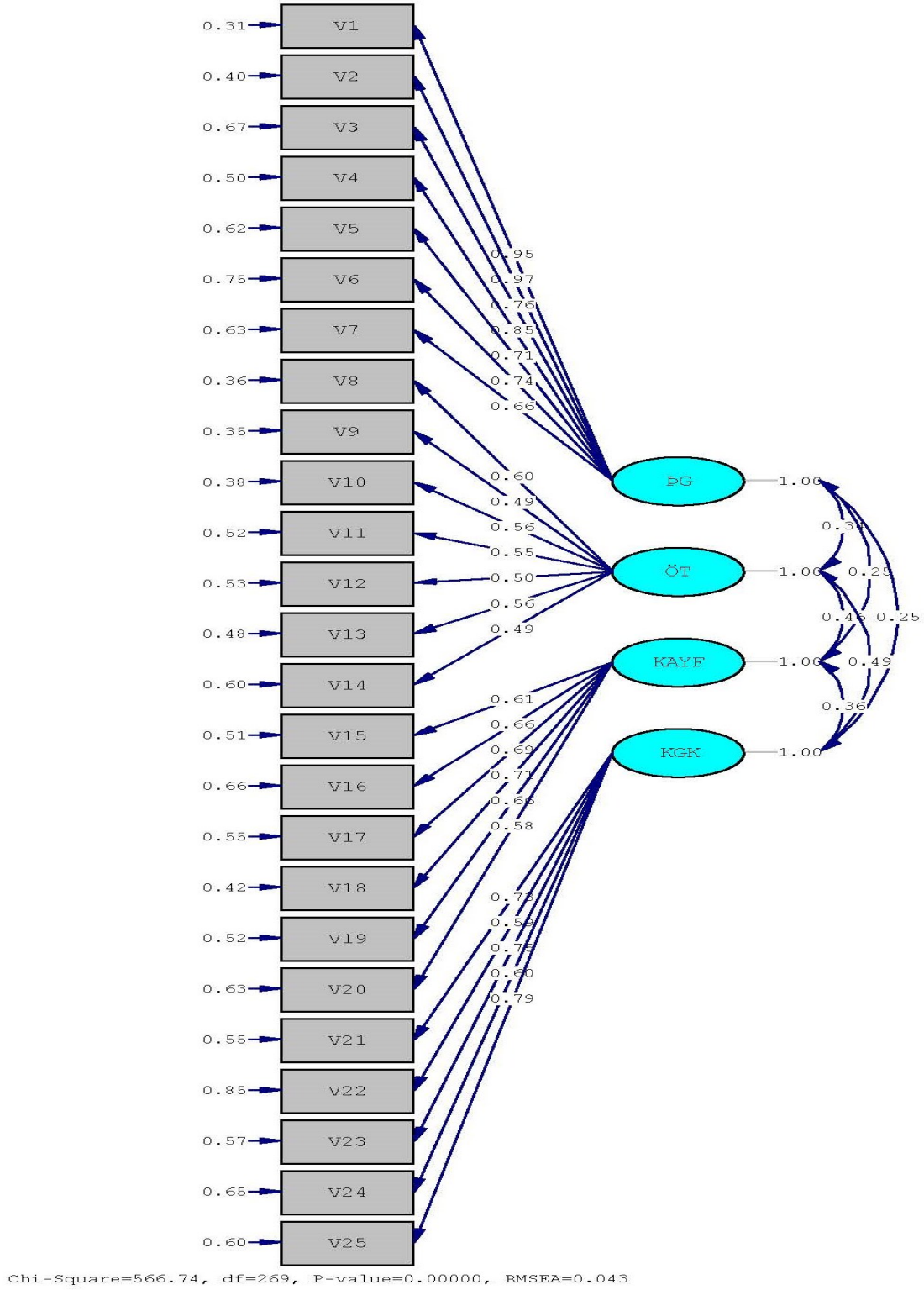
Çalışmada uygulanan AFA sonucunda 25 maddeli ve 4 faktörlü oluşan yapının uyumluluğu DFA ile kontrol edilmiştir. DFA sonuçlarının yorumlanmasında ise hangi uyum kriterlerinin alınacağına ilişkin kesinlik bulunmamakta birden fazla uyum indeksinin bir arada kullanılması önerilmektedir (Çokluk, Şekercioğlu, Büyüköztürk, 2012). Uyum indeksleri değerlendirilirken Çizelge 4,9’ da verilen uyum istatistikleri, uyum değerleri ve uyum aralıkları (Kline, 2005, Şimşek, 2007; Akt. Evcı ve Aylar, 2017; Çokluk, Şekercioğlu, Büyüköztürk, 2012) temel alınarak analiz sonuçları yorumlanmıştır.

Çizelge 4.9. DFA sonuçları

Uyum Kriterleri	Mükemmel Uyum	Kabul Edilebilir Uyum	DFA Sonuçları
χ^2 (Kikare) Uyum testi	$0,05 < p \leq 1$	$0,01 < p \leq 0,05$	
χ^2/sd	$\chi^2/sd \leq 3$	$\chi^2/sd \leq 5$	2,105
IFI	$0,95 \leq IFI \leq 1$	$0,90 \leq IFI \leq 0,96$	0,98
CFI	$0,97 \leq CFI \leq 1$	$0,90 \leq CFI \leq 0,96$	0,98
GFI	$0,95 \leq GFI \leq 1$	$0,90 \leq GFI \leq 0,96$	0,93
AGFI	$0,95 \leq AGFI \leq 1$	$0,90 \leq AGFI \leq 0,96$	0,91
NFI	$0,97 \leq NFI \leq 1$	$0,90 \leq NFI \leq 0,96$	0,96
NNFI	$0,97 \leq NNFI \leq 1$	$0,90 \leq NNFI \leq 0,96$	0,97
RMSEA	$0 < RMSEA < 0,05$	$0,06 \leq RMSEA < 0,08$	0,04
RMR	$0 < RMR \leq 0,05$	$0 < RMR \leq 0,08$	0,07
SRMR	$0 \leq S-RMR \leq 0,05$	$0,06 \leq S-RMR \leq 0,08$	0,04

Uyum iyiliği indeksleri için 0,90-0,95 kabul edilebilir ve 0,95 üzerinde olması ise yüksek bir uyumun göstergesi olarak nitelendirilmektedir (Dickey, 1996; Stapleton, 1997; Byrne, 1998, Akt. Doğan ve Başokçu, 2010; Munro 2005; Şimşek 2007). Diğer taraftan; χ^2 değerinin 0'a yakın ve p değerinin manidar olmaması, χ^2 / sd oranının 3'ten küçük olması "mükemmel uyum", 5'e kadar değerlerde "kabul edilebilir uyum" Standardize Edilmiş Hataların Ortalama Karelerinin Karekökü (S-RMS) ve Hataların Ortalama Karekökü'nün (RMSEA) ise 0,05'den küçük olması "mükemmel" 0,06 ve 0,08 aralığında olması ise "kabul edilebilir" uyum (Kline,2005; Sümer, 2000; Akt: Çokluk ve diğerleri 2012) olarak açıklanmaktadır. Bu nedenle modelin veriye uyum derecesi yorumlanırken; Karşılaştırmalı Uyum İndeksi (Comparative Fit Index -CFI), İyilik Uyum İndeksi (Goodness of Fit Index -GFI), Düzeltilmiş uyum iyiliği İndeksi (Adjusted Goodness of Fit Index-AGFI), Normlaştırılmış Uyum İndeksi (Normed Fit Index-NFI), Normlaştırılmamış Uyum İndeksi (Non-normed Fit Index-NNFI), Artımlı Uyum İndeksi (Incremental Fit Index-IFI) indekslerinin 1'e yakın olmasına, χ^2 / sd oranının 3'ten ve (Standardized Root Mean Square Residual-SRMS) ve Yaklaşık hataların ortalama Karekökü (Root Mean Square Error of Approximation- RMSEA)'nın 0,08'den küçük olmasına ve t değerlerinin 0.05 düzeyinde anlamlı olmasına dikkat edilmiştir.

LİSREL 8.80(Linear Structural Relation Statistics Package Program) programı kullanılarak yapılan DFA sonuçları aşağıda Şekil 4.4.' de verilmiştir.



Şekil 4. 4. Birinci düzey doğrulayıcı faktör analizi

Birinci düzey analiz sonuçları çizelge 4.10.' da sunulmuştur.

Çizelge 4. 10. DFA için uyum indeksleri

χ^2	Df	P	χ^2/df	GFI	CFI	RMSEA
566,44	269	0,00000	2,105	0,93	0,98	0,04

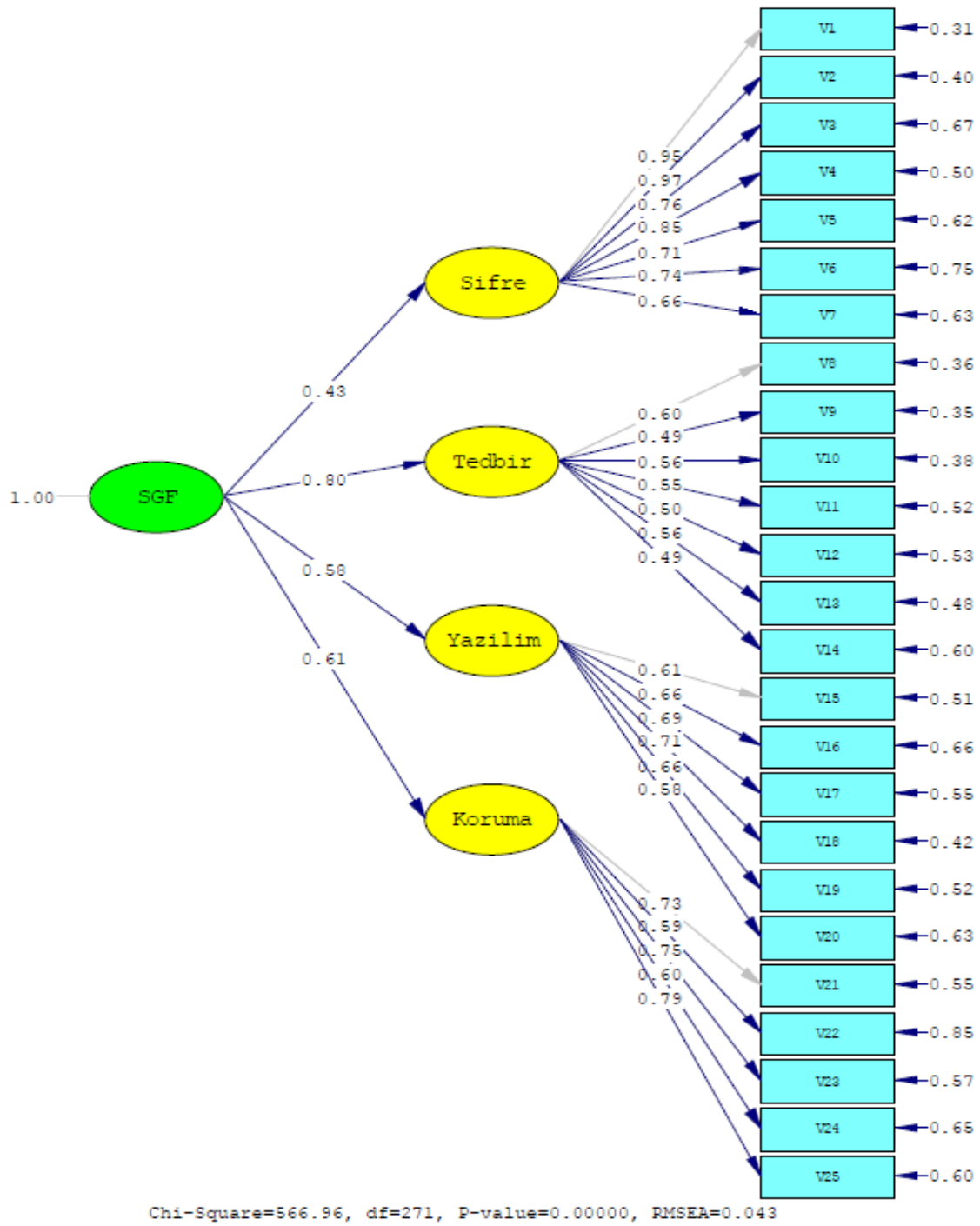
Çizelge 4.10.' a göre $\chi^2=566,44$, sd=269 olup Ki kare/sd=2,10 olduğu tespit edilmiş olup bu değer 3'ten küçük ve RMSEA=0,04 değeri ile S-RMR=0,04 değeri 0,05'den küçük olduğu için mükemmel derecede uyumlu olarak nitelendirilmiştir.

Çizelgedeki verilere göre GFI=0,93 ve AGFI= 0,91, NFI=0,96, NNFI=0,97, IFI=0,98 ve CFI=0,98 olduğu saptanmıştır. Bu değerler 1'e yakın olduğu için "mükemmel" uyum göstergesi olarak kabul edilmiştir. Bunlarla birlikte ölçekte yer alan tüm maddelerin örtük değişkenleri açıklamada t değerleri de göz önünde bulundurulmuştur. Analiz sonucunda elde edilen t değerlerine ilişkin sonuçlar aşağıda verilmiştir.

Çizelge 4. 11. Siber güvenlik farkındalığı ölçeğinde yer alan maddelere ait t değerleri

Madde Numarası	t değeri	Madde Numarası	t değeri
1	25,66	14	12,94
2	24,46	15	16,45
3	18,24	16	15,74
4	21,49	17	17,53
5	17,92	18	19,23
6	17,07	19	17,2
7	16,82	20	14,58
8	18,11	21	17,76
9	15,98	22	12,78
10	16,98	23	17,74
11	14,92	24	14,47
12	13,71	25	18,02
13	15,77		

Çizelge 4.11'deki verilere göre t değerleri; $m22=12,78$ ile $m1=25,66$ arasında değişmekte olup ölçeğe ait tüm maddelerin t değerlerinin $p<.05$ düzeyinde anlamlı olduğu görülmüştür. Birinci Düzey Faktör analizinde modifikasyon yapılmamıştır. Çok faktörlü yapı için ikinci düzey analiz uygulanarak aşağıda verilmiştir.



Şekil 4. 5. İkinci düzey doğrulayıcı faktör analizi

Şekil 4.5.'de görüldüğü üzere dört faktörün Siber Güvenlik Farkındalığı Ölçeğini açıklamada; t değerleri 0,05 düzeyinde anlamlı bulunmuştur. Ayrıca uyum indeks değerleri incelendiğinde $\chi^2 = 543,99$ değeri ve $sd = 271$ olup $Kikare/sd = 2,00$ olduğu tespit edilmiştir. Bu değer 3'ten küçük olduğu için "mükemmel derecede" uyum olarak değerlendirilmiştir. Şekil 4.11' e göre GFI=0,93 ve AGFI=0,92, NFI=0,96, NNFI=0,97, IFI=0,98 ve CFI=0,98 olduğu saptanmıştır. Analiz sonucu bulunan bu değerler ölçeğin uyumunun "mükemmel" düzeyde olduğunu göstermektedir.

4.2. Siber Güvenlik Farkındalığı Ölçeği Güvenirlik Ölçütlerini Karşılama mıdır?

Bu araştırma sorusuna cevap vermek üzere, çalışmada güvenilirlik yaklaşımlarından biri olan ve yaygın olarak kullanılan iç tutarlılık analizlerinden Cronbach Alfa olarak da bilinen, alfa katsayısı yöntemi kullanılmıştır. Kalaycı (2008:405); Alfa katsayısı 0.00-0.40 ise ölçek güvenilir değil; 0.40-0.60 ise ölçeğin güvenirliliği düşük; 0.60-0.80 ise ölçek oldukça güvenilir; 0.80-1.00 ise ölçek yüksek derecede güvenilir bir ölçek şeklinde ifade etmektedir.

Çizelge 4.12. SGFÖ güvenirlilik katsayısı değerleri

Faktörler	Cronbach Alpha Güvenirlilik Katsayısı
1. Şifre Güvenliği	0.92
2. Önleyici Tedbirler	0,82
3. Kötü Amaçlı Yazılım Farkındalığı	0,85
4. Kişisel Gizliliği Koruma	0,83
Ölçeğin Geneli	0,87

4.2.1. Ölçeğin kullanımı

Geliştirilen 25 maddelik ölçeğin son hali ek-1 de sunulmuştur. Ölçek uygulanırken Şifre Güvenliği alt boyutunda yer alan ve 3' üncü soru "Kişisel bilgilerimin yer aldığı şifre oluşturmakta sakınca görmüyorum." ve Kişisel Gizliliği Koruma alt boyutunda yer alan 22' inci soru "Tanıdığım kişiden gelen e-postada kişisel bilgilerim istenirse paylaşırım." soruları ters madde olarak hazırlanmış ve veri seti hazırlanırken ters madde olarak işlenmiştir. Ölçek puan hesaplama tablosu çizelge 4.13 'te gösterilmiştir.

Çizelge 4.13. Ölçek puan hesaplama tablosu

Ölçek Alt Boyut	Madde Sayısı	Taban Puan	Tavan Puan
1. Şifre Güvenliği	7	7	35
2. Önleyici Tedbirler	7	7	35
3. Kötü Amaçlı Yazılım Farkındalığı	6	6	30
4. Kişisel Gizliliği Koruma	5	5	25
Toplam	25	25	125

SGFÖ ölçek toplam puanı üzerinden değerlendirilmektedir. Ölçekte Şifre Güvenliği, Önleyici Tedbirler, Kötü Amaçlı Yazılım Farkındalığı ve Kişisel Gizliliği Koruma olmak üzere 4 alt boyut bulunmaktadır. Şifre Güvenliği alt boyutundan (7 madde) en az 7 en fazla 35 puan, Önleyici Tedbirler alt boyutundan (7 madde) en az 7 en fazla 35 puan, Kötü Amaçlı Yazılım Farkındalığı (6 madde) en az 6 en fazla 30 puan, Kişisel Gizliliği Koruma (5 madde) en az 5 en fazla 25 puan olmak üzere ölçekten en az 25 en fazla 125 puan alınabilir. Ölçek toplam puan değerlerine göre çizelge 4.14’ de görüldüğü gibi yorumlanmalıdır.

Çizelge 4.14. SGFÖ toplam puan yorum çizelgesi

Toplam Ölçek Puanı (x)	Değer
$25 \leq x \leq 58$	Düşük
$59 \leq x \leq 92$	Orta
$93 \leq x \leq 125$	Yüksek

Ölçekten elde edilen toplam puan 25 ve 58 aralığında ise “siber güvenlik farkındalığı düşük” ya da “düşük düzey siber güvenlik farkındalığına sahip”, 59 ve 92 aralığında ise “orta düzey siber güvenlik farkındalığına sahip”, 93 ve 125 aralığında ise “siber güvenlik farkındalığı yüksek” ya da “yüksek düzey siber güvenlik farkındalığına sahip” olarak yorumlanmaktadır.

4.3. SGFÖ’nün Uygulanmasına İlişkin Bulgular

Bu bölümde ortaokul öğrencilerinin siber güvenlik farkındalık düzeyleri, cinsiyet, sınıf düzeyi ve internet ve bilişim teknolojileri kullanım düzeyi değişkenlerine göre incelenmiş ve bulguları aşağıda sunulmuştur.

4.3.1. Cinsiyet değişkenine yönelik bulgular

Araştırmanın birinci alt problemi “Ortaokul öğrencilerinin siber güvenlik farkındalıkları toplam puan ve alt boyutlarda cinsiyet değişkenine göre farklılaşmakta mıdır?” olarak belirlenmiştir. Yapılan bağımsız örneklem t testi sonucu çizelge 4.15’ de sunulmuştur.

Çizelge 4.15. Cinsiyet değişkenine göre T testi sonuçları

	Cinsiyet	N	$\bar{x}$	ss	t	sd	p
Şifre	Kız	246	3,6905	,60431	-1,582	528	,114
Güvenliği	Erkek	284	3,7681	,52532			
Önleyici	Kız	246	4,1190	,65307	-2,342	528	,020
Tedbirler	Erkek	284	4,2505	,63711			
Kötü Amaçlı	Kız	246	3,8855	,75284	-,429	510,923	,668
Yazılım	Erkek	284	3,9131	,72404			
Farkındalığı							
Kişisel	Kız	246	3,5634	,58313	,001	527,639	,999
Gizliliği	Erkek	284	3,5634	,65598			
Koruma							
SGFÖ Toplam	Kız	246	3,8319	,51253	-1,498	507,525	,135
	Erkek	284	3,8970	,48401			

Ortaokul öğrencilerinin SGFÖ toplam puanları cinsiyete göre farkların istatistiksel olarak anlamlı bulunmamıştır ($t=-1,498$; $p > 0,05$). Çizelge 4.15’de SGFÖ ölçeği alt boyutlarında Şifre Güvenliği ($t=-1,582$; $p>0,05$), Kötü Yazılım($t=-,429$; $p>0,05$) ve Kişisel Gizliliği Koruma ($t=,001$; $p>0,05$) alt boyutlarında istatistiksel olarak anlamlı bir farklılık bulunmamıştır. Önleyici Tedbirler alt boyutunda cinsiyete göre farkların istatistiksel olarak erkek öğrenciler lehine anlamlı bulunmuştur ($t=-2,342$; $p<0,05$).

4.3.2. Sınıf düzeyi değişkenine yönelik bulgular

Araştırmanın ikinci alt problemi “Ortaokul öğrencilerinin siber güvenlik farkındalıkları toplam puan ve alt boyutlarda sınıf düzeyi değişkenine göre farklılaşmakta mıdır?” olarak belirlenmiştir. Öğrencilerin siber güvenlik farkındalık düzeylerinin sınıf değişkenine göre

anlamlı farklılık olup olmadığını tespit edebilmek için Tek Yönlü Varyans Analizi (One-Way Anova) yapılmış ve sonuçları aşağıda Çizelge 4.16.’da verilmiştir.

Çizelge 4.16. SGFÖ sınıf düzeyi değişkenine göre Anova testi sonuçları

Faktörler	Varyansın Kaynağı	Kareler Toplamı	sd	Kareler ortalaması	F	p
Şifre Güvenliği	Gruplar Arası	2,527	3	,842	2,671	0,05
	Grup İçi	165,836	526	,315		
	Toplam	168,363	529			
Önleyici Tedbirler	Gruplar Arası	,976	3	,325	0,775	0,51
	Grup İçi	220,668	526	,420		
	Toplam	221,643	529			
Kötü Yazılım	Gruplar Arası	1,018	3	,339	0,623	0,60
	Grup İçi	286,299	526	,544		
	Toplam	287,317	529			
Kişisel Gizliliği Koruma	Gruplar Arası	3,386	3	1,129	2,943	0,03*
	Grup İçi	201,704	526	,383		
	Toplam	205,090	529			
SGFÖ Toplam	Gruplar Arası	1,152	3	,384	1,554	0,20
	Grup İçi	130,062	526	,247		
	Toplam	131,215	529			

Çizelge 4.16.’ da yer alan analiz sonucuna ilişkin değerlerde “Kişisel Gizliliği Koruma” faktörü dışında ($F_{(3,526)} = 2,943$, $p < ,05$) SGFÖ toplamında ve diğer alt boyutlarında sınıf düzeyine göre istatistiksel olarak anlamlı farklılık olmadığı görülmüştür ($p > 0,05$). Ortalamaları kıyaslanan 4 gruptan en az ikisinin ortalamaları arasında anlamlı fark vardır. Anlamlı farkın hangi gruplar arasında oluştuğunu tespit etmek için yapılan Post-Hoc (Tukey) testi sonucu çizelge 4.17’ de sunulmuştur.

Çizelge 4.17. Sınıf değişkenine göre kişisel gizliliği koruma faktörü Tukey testi sonuçları

Sınıflar	N	$\bar{X}$	ss	Sınıf Değişkeni	Ortalama Farkı	Std. Hata	Sig.	Farkın Kaynağı	η^2
5. Sınıf	204	3,52	0,67	6. Sınıf	5. Sınıf	-,07859	,07867	0,75	6-8. Sınıf
6. Sınıf	89	3,44	0,59		7. Sınıf	-,14831	,09283	0,38	
7. Sınıf	89	3,59	0,63		8.Sınıf	-,22668*	,08306	0,03	
8.Sınıf	148	3,67	0,54						

Yapılan Post-Hoc (Tukey) testi sonucunda farkın 6'ıncı sınıf ile ($\bar{x}=3,44$) 8'inci sınıf ($\bar{x}=3,67$) arasında olduğu belirlenmiştir. Ortalamalar incelendiğinde bu farkın 6. sınıf öğrencilerinin kişisel gizliliği koruma farkındalıklarının ($\bar{x}=3,44$) olduğu, 8. Sınıf lehine olduğu gözlemlenmiştir. Test sonucu hesaplanan etki büyüklüğü ($\eta^2=0.01$) bu farkın düşük düzeyde olduğunu göstermektedir. Öğrencilerin kişisel gizliliği koruma farkındalıklarının ise ($\bar{x}=3,67$) olduğu belirlenmiştir.

4.3.3. İnternet ve bilişim teknolojileri kullanım sürelerine göre Anova testi sonuçları

Araştırmanın üçüncü alt problemi “Ortaokul öğrencilerinin siber güvenlik farkındalıkları toplam puan ve alt boyutlarda internet ve bilişim teknolojileri kullanma sürelerine göre farklılaşmakta mıdır?” olarak belirlenmiştir. Yapılan ANOVA testi sonucu çizelge 4.18.' de sunulmuştur.

Çizelge 4.18. İnternet ve bilişim teknolojileri kullanma sürelerine göre Anova testi sonuçları

Faktörler	Varyansın Kaynağı	Kareler Toplamı	sd	Kareler ortalaması	F	p
Şifre Güvenliği	Gruplar Arası	,424	3	,141	,443	0,72
	Grup İçi	167,938	526	,319		
	Toplam	168,363	529			
Önleyici Tedbirler	Gruplar Arası	,036	3	,012	,029	0,99
	Grup İçi	221,607	526	,421		
	Toplam	221,643	529			
Kötü Amaçlı Yazılım Farkındalığı	Gruplar Arası	,624	3	,208	,382	0,76
	Grup İçi	286,693	526	,545		
	Toplam	287,317	529			
Kişisel Gizliliği Koruma	Gruplar Arası	,733	3	,244	,629	0,59
	Grup İçi	204,356	526	,389		
	Toplam	205,090	529			
SGFÖ Toplam	Gruplar Arası	,274	3	,091	,367	0,77
	Grup İçi	130,941	526	,249		
	Toplam	131,215	529			

Analiz sonuçlarına göre SGFÖ ve alt boyutlarında internet ve bilişim teknolojileri kullanma sürelerine göre istatistiksel olarak anlamlı farklılık bulunmamaktadır ($p>,05$).

5. SONUÇ, TARTIŞMA VE ÖNERİLER

Sonuçlar ve tartışma bölümünde gerçekleştirilen araştırma neticesinde elde edilen bulgular ile ortaya çıkan sonuçlara yer verilmiş ve alan yazında yer alan benzer çalışmalarla karşılaştırılmıştır. Öneriler bölümünde ise uygulamacılara ve araştırmacılara önerilere yer verilmiştir.

5.1. Sonuç ve Tartışma

Teknoloji ve internetin gelişmesiyle birlikte bilişim teknolojileri kullanımında ciddi artış olmuş, bunula birlikte bilişim teknolojilerine erişim ve kullanım yaşı ise git gide azalmıştır. Bu durum kullanıcıları özellikle de bu sistemin en zayıf halkası olan çocukları tehlikelere açık hale getirmektedir. Bu tehlikelerden korunmalarının en temel yollarından biri siber güvenlik farkındalıklarının belirlenmesi ve artırılmasına yönelik çalışmalar yapılmasıdır. Bu kapsamda çocukların siber güvenlik farkındalıklarının belirlenmesine yönelik ölçme aracı geliştirilmesine ihtiyaç vardır. Bu ihtiyaç doğrultusunda çalışma iki amaç dikkate alınarak tasarlanmıştır. Çalışmanın ilk bölümünde ortaokul öğrencilerinin siber güvenlik farkındalık düzeylerinin ölçülebilmesi için geçerli, güvenilir ve dört alt boyuttan (Şifre Güvenliği, Önleyici Tedbirler, Kötü Amaçlı Yazılım Farkındalığı, Kişisel Gizliliği Koruma) oluşan bir ölçek geliştirilmiştir. İkinci bölümünde ise ortaokul öğrencilerinin siber güvenlik farkındalık düzeyleri farklı değişkenler açısından (sınıf, cinsiyet ve internet kullanımı) incelenmiştir.

Bulgular araştırma sorularına göre tartışılmıştır.

5.1.1. Birinci alt probleme ilişkin sonuçlar ve tartışma

Bu araştırmanın birinci alt problemi kapsamında ortaokul öğrencileri için geliştirilen SGFÖ' nün geçerli bir ölçek olup olmadığı araştırılmıştır. Geçerliklerin belirlenmesinde, kapsam geçerliği ve yapı geçerliği gibi geçerlik türleri kullanılabilir (Atılğan, Kan ve Doğan, 2013). Ölçeğin geçerlik özellikleri benzer ölçekler ile karşılaştırılmış ve SGFÖ' nün korelasyon katsayısının benzer ölçeklere ait korelasyonlara göre kabul edilebilir sınırlar içerisinde olduğu tespit edilmiştir. Ölçeğin yapı geçerliğinin belirlenmesi amacıyla AFA ve DFA yapılmıştır. Faktör analizi neticesinde ölçeğin birden çok boyutlu bir yapıya sahip

olduğu ve uyum değerlerinin de kabul edilebilir sınırların üzerinde olduğu görülerek ölçeğin geçerli olduğu belirlenmiştir.

Erol ve diğerleri (2015) tarafından geliştirilen kişisel siber güvenliği sağlama ölçeği ve Çetinkaya ve Öktelik (2022) tarafından hazırlanan bilgi güvenliği farkındalık ölçeğine yakın sonuçlar elde edildiği tespit edilmiştir.

Geliştirilen ölçeğin en önemli özelliği yüksek geçerlik oranı yanında belirli bir yaş grubuna göre hazırlanmış olmasıdır. Farkındalık ölçeği olması ve belirli bir yaş grubuna göre hazırlanmış olması siber güvenlik eğitimi üzerine ortaokul düzeyine yönelik planlama yapacak kişi ve kurumlara daha doğru ölçüm yapma imkânı sunacaktır. Alan yazında anket veya Erol ve diğerleri (2015) tarafından hazırlanan siber güvenlik ölçeği farklı gruplara uygulanmaktadır. Ancak yetişkinler, yüksek öğretim, ortaöğretim ve ortaokul öğrencileri gibi farklı yaş gruplarını aynı düzey sorular ile değerlendirmek ölçülmek istenen düzeyi yeterince açıklayamayacağı değerlendirilmektedir.

5.1.2. İkinci alt probleme ilişkin sonuçlar ve tartışma

Araştırmanın ikinci alt problemi için ortaokul öğrencileri için geliştirilen SGFÖ' nün güvenilir bir ölçek olup olmadığı incelenmiştir. Ölçeklerin güvenilirlik derecelerini test etmek için farklı yöntemler geliştirilmiştir. SGFÖ' nün güvenilirliğini ölçmek için iç tutarlık (Cronbach Alpha) güvenilirliği incelenmiştir.

Likert türü ölçeklerde Cronbach Alpha katsayısı güvenilirlik belirlemede en çok kullanılan güvenilirlik belirleme yöntemlerindendir. Ölçekte yer alan maddelerin arasındaki uyum Cronbach Alpha katsayısına göre belirlenmektedir (Seçer, 2015). Cronbach Alpha katsayısının; 0,40' ın altında olması ölçeğin güvenilir olmadığını, 0.40 – 0.60 arasında olması güvenilirliğinin düşük olduğunu; 0.60-0.80 arasında olması güvenilir olduğunu ve 0,80'in üzerinde olması da güvenilirliğinin yüksek olduğunu gösterir (Karagöz, 2019). Bu çalışmada hesaplanan toplam ölçek ve alt ölçek güvenilirlik değerlerinin “güvenilir” ve “güvenirliği yüksek” değerler aralığında olduğu görülmüştür.

Erol ve diğerleri (2015) tarafından geliştirilen kişisel siber güvenliği sağlama ölçeğinin geçerlilik katsayısı 0,735 olduğu belirtilmiştir. Makhabbat ve Gülseçen (2020) tarafından

ortaokul öğrencileri gerçekleştirilen çalışmada geçerlilik katsayısının 0,745'e yükseldiği belirtilmiştir. Anılan ölçeğin geliştirilmesi aşamasında kullanılan örneklemin güvenilirlik düzeyini düşürdüğü değerlendirilmektedir. Ortaokul öğrencilerine yönelik Çetinkaya ve Öktelik (2022) tarafından geliştirilen bilgi güvenliği farkındalığı ölçeği incelendiğinde geçerlik katsayısının 0,90 olduğu belirtilmiştir. Anılan çalışmanın örneklem büyüklüğünün AFA için 410, DFA için 265 olduğu belirtilmiştir. Araştırma kapsamında geliştirilen ölçeğin örneklem büyüklüğünün daha büyük olması ve iç tutarlık katsayısının geçerlik açısından tarafından geliştirilen ölçeğin yüksek güvenilirliğe sahip olması önemli bir etken olarak değerlendirilmektedir. Geliştirilen ölçeğin SGF düşük öğrenciler ile yüksek olan öğrencileri ayırt edebildiği görülmüştür.

5.1.3. Üçüncü alt probleme ilişkin sonuçlar ve tartışma

Araştırmada üçüncü olarak; Ortaokul öğrencilerinin siber güvenlik farkındalıkları toplam puan ve alt boyutlarda cinsiyet, sınıf düzeyi, internet ve bilişim teknolojileri kullanma süreleri açısından incelenmiştir.

Araştırma bulgularının ortaya koyduğu en genel sonuç 530 katılımcıdan oluşan öğrencilerin siber güvenlik farkındalık düzeylerinin Orta Düzeyde Yeterli olarak değerlendirilmesidir. Ölçeğin tamamı incelendiğinde en düşük farkındalık puanı değeri 61 ($\bar{x}=2,44$) puan olurken en yüksek 124 ($\bar{x}=4,96$) puan olduğu tespit edilmiştir. Makhabbat ve Gülseçen, (2020) tarafından gerçekleştirilen çalışmada katılımcıların toplam puan oranını 2,96 olarak belirtmişlerdir. Anılan çalışmada kullanılan veri toplama aracı Erol ve diğerleri (2015) tarafından geliştirilen Siber Güvenlik Ölçeği olup aradaki farkın kullanılan ölçeğin yaş grubuna uygun olmamasından kaynaklandığı düşünülmektedir. Çalışma grubunun alt boyutlara göre incelendiğinde en yüksek farkındalık düzeyinin “Önleyici Tedbirler” alt boyutunda olduğu tespit edilirken en düşük farkındalık düzeyinin “Kişisel Gizliliği Koruma” alt boyutunda olduğu tespit edilmiştir. “Kötü amaçlı Yazılım Farkındalığı” alt boyutunun ve “Şifre Güvenliği” alt boyutu farkındalık düzeylerinin ortalama olduğu tespit edilmiştir.

Araştırma kapsamında öğrencilerin “Şifre Güvenliği” alt boyutunda verdiği cevaplar incelendiğinde %65,5'i şifrelerinde özel karakterler, rakam ve harf kullanmaları gerektiğini bildikleri, %61,9'unun şifrelerini en az 8 karakter olarak belirledikleri, %67'sinin şifrelerini kimseyle paylaşmadıkları ve bu konularda yüksek farkındalık sergiledikleri tespit edilmiştir.

Katılımcıların sadece %18,3'ünün kişisel veriler içeren şifre oluşturmamaları gerektiğine tamamen katıldığı, işlem yapmamalarına rağmen e-postalarına gelen sıfırlama iletilerini yok saymaları gerektiğini düşünenlerin oranının %19,4' ve şifrelerini sıklıkla değiştirenlerin oranının %24' olduğu tespit edilmiştir. Sonuçlar, Aksoy ve Sayın (2018) tarafından gerçekleştirilen ortaokul öğrencilerinin şifre oluşturma bilincinin belirlenmesi çalışmasındaki sonuçlarla paralellik göstermektedir. Şifrelerin sıklıkla değiştirilmesi ve şifrelerin paylaşılmaması hususlarında yüksek farkındalık tespit edilirken şifre sıfırlama iletileri, şifre değiştirme sıklığı ve kişisel bilgiler içeren şifreler konusunda düşük farkındalık olduğu tespit edilmiştir. İki faktörlü kimlik doğrulamayı tam anlamıyla bildiklerini belirtenlerin oranının sadece %30,6' olduğu tespit edilmiştir.

Araştırmanın “Önleyici Tedbirler” alt boyutunda yüksek farkındalık gösterdiği tespit edilmiş en yüksek farkındalığın gelen e-postadaki samimi ifadeler “sevgili beyefendi/hanımefendi vb.” varsa dikkatli olmam gerektiğini bilirim maddesine verildiği tespit edilirken ($\bar{x}_9=4,37$), en düşük farkındalık bağlantı adresindeki “https://” ifadesinin kontrol edilip edilmediği ($\bar{x}_{13}=4,01$) maddesi olduğu belirlenmiştir. Bu sonuçlar doğrultusunda öğrencilerin e-posta kullanım oranlarının ve e-posta üzerinden gelebilecek tehditlere karşı farkındalık düzeylerinin daha yüksek olduğu tespit edilmiştir. Peker ve Akbaba (2016) öğrencilerin e-posta üzerinden sadece siber saldırıya maruz kalmadıkları siber zorbalığa da maruz kalabildiklerini belirtmiş ve bu yüksek farkındalığın bu etmenden de kaynaklanabileceği düşünülmektedir.

“Kötü Amaçlı Yazılım Farkındalığı” alt boyutunda katılımcıların ortalamasının $\bar{x}=3,90$ olduğu tespit edilmiştir. Alt boyutta bulunan maddelerden en düşük olan “Solucan ve Virüslerin Farkını Bilirim” maddesi ($\bar{x}_{16}=3,51$), en yüksek farkındalık gösterilen maddenin ise “Cihazlarımda Gerekli Yazılım Güncellemelerini Yaparım” ($\bar{x}_{15}=4,37$) olduğu belirlenmiştir. Günümüzde gerek işletim gerekse güvenlik yazılımlarının güncelleştirme işlemleri otomatik bir şekilde gerçekleştirilebilmektedir (Eriş ve Kaya, 2018). Bu özellikler sayesinde öğrencilerin yazılımlarını güncel tutmalarının önünün açıldığı değerlendirilmektedir. Ortaokul öğrencilerinin teknik bilgi eksikliklerinin yanı sıra risk değerlendirme yeteneklerinin gelişmemesinin madde 16'nın farkındalık düzeyinin diğer maddelere göre düşük çıkmasına sebep olabileceği düşünülmektedir (Özbay,2021).

“Kişisel Gizliliği Koruma” alt boyutunda madde 21-“Sosyal Medyada adıma hesap açılmasının kimlik hırsızlığı olduğunu bilirim” maddesinin en yüksek farkındalık olduğu ($\bar{x}_{21}=4,33$) tespit edilmiştir. En düşük farkındalık ters madde olarak belirlenen ve veri setine bu şekilde işlenen “Tanıdığım kişiden gelen e-postada kişisel bilgilerim istenirse paylaşırım” madde-22’de olduğu tespit edilmiştir ($\bar{x}_{22}=1,93$). Sonuç incelendiğinde öğrencilerin direkt kendilerine karşı olabilecek talepleri reddederken tanıdıkları hesaplar üzerinden kimlik avı saldırılarına karşı daha korumasız oldukları sonucuna ulaşılmıştır.

Ortaokul öğrencilerinin SGFÖ toplam puanları cinsiyete göre istatistiksel olarak incelendiğinde anlamlı farklılık olmadığı sonucuna ulaşılmıştır. Ölçeğe ait alt faktörlerden “Önleyici tedbirler” alt boyutunda erkek öğrenciler lehine anlamlı farklılık bulunduğu saptanmıştır. Alanyazında ortaokul öğrencilerinin SGF cinsiyet değişkenine göre farklılaşma durumuna ilişkin birbiriyle örtüşen ve çelişen bulgular mevcuttur. Beder (2015), beşinci ila sekizinci sınıf öğrencilerinin güvenli İnternet kullanımı konusundaki farkındalık düzeylerini incelediği çalışmasında kız öğrencilerin erkek öğrencilere göre interneti daha dikkatli kullandıkları sonucuna ulaşmıştır. Derin ve Gençoğlu (2020), ortaokul öğrencileri üzerinde yaptıkları bilgi güvenliği farkındalığı çalışmasında ortalaması yüksek olan kız öğrencilerin erkek öğrencilere oranla bilgi güvenliği farkındalık seviyesinin yüksek olduğunu tespit etmişlerdir. Makhabbat ve Gülseçen, (2022) Ortaokul Öğrencilerinin Siber Güvenlik Durumları çalışmalarında cinsiyet değişkenine göre erkek öğrencilerin farkındalıklarının yüksek olduğu sonucuna ulaşmışlardır. Çetinkaya ve Ökdelik (2022) tarafından geliştirilen “Ortaokul Düzeyi Öğrencilerine Yönelik Bilgi Güvenliği Farkındalık Ölçeği Geliştirme” çalışmasında bilgi güvenliği farkındalığı kapsamında kız öğrenciler lehine anlamlı farklılık bulunduğunu belirtmiştir.

Sınıf değişkenine göre ortaokul öğrencilerinin SGF düzeyleri arasında anlamlı bir farklılık olduğu ve yapılan Tukey testi ile bu farkın 8’inci sınıflar ile 6’ncı sınıflar arasında ve 8’inci sınıflar lehine olduğu tespit edilmiştir. Alanyazında ortaokul öğrencilerinin SGF sınıf değişkenine göre farklılaşma durumuna ilişkin farklı bulgular mevcuttur. Makhabbat ve Gülseçen, (2022) ortaokul öğrencilerinin sınıflara göre siber güvenlik farkındalık durumunun önemli bir etken olmadığı ve fark bulunmadığı belirtilmiştir. Derin ve Gençoğlu (2020), 8’inci sınıfların bilgi güvenliği bakımında daha düşük sınıf düzeylerine göre pozitif farkındalıkları olduğunu belirtmiştir. Derin ve Gençoğlu (2020) sınıf düzeyine göre gruplandıkları 7 ve 8’inci sınıfların 5 ve 6’ncı sınıf düzeyindeki öğrencilere göre bilgi

güvenliği farkındalıklarının yüksek olduğunu belirtmiştir. Talan ve Aktürk (2021) ortaöğretim öğrencilerinin bilgi güvenliği farkındalığı seviyelerinin incelenmesi çalışmasında sınıf seviyelerine göre bilgi güvenliği farkındalıklarında anlamlı bir fark olmadığını belirtmişlerdir.

İnternet kullanım sürelerine göre ortaokul öğrencilerinin SGF düzeyleri arasında anlamlı bir farklılık olmadığı sonucuna ulaşılmıştır. Alanyazında ortaokul öğrencilerinin SGF günlük internet kullanım zamanlarına göre farklılaşma durumuna ilişkin farklı bulgular mevcuttur. Makhabbat ve Gülseçen, (2022) ve Gençoğlu (2020), internet kullanım sürelerinde fazla süre kullanan öğrencilerin diğer gruplara göre SGF farkındalıklarının ve tehditleri elemine etme hususunda daha başarılı olduklarını belirtmişlerdir. Öğrencilerin günlük internet kullanım süreleri incelendiğinde %30'unun 1 saatten az, %50,9'unun 1-3 saat arası, %13' ünün 3-5 saat arası ve %5,3'ünün 5 saatten fazla internet kullanıldığı tespit edilmiştir. Talan ve Aktürk (2021) günlük internet kullanım saatinin 7 saat ve üstüne çıktığında bilgi güvenliği farkındalığının anlamlı bir farkla yüksek olduğunu belirtmiştir. Ortaokul öğrencilerinin yaş grubu (11-14 arası) günlük internet kullanım saatlerinin 7 saati bulmasının mümkün olmadığı düşünülmektedir.

Bu araştırma; eğitim, sağlık ve iletişim başta olmak üzere hayatın her alanında kullanılan teknolojinin, ortaokul öğrencilerinin tehlikeler karşısında ne kadar bilinçli olduklarını tespit etmeyi amaçlamıştır. Çıkan sonuçlar incelendiğinde özellikle pandemi öncesi yapılan çalışmalarda ortaya çıkan yetersiz farkındalık oranlarının pandemi sonrası hızlı bir yükselişe geçtiğini, teknolojiye ve internete erişimin kolaylaşmasının tehlikeleri artırdığını ortaya koymaktadır.

Öğrencilerin, SGF belirlemek için yapılan ankette öğrencilerin büyük bir çoğunluğunun bilişim teknolojilerine erişimi olduğu ve interneti etkin bir şekilde kullandığı görülmektedir. Araştırma sonuçları, öğrencilerin internette rahatsız edici içeriklerle karşılaştığı ve bu durumda ne yapması gerektiğine dair fikir sahibi olduklarını ortaya çıkarmıştır. Yaşları bakımından siber saldırıya uğrama oranları düşük olsa bile yakın çevrelerinde yaşanan yoğun siber saldırılar hakkında fikir sahibi oldukları ve gelecekte saldırganların potansiyel hedefi haline gelecek öğrencilerin farkındalıklarının sürekli artırılması gerekliliği ortadadır.

5.2. Öneriler

Bu bölümde uygulamaya yönelik öneriler ile araştırmaya yönelik önerilerden bahsedilmiş olup, gelecek araştırmalara yönelik fikirler paylaşılmıştır.

5.2.1. Uygulamaya yönelik öneriler

İlk defa geliştirilen ölçeğin yapısının gelişebilmesi için farklı çalışmalarda kullanılması önemlidir. Geliştirilen ölçeğin kullanıldığı geniş kapsamlı taramalar ya da boylamsal çalışmaların yapılabilir.

Bu çalışma Amasya ilindeki ortaokul öğrencilerine yönelik yapılmıştır. Çalışma sonucunda öğrencileri cinsiyet, sınıf düzeyi, internet ve bilişim teknolojileri kullanma süreleri değişkenlerine göre incelenmiştir. Farklı iller ve bölgelerdeki öğrencilerin yanı sıra farklı ortaokul türleri (imam hatip ortaokulları, yatılı bölge ortaokulları, özel öğretim ortaokulları) ile aynı çalışma tekrarlanabilir ya da SGFÖ ile farklı değişkenler arasındaki ilişkiler incelenebilir. Farklı özellikteki çocuklarla (özellikle sosyal dezavantajlı) karşılaştırmalı çalışmalar yapılabilir.

5.2.2. Araştırmaya yönelik öneriler

Öğrencilerin SGF farkındalıklarının artırılması için SG konusu ortaokul Bilişim Teknolojileri ve Yazılım dersi müfredatında ders sayısı bakımından daha uzun süre yer alması sağlanabilir.

Ulusal siber güvenlik farkındalığı artırma çalışmaları kapsamında okullarda uygulanan Siberay faaliyetlerinin ortaokul öğrencileri düzeyinde verimliliğinin ölçülmesi amacıyla araştırma yapılabilir

KAYNAKLAR

- Ab Hamid, R. S., Yunus, Z. and Ahmad, M. (2018). *Cyber Parenting Module Development for Parents*. 12th International Technology, Education and Development Conference, Valencia, Spain.
- Abd Rahim, N. H., Hamid, S., Kiah, M. L. M., Shamshirband, S. and Furnell, S. (2015). A Systematic Review of Approaches to Assessing Cybersecurity Awareness. *Kybernetes*, 44(4), 606-622.
- Ahmad, N., Asma'Mokhtar, U., Fauzi, W. F. P., Othman, Z. A., Yeop, Y. H. and Abdullah, S. N. H. S. (2018). *Cyber Security Situational Awareness Among Parents*. Cyber Resilience Conference, Putrajaya, Malaysia.
- Al Hayani, B. and Ilhan, H. (2020). Image Transmission Over Decode and Forward Based Cooperative Wireless Multimedia Sensor Networks for Rayleigh Fading Channels in Medical Internet of Things (MIoT) for Remote Health-Care and Health Communication Monitoring. *Journal of Medical Imaging And Health Informatics*, 10(1), 160-168.
- Al Shamsi, A. A. (2019). Effectiveness of Cyber Security Awareness Program for Young Children: A Case Study in UAE. *International Journal of Information Technology and Language Studies*, 3(2), 8-29.
- Al-Ghamdi, M. I. (2021). Effects of Knowledge of Cyber Security on Prevention of Attacks. *Materials Today: Proceedings*, 10.
- Alghamdie, M. I. (In press). Withdrawn: A Novel Study Of Preventing The Cyber Security Threats. *Materials Today: Proceedings*.
- Alhayani, B., Abbas, S. T., Khutar, D. Z. and Mohammed, H. J. (In press). Best Ways Computation Intelligent of Face Cyber Attacks. *Materials Today: Proceedings*.
- Alotaibi, F., Furnell, S., Stengel, I. and Papadaki, M. (2016). A Review of Using Gaming Technology for Cyber-Security Awareness. *International Journal for Information Security Research*, 6(2), 660-666.
- Alpar, R. (2012). *Spor Sağlık ve Eğitim Bilimlerinden Örneklerle Uygulamalı İstatistik ve Geçerlik Güvenirlik* (İkinci baskı). Ankara: Detay Yayıncılık, 420-440.
- Alqarni, A. (2017). *Exploring Factors That Affect Adoption of Computer Security Practices Among College Students*. Unpublished Doctorate Thesis, Eastern Michigan University, USA.
- Altunışık, R., Coşkun, R., Bayraktaroğlu, S. ve Yıldırım, E. (2005). *Sosyal Bilimlerde Araştırma Yöntemleri SPSS Uygulamalı* (Dördüncü baskı). Sakarya: Sakarya Kitabevi, 139-159.
- Alzubaidi, A. (2021). Measuring the Level of Cyber-security Awareness for Cybercrime in Saudi Arabia. *Heliyon*, 7(1), e06016.

- Amoroso, E. (2006). *Cyber Security* (First edition). New Jersey: Silicon Press, USA, 78-98.
- Andress, J. (2014). *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice* (Second edition). Oxford: Syngress, United Kingdom, 220-249.
- Aslay, F., Handan, Ç. ve Üstün, Ö. (2019). Yükseköğretim Kurumlarında Bilgi Güvenliği Farkındalık Düzeylerinin Ölçümlemesi. *Yönetim Bilişim Sistemleri Dergisi*, 5(2), 1-11.
- Aydeger, A., Saputro, N. and Akkaya, K. (2019). A Moving Target Defense and Network Forensics Framework for ISP Networks Using SDN and NFV. *Future Generation Computer Systems*, 94, 496-509.
- Aziz, A. A. and Amtul, Z. (2019). Developing Trojan Horses to Induce, Diagnose and Suppress Alzheimer's Pathology. *Pharmacological Research*, 149, 104471.
- Bandalos, D. L., Finney, S. J., Hancock, G. R. and Mueller, R. O. (2010). *The Reviewer's Guide to Quantitative Methods in the Social Sciences* (First edition). New York: Routledge, USA, 225-247.
- Baumann, K. A. (2016). *Computer security in elementary schools: Faculty perception of curriculum adequacy*. Unpublished Doctorate Thesis, Northcentral University, USA.
- Bentley, H., Fellowes, A., Glenister, S., Mussen, N., Ruschen, H., Slater, B. and Wilson, P. (2020). How Safe are Our Children?: An Overview of Data on Adolescent Abuse, *NSPCC Report*, London, 1-66.
- Blanke, S., Nielsen, P. C. and Wrozek, B. (2022). How Can A Cybersecurity Student Become A Cybersecurity Professional and Succeed in A Cybersecurity Career? *Research Anthology on Advancements in Cybersecurity Education*, 19, 74-92.
- Boyd, D. and Hargittai, E. (2013). Connected and Concerned: Variation in Parents' Online Safety Concerns. *Policy & Internet*, 5(3), 245-269.
- Büyüköztürk, Ş. (2012). *Veri Analizi El Kitabı* (Onaltıncı baskı). Ankara: Pegem Akademi, 250-277.
- Büyüköztürk, Ş., Kılıç Çakmak, E. E., Akgün, Ö. E., Karadeniz, Ş. ve Demirel, F. (2009). *Bilimsel Araştırma Yöntemleri* (Dördüncü baskı). Ankara: Pegem Akademi, 127-147.
- Byrne, S., Katz, S. J., Lee, T., Linz, D. and McIlrath, M. (2014). Peers, Predators, and Porn: Predicting Parental Underestimation of Children's Risky Online Experiences. *Journal of Computer-Mediated Communication*, 19(2), 215-231.
- Byron, T. (2008). Safer Children in A Digital World: The Report of the Byron Review : Be safe, Be Aware, Have Fun. Department for Children, Schools and Families. *Dera Report*, London, 1-224.
- Camp, L. J. (1999). Web Security and Privacy: An American Perspective. *The Information Society*, 15(4), 249-256.

- Canbek, G. ve Sağıroğlu, Ş. (2006). Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme. *Politeknik Dergisi*, 9(3), 165-174.
- Choong, Y. Y., Theofanos, M. F., Renaud, K. and Prior, S. (2019). Passwords Protect My Stuff A Study Of Children's Password Practices. *Journal of Cybersecurity*, 5(1), tyz015.
- Clements, J., Yang, Y., Sharma, A. A., Hu, H. and Lao, Y. (2021). *Rallying Adversarial Techniques Against Deep Learning for Network Security*. IEEE Symposium Series on Computational Intelligence, Orlando, Florida, USA.
- Clemmer, L. (2010). Information Security Concepts: Confidentiality, Integrity, Availability, and Authenticity. *Computer Science*, 1-94.
- Clemons, E. K. and Wilson, J. S. (2015). Family Preferences Concerning Online Privacy, Data Mining, and Targeted Ads: Regulatory Implications. *Journal of Management Information Systems*, 32(2), 40-70.
- Cooke, A. (2020). A Unique Year for Cyber Security. *Network Security*, 9, 20-21.
- Craigien, D., Diakun-Thibault, N. and Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, 4(10), 13-21.
- Creswell, J. W. (2017). *Eğitim Araştırmaları: Nicel ve Nitel Araştırmanın Planlanması, Yürütülmesi ve Değerlendirilmesi* (Birinci baskı) Türkiye: Edam Yayıncılık, 1-880.
- Cronbach, L. J. (1984). A Research Worker's Treasure Chest. *Multivariate Behavioral Research*, 19(2-3), 223-240.
- Cukier, K. Data, Data Everywhere (2010). *The Economist*, 85-86.
- Çapa, Y., Çakıroğlu, J. ve Sarıkaya, H. (2005). Öğretmen Özyeterlik Ölçeği Türkçe Uyarlamasının Geçerlik ve Güvenirlik Çalışması. *Eğitim ve Bilim*, 30(137), 1300-1337.
- Çetinkaya, L., Güldüren, C. ve Keser, H. (2017). Öğretmenler İçin Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) Geliştirme Çalışması. *Milli Eğitim Dergisi*, 46(216), 33-52.
- Çokluk, Ö., Şekercioğlu, G. ve Büyüköztürk, Ş. (2012). *Sosyal Bilimler İçin Çok Değişkenli İstatistik: SPSS ve LISREL Uygulamaları* (Altıncı baskı). Ankara:Pegem Akademi 165-186.
- Da Veiga, A. (2016). Comparing the Information Security Culture of Employees Who Had Read The Information Security Policy and Those Who Had Not: Illustrated Through An Empirical Study. *Information & Computer Security*, 24(2), 139-151.
- Das Purba, M., Chu, B. and Al-Shaer, E. (2020). *From Word Embedding to Cyber-Phrase Embedding: Comparison of Processing Cybersecurity Texts*. IEEE International Conference on Intelligence and Security, Arlington, VA, USA.

- Dempsey, J., Sim, G. ve Cassidy, B. (2018). *Designing for GDPR-Investigating Children's Understanding of Privacy: A survey approach*. Human Computer Interaction Conference, Belfast, United Kingdom.
- Dempsey, J., Sim, G., Cassidy, B. and Ta, V. T. (2022). Children Designing Privacy Warnings: Informing A Set of Design Guidelines. *International Journal of Child-Computer Interaction*, 31, 100446.
- Donoso, V., Verdoodt, V., Van Mechelen, M. and Jasmontaite, L. (2016). Faraway, So Close: Why the Digital Industry Needs Scholars and the Other Way Around. *Journal of Children and Media*, 10(2), 200-207.
- Egelman, S. and Peer, E. (2015). *Scaling the Security Wall: Developing a Security Behavior Intentions Scale (sebis)*. 33rd Annual Acm Conference on Human Factors In Computing, Seoul, Republic of Korea.
- Ercan, I. ve Kan, I. (2004). Reliability and Validity in the Scales. *Uludağ Üniversitesi Tıp Fakültesi Dergisi*, 30(3), 211-216.
- Erol, O., Şahin, Y. L., Yılmaz, E. and Haseski, H. İ. (2015). Personal Cyber Security Provision Scale Development Study. *International Journal of Human Sciences*, 12(2), 75-91.
- Fielding, J. (2020). The People Problem: How Cyber Security's Weakest Link Can Become A Formidable Asset. *Computer Fraud & Security*, 1, 6-9.
- Fratantonio, Y., Bianchi, A., Robertson, W., Kirda, E., Kruegel, C. and Vigna, G. (2016). *TriggerScope: Towards Detecting Logic Bombs in Android Applications*. IEEE Symposium on Security and Privacy, San Jose, USA.
- Gay, L. R., Mills, G. E. and Airasian, P. (1987). *Educational Research Competencies for Analysis and application* (Third edition). London: Merrill Publishing Company, 183-203.
- Giannakas, F., Papasalouros, A., Kambourakis, G. and Gritzalis, S. (2019). A Comprehensive Cybersecurity Learning Platform for Elementary Education. *Information Security Journal: A Global Perspective*, 28(3), 81-106.
- Giannakas, F., Papasalouros, A., Kambourakis, G. and Gritzalis, S. (2019). A Comprehensive Cybersecurity Learning Platform for Elementary Education. *Information Security Journal: A Global Perspective*, 28(3), 81-106.
- Gibson, W. (2017). *Burning Chrome* (First edition). Hachette: United Kingdom, 85-96.
- Gökçearslan, Ş., Günbatar, M. S. ve Sarıtepeci, M. (2021). Ortaöğretim Öğrencilerinin Bilgi Güvenliği Farkındalıklarının İncelenmesi. *Van Yüzüncü Yıl Üniversitesi Eğitim Fakültesi Dergisi*, 18(1), 354-373.
- Grabosky, P. (2016). *The Evolution of Cybercrime* (First edition). New York: Routledge, 15-36.

- Gratian, M., Bandi, S., Cukier, M., Dykstra, J. and Ginther, A. (2018). Correlating Human Traits and Cyber Security Behavior Intentions. *Computers & Security*, 73, 345-358.
- Güçlü, İ. (2019). *Sosyal Bilimlerde Nitel Araştırma Yöntemleri* (İkinci baskı). Ankara: Nika Yayıncılık, 278-299.
- Güldüren, C., Çetinkaya, L. ve Keser, H. (2016). Ortaöğretim Öğrencilerine Yönelik Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) Geliştirme Çalışması. *İlköğretim Online*, 15(2), 682-695.
- Hacımustafaoğlu, R. (2019). *Ortaöğretim Öğrencilerinin Bilgi Güvenliği Farkındalık Düzeylerinin Siber Mağdur Olma Durumlarına Etkisinin İncelenmesi (Üsküdar Örneği)*, Yayınlanmamış Doktora Tezi, Sakarya Üniversitesi Fen Bilimleri Enstitüsü, Sakarya.
- Halevi, T., Lewis, J. and Memon, N. (2013). *A Pilot Study of Cyber Security and Privacy Related Behavior and Personality Traits*. 22nd International World Wide Web, Rio de Janeiro, Brazil.
- Hamdan, Z., Obaid, I., Ali, A., Hussain, H., Rajan, A. V. and Ahamed, J. (2013). *Protecting Teenagers From Potential Internet Security Threats*. International Conference on Current Trends in Information Technology, Dubai, United Arab Emirates.
- Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W. and Spiegel, J. (2012). The Law of Cyber-Attack. *California Law Review*, 100(4), 817-885.
- Hayton, J. C., Allen, D. G. and Scarpello, V. (2004). Factor Retention Decisions in Exploratory Factor Analysis: A Tutorial on Parallel Analysis. *Organizational Research Methods*, 7(2), 191-205.
- Hershberger, S. L. (2003). The Growth of Structural Equation Modeling: 1994-2001. *Structural Equation Modeling*, 10(1), 35-46.
- Holloway, D., Green, L. and Livingstone, S. (2013). Zero to Eight: Young Children and Their Internet Use. *EU Kids Online*, 1-35.
- Hourcade, J. P. (2008). Interaction Design and Children. *Foundations and Trends in Human-Computer Interaction*, 1(4), 277-392.
- Hyla, T. and Fabisiak, L. (2020). *Measuring Cyber Security Awareness Within Groups of Medical Professionals in Poland*. Hawaii International Conference on System Sciences, Hawaii, USA.
- International Telecommunication Union (2021). Committed to Connecting the World: Cybersecurity. *ITU Report*, Dubai, 1-40.
- Ioannou, M., Stavrou, E. and Bada, M. (2019). *Cybersecurity Culture in Computer Security Incident Response Teams: Investigating difficulties in Communication and Coordination*. International Conference on Cyber Security and Protection of Digital Services, Oxford, United Kingdom.

- Karakuş, T., Çağıltay, K., Kaşıkçı, D., Kurşun, E. ve Ogan, C. (2014). Türkiye ve Avrupa'daki Çocukların İnternet Alışkanlıkları ve Güvenli İnternet Kullanımı. *Eğitim ve Bilim*, 39 (171), 1300-1337.
- Karasar, N. (2006). *Bilimsel araştırma yöntemleri* (İkinci baskı). Ankara: Nobel Yayıncılık, 175-198.
- Kaur, J. and Ramkumar, K. R. (2022). The Recent Trends in Cyber Security: A review. *Journal of King Saud University-Computer and Information Sciences*, 34(8), 5766-5781.
- Keser, H. ve Güldüren, C. (2015). Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) Geliştirme. *Kastamonu Eğitim Dergisi*, 23(3), 1167-1184.
- Kharlamova, N., Hashemi, S. and Træholt, C. (2021). Data-driven Approaches for Cyber Defense of Battery Energy Storage Systems. *Energy and AI*, 5, 100095.
- Kianpour, M., Kowalski, S. J. and Øverby, H. (2022). Advancing the Concept of Cybersecurity as a Public Good. *Simulation Modelling Practice and Theory*, 116, 102493.
- Kristjánsson, H., Gardner, R. and Chiribella, G. (2021). Quantum Communications Report for Ofcom, *Ofcom Report*, 20-52.
- Kritzinger, E., Bada, M. and Nurse, J. R. (2017). *A Study Into the Cybersecurity Awareness Initiatives for School Learners in South Africa and the UK*. Information Security Education for a Global Digital Society, Rome, Italy
- Lewallen, J. (2021). Emerging Technologies and Problem Definition Uncertainty: The Case of Cybersecurity. *Regulation & Governance*, 15(4), 1035-1052.
- Lewis, J. A. (2006). Cybersecurity and Critical Infrastructure Protection. *Center for Strategic and International Studies*, 9, 1-12.
- Liao, Y. F. (2004). Issues of Validity and Reliability in Second Language Performance Assessment. *Studies in Applied Linguistics and Tesol*, 4(2), 1-4.
- Liu, Y., Peng, W. and Su, J. (2014). A study of IP Prefix Hijacking in Cloud Computing Networks. *Security and Communication Networks*, 7(11), 2201-2210.
- Livingstone, S., Mascheroni, G. and Staksrud, E. (2015). Developing a framework for researching children's online risks and opportunities in Europe. *EU Kids Online*, 1-21.
- Livingstone, S., Stoilova, M. and Nandagiri, R. (2019). Children's data and privacy online: Growing up in a digital age: an evidence review. *Media and Communications*, 1-57.
- Lobe, B., Velicu, A., Staksrud, E., Chaudron, S. and Rosanna, D. G. (2021). How children (10-18) experienced online risks during the Covid-19 lockdown-Spring 2020 *Publications Office of the European Union*, 1-50.

- Lu, S., Phung, B. T. and Zhang, D. (2018). A Comprehensive Review on Dc Arc Faults and Their Diagnosis Methods in Photovoltaic Systems. *Renewable and Sustainable Energy Reviews*, 89, 88-98.
- Madeti, S. R. and Singh, S. N. (2017). A Comprehensive Study on Different Types of Faults and Detection Techniques for Solar Photovoltaic System. *Solar Energy*, 158, 161-185.
- MadhuSudanan, V. and Geetha, R. (2020). Dynamics of Epidemic Computer Virus Spreading Model with Delays. *Wireless Personal Communications*, 115(3), 2047-2061.
- Magkos, E., Kleisiari, E., Chanas, P. and Giannakouris-Salalidis, V. (2014). *Parental Control and Children's Internet Safety: The Good, The Bad and The Ugly*. Proc. International Conference on Information Law and Ethics, Thessaloniki, Greece.
- Makhabbat, A. ve Gülseçen, S. (2020). Ortaokul Öğrencilerinin Siber Güvenlik Farkındalık Durumu. *Edebiyat, Dil ve Eğitim*, 213, 1-12.
- Mayer, M., Martino, L., Mazurier, P. and Tzvetkova, G. (2014). How Would You Define Cyberspace. *First Draft Pisa*, 19, 1-3.
- McReynolds, E., Hubbard, S., Lau, T., Saraf, A., Cakmak, M. and Roesner, F. (2017). *Toys That Listen: A Study of Parents, Children, and Internet-Connected Toys*. Conference on Human Factors in Computing Systems, NY, USA.
- Mihçı Türker, P. and Kılıç Çakmak, E. (2019). An Investigation of Cyber Wellness Awareness: Turkey Secondary School Students, Teachers, and Parents. *Computers In The Schools*, 36(4), 293-318.
- Mohammad, R. M., Thabtah, F. and McCluskey, L. (2015). Tutorial and Critical Analysis of Phishing Websites Methods. *Computer Science Review*, 17, 1-24.
- Mohsin, A. H., Zaidan, A. A., Zaidan, B. B., Albahri, O. S., Albahri, A. S., Alsalem, M. A. and Mohammed, K. I. (2019). Based Medical Systems for Patient's Authentication: Towards A New Verification Secure Framework Using CIA Standard. *Journal of Medical Systems*, 43, 1-34.
- Moore, D., Paxson, V., Savage, S., Shannon, C., Staniford, S. and Weaver, N. (2003). Inside the Slammer Worm. *IEEE Security & Privacy*, 1(4), 33-39.
- National Cyber Security Index (2023). NCSI Ranking, *NCSI Report*, Estonia, 10111.
- Neuman, W. L. and Robson, K. (2014). *Basics of Social Research* (Second edition). Toronto: Pearson Publisher, 296-310.
- Nielsen, S. C. (2012). Pursuing Security in Cyberspace: Strategic and Organizational Challenges. *Orbis*, 56(3), 336-356.
- Ning, H., Ye, X., Bouras, M. A., Wei, D. and Daneshmand, M. (2018). General Cyberspace: Cyberspace and Cyber-Enabled Spaces. *IEEE Internet of Things Journal*, 5(3), 1843-1856.

- Ofcom, (2016). Children and Parents: Media Use and Attitudes Report. *Ofcom*, Office of Communications London, 1-233.
- Ottis, R. and Lorents, P. (2010). *Cyberspace: Definition and Implications*. International Conference on Information Warfare and Security, Reading, United Kingdom.
- Owens, K., Fulton, A., Jones, L. and Carlisle, M. (2019). How to avoid scaring students away in a ctf competition. *Journal of The Colloquium for Information System Security Education*, 1-6.
- Öğütçü, G., Testik, Ö. M. ve Chouseinoglou, O. (2016). Analysis of Personal Information Security Behavior and Awareness. *Computers & Security*, 56, 83-93.
- Önaçan, M. B. K. ve Hasan, A. (2016). Siber Güvenlikte Lisansüstü Eğitim: Deniz Harp Okulu Örneği. *Trakya Üniversitesi Mühendislik Bilimleri Dergisi*, 17(1), 13-21.
- Panimalar, A., Pai, G. and Khan, S. (2018). Artificial Intelligence Techniques for Cyber Security. *International Research Journal of Engineering and Technology*, 5(3), 122-124.
- Papakonstantinou, V. (2022). Cybersecurity as Praxis and as A State: The EU Law Path Towards Acknowledgement of A New Right to Cybersecurity?. *Computer Law & Security Review*, 44, 105653.
- Parker, D. (2010). Our Excessively Simplistic Information Security Model and How to Fix It. *ISSA Journal*, 8(7), 12-21.
- Patterson, A., Ryckman, L. and Guerra, C. (2022). A Systematic Review of the Education and Awareness Interventions to Prevent Online Child Sexual Abuse. *Journal of Child & Adolescent Trauma*, 15(3), 857-867.
- Pattinson, M. R. (2012). *An Examination of Information System Risk Perceptions Using The Repertory Grid Technique*. Unpublished Phd Thesis, University of Adelaide, Australia.
- Patton, M. Q. (2002). Two Decades of Developments in Qualitative Inquiry: A Personal, Experiential Perspective. *Qualitative Social Work*, 1(3), 261-283.
- Pender-Bey, G. (2016). *The parkerian hexad: The CIA Expanded (First edition)*. Illinois: Lewis University Press, 1-31.
- Polanin, J. R., Espelage, D. L., Grotz, J. K., Spinney, E., Ingram, K. M., Valido, A. and Robinson, L. (2021). A Meta-Analysis of Longitudinal Partial Correlations Between School Violence and Mental Health, School Performance, and Criminal Or Delinquent Acts. *Psychological Bulletin*, 147, 115-133.
- Quayyum, F., Cruzes, D. S. and Jaccheri, L. (2021). Cybersecurity Awareness for Children: A Systematic Literature Review. *International Journal of Child-Computer Interaction*, 30, 100343.

- Rahim, N. H. A., Hamid, S., Mat Kiah, M. L., Shamshirband, S. and Furnell, S. (2015). A Systematic Review of Approaches to Assessing Cybersecurity Awareness. *Kybernetes*, 44(4), 606-622.
- Raja, M. A. Z., Mehmood, A., Ashraf, S., Awan, K. M. and Shi, P. (2022). Design of Evolutionary Finite Difference Solver for Numerical Treatment of Computer Virus Propagation with Countermeasures Model. *Mathematics and Computers in Simulation*, 193, 409-430.
- Roscini, M. and Trust, L. (2014). *Cyber Operations and the Use of Force in International Law* (First edition). New York: Oxford University Press, 284-290.
- Schumacker, R. E. and Lomax, R. G. (2004). *A Beginner's Guide to Structural Equation Modeling (Second edition)*. New York: Psychology Press, 185-194.
- Scott, S. G. and Bruce, R. A. (1995). Decision-making Style: The Development and Assessment of A New Measure. *Educational and Psychological Measurement*, 55(5), 818-831.
- Selwyn, N. (2015). Data Entry: Towards the Critical Study of Digital Data and Education. *Learning, Media and Technology*, 40(1), 64-82.
- Sharma, S. (1996). *Applied Multivariate Techniques* (First edition). New York: John Wiley&Sons. Inc, 144-156.
- Shaw, R. S., Chen, C. C., Harris, A. L. and Huang, H. J. (2009). The Impact of Information Richness on Information Security Awareness Training Effectiveness. *Computers & Education*, 52(1), 92-100.
- Shin, W. and Kang, H. (2016). Adolescents' Privacy Concerns and Information Disclosure Online: the Role of Parents and the Internet. *Computers in Human Behavior*, 54, 114-123.
- Shoufan, A. and Damiani, E. (2017). On Inter-Rater Reliability of Information Security Experts. *Journal of Information Security and Applications*, 37, 101-111.
- Siddiqui, Z. and Zeeshan, N. (2020). A Survey on Cybersecurity Challenges And Awareness For Children of All Ages. 2020 International Conference on Computing, Electronics & Communications Engineering, Southend, UK.
- Singer, P. W. ve Friedman, A. (2014). *Cybersecurity: What Everyone Needs to Know* (Second edition). New York: Oxford University Press, 96-99.
- Slavtcheva-Petkova, V., Nash, V. J. and Bulger, M. (2015). Evidence on the Extent of Harms Experienced by Children as a Result of Online Risks: Implications for Policy and Research. *Information, Communication & Society*, 18(1), 48-62.
- Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K. and Hasebrink, U. (2020). Survey Results From 19 Countries. *EU Kids Online*, 1-156.
- Snyman, D. P., Drevin, G. R., Kruger, H. A., Drevin, L. and Allers, J. (2021). *A Wolf, Hyena, and Fox Game to Raise Cybersecurity Awareness Among Pre-School Children*.

- International Symposium on Human Aspects of Information Security and Assurance, Lesbos, Greece.
- Staff, U. A. F. J. (2010). Joint Terminology for Cyberspace Operations. *Département de la Défense Etats-Unis*, 1-16.
- Staksrud, E., Livingstone, S. and Haddon, L. (2007). What Do We Know About Children's Use Of Online Technologies?: A Report on Data Availability and Research Gaps in Europe. *EU Kids Online*, 1-49.
- Steichen, P. (2012). Principles and Fundamentals of Security Methodologies of Information Systems-Introduction (First edition). Metz: M2SSIC Publishing, 78-84.
- Stewart, H. and Jurjens, J. (2017). Information Security Management and the Human Aspect in Organizations. *Information & Computer Security*, 25(5), 494-534.
- Şencan, H. (2005). *Güvenilirlik ve Geçerlilik*. (Birinci baskı). Ankara: Seçkin Yayıncılık, 460-472.
- Tabachnick, B. G. and Fidell, L. S. (2013). *Using Multivariate Statistics*. (Sixth edition). Northridge: Pearson Education. 344-375
- Tanrıöğen, A. (2012). *Bilimsel Araştırma Yöntemleri* (Birinci baskı). Ankara: Anı Yayıncılık.
- Tavlaş, H. (2019). *Ortaöğretim Kurumlarında Uygulanan Uygulanan Siber Güvenlik Farkındalık Eğitiminin Öğrenciler Üzerindeki Etkisi*. Yayımlanmamış Yüksek Lisans Tezi, İstanbul Şehir Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.
- Tavsancil, E. (2006). *Tutumların Ölçülmesi ve Spss ile Veri Analizi* (Altıncı baskı). Ankara: Nobel Yayıncılık, 78-94.
- Tavşancil, E. and Keser, H. (2002). Development of a Likert Type Attitude Scale towards Internet Usage. *Journal of Educational Sciences & Practices*, 1, 1.
- Teimouri, M., Benrazavi, S. R., Griffiths, M. D. and Hassan, M. S. (2018). A Model of Online Protection to Reduce Children's Online Risk Exposure: Empirical Evidence from Asia. *Sexuality & Culture*, 22, 1205-1229.
- Tekerek, M. ve Tekerek, A. (2013). Öğrencilerin Bilgi Güvenliği Farkındalığı Üzerine Bir Araştırma. *Turkish Journal of Education*, 2(3), 61-70.
- Thomson, Mark E. and von Solms, R. (1998). Information Security Awareness: Educating Your Users Effectively. *Information Management & Computer Security*, 6(4), 167-173.
- Thunholm, P. (2004). Decision-making Style: Habit, Style or Both? *Personality and Individual Differences*, 36(4), 931-944.
- Tirumala, S. S., Valluri, M. R. and Babu, G. A. (2019). *A Survey on Cybersecurity Awareness Concerns, Practices and Conceptual Measures*. 2019 International Conference on Computer Communication and Informatics, Coimbatore, India.

- Tirumala, S. S., Sathu, H. and Naidu, V. (2015). *Analysis and Prevention of Account Hijacking Based Incidents in Cloud Environment*. 2015 International Conference on Information Technology, Bhubaneswar, India.
- Toch, E., Bettini, C., Shmueli, E., Radaelli, L., Lanzi, A., Riboni, D. and Lepri, B. (2018). The privacy implications of cyber security systems: A technological survey. *ACM Computing Surveys (CSUR)*, 51(2), 1-27.
- Tomer, P., Lade, S., Kumar, M. S. and Patel, D. (2013). On Line Social Network Content and Image Filtering, Classifications. *International Journal of Engineering Research and Science & Technology*, 2(4), 16.
- Topping, C., Dwyer, A., Michalec, O., Craggs, B. and Rashid, A. (2021). Beware Suppliers Bearing Gifts!: Analysing Coverage of Supply Chain Cyber Security in Critical National Infrastructure Sectorial and Cross-Sectorial Frameworks. *Computers & Security*, 108, 102324.
- Trueltzsch-Wijnen, C. W., Milosevic, T., Mifsud, C. and Dias, P. (2018). Media Representation of Children's Privacy in the Context of the Use of "Smart" Toys and Commercial Data Collection. *Media Studies*, 9(18), 6-25.
- Tuğal, İ., Almaz, C. ve Mehmet, S. (2021). Üniversitelerdeki Siber Güvenlik Sorunları ve Farkındalık Eğitimleri. *Bilişim Teknolojileri Dergisi*, 14(3), 229-238.
- Ulusal Siber Güvenlik Stratejisi (2020). Ulusal Siber Güvenlik Stratejisi ve Eylem Planı; *UAB Raporu*, Ankara, 11-31.
- Ulusal Siber Olaylara Müdahale Merkezi (2014). Siber Güvenliğe İlişkin Temel Bilgiler; *USOM Raporu*, Ankara, 1-14.
- Uma, M. and Padmavathi, G. (2013). A Survey on Various Cyber Attacks and Their Classification. *International Journal of Network Security*, 15(5), 390-396.
- UNESCO. (2020). Education: From school closure to recovery; *UNESCO Report*, United Kingdom, 1-60.
- Ünver, M. (2012). Ulusal Siber Güvenliğin Sağlanmasında Farkındalık Çalışmaları. *Mimar Mühendisler Dergisi*, (60), 1-8.
- Vaczi, D., Toth-Laufer, E. and Szadeczky, T. (2020). *Fuzzy-based Cybersecurity Risk Analysis of The Human Factor From The Perspective of Classified Information Leakage*. 18th International Symposium on Intelligent Systems and Informatics, Subotica, Serbia.
- Valcke, M., De Wever, B., Van Keer, H. and Schellens, T. (2011). Long-term Study of Safe Internet Use of Young Children, *Computers & Education*, 57(1), 1292-1305.
- Valli, C. , Martinus, I. C., and Johnstone, M. N. (2014). *Small to Medium Enterprise Cyber Security Awareness: An Initial Survey of Western Australian Business*. International Conference on Security and Management, Las Vegas, USA.

- Velki, T., Solic, K., Gorjanac, V. and Nenadic, K. (2017). *Empirical Study on the Risky Behavior and Security Awareness Among Secondary School Pupils-Validation and Preliminary Results*. 40th International Convention on Information and Communication Technology, Electronics and Microelectronics , Opatija, Croatia.
- Vishwanath, A., Neo, L. S., Goh, P., Lee, S., Khader, M., Ong, G. and Chin, J. (2020). Cyber Hygiene: The Concept, its Measure, and its Initial Tests. *Decision Support Systems*, 128, 113160.
- Von Solms, R. and Van Niekerk, J. (2013). From Information Security to Cyber Security. *Computers & Security*, 38, 97-102.
- Waldrop, M. (2008). DARPA and the Internet Revolution. *Bridging The Gap*, 78-85.
- Waxman, M. C. (2011). Cyber-attacks and the Use of Force: Back to the Future of Article. *Yale Journal of International Law*, 36, 421.
- Whitson, J. (2009). Feature Identity Theft and the Challenges of Caring for Your Virtual Self. *Interactions*, 16(2), 41-45.
- Witsenboer, J. W. A., Sijtsma, K. and Scheele, F. (2022). Measuring Cyber Secure Behavior of Elementary and High School Students in the Netherlands. *Computers & Education*, 186, 104536.
- Yang, L.-X., Yang, X., Zhu, Q. and Wen, L. (2013). A Computer Virus Model with Graded Cure Rates. *Nonlinear Analysis: Real World Applications*, 14(1), 414-422.
- Yu, W., Boyer, C., Chellappan, S. and Xuan, D. (2005). *Peer-to-Peer System-Based Active Worm Attacks: Modeling and Analysis*. IEEE International Conference on Communications, Seoul, Korea.
- Yuliana, Y. (2022). The Importance of Cybersecurity Awareness for Children. *Lampung Journal of International Law*, 4(1), 41-48.
- Zhu, N., Liu, X., Liu, J. and Hua, Y. (2014). Towards a Cost-efficient MapReduce: Mitigating Power Peaks for Hadoop Clusters. *Tsinghua Science and Technology*, 19(1), 24-32.
- Zwick, W. R. and Velicer, W. F. (1986). Comparison of Five Rules for Determining the Number of Components to Retain. *Psychological Bulletin*, 99(3), 432.



EKLER

Ek-1: SGFÖ Nihai Form

FAKTÖR İSMİ	S.No	MADDELER
Şifre Güvenliği	1	Şifre oluştururken özel karakterler, rakam ve harf kullanılması gerektiğini bilirim.
	2	Parolamı en az 8 karakterden oluşması gerektiğini bilirim.
	3	Kişisel bilgilerimin yer aldığı şifre oluşturmakta sakınca görmüyorum. (T)
	4	Şifre kimseyle paylaşmam.
	5	Şifrelerimi sıklıkla değiştiririm.
	6	İki faktörlü kimlik doğrulamanın ne olduğunu bilirim.
	7	Herhangi bir işlem yapmadığım halde e-postama gelen parola sıfırlama iletilerini dikkate almam.
Önleyici Tedbirler	8	Gelen e-postalarda isim ve e-posta adresini kontrol ederim.
	9	Tanımadığım kişilerden gelen e-postada samimi ifadeler varsa (sevgili beyefendi/ hanımefendi vb.) dikkatli olmam gerektiğini bilirim.
	10	Bir e-postadaki veya sosyal medya gönderisindeki bağlantılara tıklama konusunda dikkat ederim.
	11	Bir e-posta ekini açmadan önce, ekteki dosya adının anlamlı olup olmadığını kontrol ederim.
	12	Acil, önemli başlığıyla gelen e-postalara şüpheyile yaklaşırım.
	13	Bağlantının güvenli olduğunu teyit etmek amacıyla bağlantı adresinin https:// olup olmadığını kontrol ederim.
	14	Bir e-postayı okumadan önce e posta konusunun anlamlı ve gönderenin gerçek bir kişi olup olmadığına bakarım.
Kötü Amaçlı Yazılım Farkındalığı	15	Cihazlarımda gerekli yazılım güncellemelerini yaparım.
	16	Solucan ve virüsün farkını bilirim.
	17	Kötü amaçlı yazılım kullanılarak uzaktan bağlantı ile bilgisayarımın ele geçirilebileceğini düşünürüm.
	18	Bilgisayarıma saldırı olabilecek kötü amaçlı yazılım türlerinin farkındayım.
	19	Kötü amaçlı yazılımların internete erişmeme engel olabileceğini düşünürüm.
	20	Cihazımın/cihazlarımda verilerinin yedek kopyalarını oluştururum.
Kişisel Gizliliği Koruma	21	Sosyal medyada adıma hesap açılmasının kimlik hırsızlığı olduğunu bilirim.
	22	Tanıdığım kişiden gelen e-postada kişisel bilgilerim istenirse paylaşırım. (T)
	23	E-posta ile gelen kimlik bilgilerini doğrulama mesajlarına (parola, kredi kartı vb.) itibar edilmemesi gerektiğini bilirim.
	24	Sosyal medya servislerinde kişisel bilgilerimi koruyan özellikler olduğunu bilirim.
	25	Kimlik avının ne olduğunu bilirim.

* (T): Ters maddeleri belirtmektedir.

Ek-2 Ölçek Geliştirme İzinleri ve Veri Toplama Araçları



T.C.
AMASYA VALİLİĞİ
İl Millî Eğitim Müdürlüğü



Sayı : E-47613789-44-38058231
Konu : Tez Çalışması Kapsamında
Araştırma İzni

01.12.2021

VALİLİK MAKAMINA

- İlgi : a) Amasya Üniversitesi Rektörlüğü Öğrenci İşleri Daire Başkanlığı'nın 29/11/2021 tarih ve E-47526769-302.08.01-44503 sayılı yazısı.
b) Millî Eğitim Bakanlığı'nın 21/01/2020 tarihli ve 1563890 (2020/2) Sayılı Genelgesi.

İlgi yazı (a) ile; Amasya Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar ve Öğretim Teknolojileri Anabilim Dalı Tezli Yüksek Lisans 198113010 nolu öğrencisi Fırat YILMAZ tarafından uygulanması planlanan "Ortaokul Öğrencilerinin Siber Güvenlik Bilgi Düzeylerini Geliştirmeye Yönelik Oyun Tasarımı" konulu tez çalışması kapsamında, Dr. Öğr. Üyesi Aşlıhan İSTANBULLU danışmanlığında, Müdürlüğümüze bağlı Merkez ilçede bulunan Ziyapaşa Ortaokulu, Amasya Çelebi Mehmet Ortaokulu, Abdurrahman Kamil Ortaokulu, Gazi Ortaokulu ile Yavuz Selim Ortaokulu'nda öğrenim gören öğrencilere belirtilen anketi uygulayabilmek için izin talep edilmektedir.

Bu bağlamda; söz konusu talebin, ilgi (b) 21/01/2020 tarihli ve 1563890 (2020/2) sayılı Genelge (Araştırma Uygulama İzinleri) de belirtilen hususlar doğrultusunda ve Türkiye Cumhuriyeti Anayasası ve insan hakları alanındaki uluslararası sözleşmeler başta olmak üzere 6698 sayılı Kişisel Verilerin Korunması Hakkındaki Kanun ile yürürlükte olan tüm yasal düzenlemeler ve politika belgelerine uygun, Türkiye Cumhuriyeti Anayasası, Millî Eğitim Temel Kanunu ile Türk Millî Eğitiminin genel amaçlarına uygun olarak ilgili yasal düzenlemelerde belirtilen ilke, esas ve amaçlara aykırılık teşkil etmeyecek şekilde, denetimleri ilgili okul müdürlükleri tarafından gerçekleştirilmek üzere, derslerin aksatılmaması ve gönüllülük esasına göre araştırma yapılması, araştırma ile ilgili sonuç raporlarını çalışmanın bitiş tarihinden itibaren 30 (otuz) gün içinde izin alınan kuruma ulaştırılması, uygulama sırasında da mühürlü ve imzalı örnekten çoğaltılan veri toplama araçlarının kullanılması Müdürlüğümüzce uygun görülmektedir.

Makamlarınızca da uygun görüldüğü takdirde Ohurlarınıza arz ederim.

Alpaslan KANAR
Müdür a.
İl Millî Eğitim Şube Müdürü

OLUR
01.12.2021
Bedir ARSLAN
Vali a.
İl Millî Eğitim Müdür V.

Bu belge güvenli elektronik imza ile imzalanmıştır.

Adres : Hızırpaşa Mah. İstasyon Cad. No: 72 Merkez/AMASYA

Belge Doğrulama Adresi : <https://www.turkiye.gov.tr/mob-ebys>

Bilgi için: Ahmet D.DURMUŞ

Teléfono No : (0358) 212 29 93/2041

E-Posta : argo05@msb.gov.tr

Kop Adresi : msb@hs01.kop.tr

İnternet Adresi: Uzman : Memur

Faks : (0358) 218 50 :

Bu evrak güvenli elektronik imza ile imzalanmıştır. <https://evrak.sorgu.msb.gov.tr> adresinden **effb-1ae2-3d21-a169-f477** kodu ile teyit edilebilir.



Ek-2 Ölçek Geliştirme İzinleri ve Veri Toplama Araçları (Devamı)

B. SİBER GÜVENLİK FARKINDALIĞI					
Ölçek Maddeleri	Tanımadım Katılmıyorum	Kısmen Katılmıyorum	Ne Katılmıyorum Ne Katılmıyorum	Katılmıyorum	Kesinlikle Katılmıyorum
1. Kişisel bilgilerin çevrimiçi ortamda ifşa edilmesinden kaçınılmaz olduğunu düşünüyorum.					
2. Şifre oluştururken özel karakter, rakam ve harf kullanmayı önem gösteririm.					
3. Kişisel bilgilerimi sosyal medya üzerinden paylaşmamaya özen gösteririm.					
4. Dijital cihazımda bilgisayar korsanları için tehlike olmadığını düşünüyorum.					
5. Sosyal ağ sitelerinde kendi ad ve soyadımı kullanırım.					
6. Bir e-posta ekini açmadan önce, ekteki dosya adının belirsiz olup olmadığını kontrol ederim.					
7. Tanımadığım kişilerden gelen e-posta içeriğinde posta karanılağıyla belirsiz bağlantı verilmeye çalışıldığına inanırım.					
8. Kişisel bilgilerimin yer aldığı şifre oluşturmakta sakınca görmüyorum.					
9. İçeriklerin ne olduğunu bilmediğim yazımları indirmem.					
10. E-postamın içeriği güvenli görünmüyorsa e-posta eklenmiş olabilir.					
11. Bilgisayar söküpçisi ve virüsünün farkında değilim.					
12. Cihazımı/cihazıma verilecek kodlarımdan dikkatliyim.					
13. Şifrelerimi sürekli değiştiririm.					
14. Sosyal medya hesaplarımda gültük olarak gereken bakiyeyle çalışırım.					
15. Lütfen "Kesinlikle Katılmıyorum" seçeneğini işaretleyiniz.					
16. Bağlantıları güvenli olduğuna bizzat etmek amacıyla bağlantı adresini https:// olup olmadığını kontrol ederim.					
17. Sosyal medya verilerimde kişisel bilgilerimi koruyan özellikler olduğuna inanırım.					
18. Herhangi bir işlem yapmadığım halde e-postama gelen posta virüsüne bulaşmış olabilir.					
19. E-posta ile gelen kimlik bilgilerini diğer sosyal medya hesaplarıma (parola, kredi kartı vb.) ilebir edilmemesi gerektiğini bilirim.					
20. Sosyal medyada adımı hesap açmam kimlik baskınlığı olduğunu bilirim.					
21. Kötü amaçlı yazılım hakkında olumlu duyuyorum.					
22. Sosyal ağ sitelerinde doğan taktikleri paylaşıyorum.					
23. Tanımadığım kişilerden gelen e-postada kişisel bilgilerim istenirse paylaşıyorum.					
24. Tanımadığım kişilerden gelen e-postalara bakarken dikkatli olurum.					
25. Uzaktan eğitim derslerimi ve diğer bilgileri başka kişilerle paylaşıyorum.					
26. Şifremi kimseye paylaşıyorum.					
27. Kimlik avımı ne olduğunu bilirim.					
28. Bilgisayarına saldırı olabilecek kötü amaçlı yazılım türlerinin farkındayım.					
29. Bir e-postadaki veya sosyal medya gönderisindeki bağlantılara bulaşma konusunda dikkat ederim.					
30. Tanımadığım kişilerden gelen e-postada sakıncalı ifadeler varsa (sevgi, beğeniler, huzursuzluk, şüpheli vb.) dikkatli olmaya gerektiğini bilirim.					
31. Tanımadığım kişilerden gelen e-postamın içeriğinde yazan ve dil bilgisi tutmaz varsa dikkatli olurum.					
32. Ansa, önemli bilgileri gelen e-postalara şüpheliye sokuyorum.					
33. Sosyal ağ sitelerine bulaşıcı sığınırım.					
34. Lütfen "Kesinlikle Katılmıyorum" seçeneğini işaretleyiniz.					
35. Kötü amaçlı yazılımların internete erişimine engel olabileceğini düşünüyorum.					
36. Siber saldırılarla USOM ile ilgilediğimi bilirim.					



Ek-2 Ölçek Geliştirme İzinleri ve Veri Toplama Araçları (Devamı)

Ölçek Maddeleri	Tamamen Katılmıyorum	Kısmen Katılmıyorum	Ne Katılmıyorum Ne Katılmıyorum	Kısmen Katılmıyorum	Kesinlikle Katılmıyorum
37. Okullarda geçirdiğim günlerini verim verim yapıyorum					
38. Tanıdığım kişileri gelen e-postada yer alan bağlantı adresi ilgili kişilerle buluşturuyorum					
39. Bir e-postayı okumadan önce e-posta kutusundaki bilgileri ve göndereni gerçek bir kişi olup olmadığını araştırıyorum					
40. Gelen e-postalarda isim ve e-posta adresini kontrol ediyorum					
41. Lütfen "Ne Katılmıyorum Ne Katılmıyorum" seçeneğini işaretleyiniz					
42. İki faktörle ilgili olarak, ilahî bir güç olduğunu biliyorum					
43. Hiç bilmediğim kişilerle görüntülü ve sesli görüşmeler yapıyorum					
44. Aradığım e-posta üzerinden benden para isterse gönderirim					
45. Sosyal ağ sitelerinde kendimin veya tanıdıklarımın hesablarını kontrol ediyorum					
46. Kod amaçlı yazılım kullanarak istikrarlı bağlantı ile bilgisayarımı etkinleştiriyorum					
47. Dijital ortamların güvenli olmadığını fark ediyorum					
48. Site oluştururken özel karakter, rakam ve harf kullanmanın gerekliliğini biliyorum					
49. Parola ve e-posta adresi karakterlerini değiştirmeyi biliyorum					
50. Bilgi saklama ortamında nereye başvuracağımı biliyorum					

Not: 50 maddeli de doldurduğunuzdan emin olunuz

Sevgili öğrenciler,
Katkılarınız için teşekkür ederiz



Ek-2 Ölçek Geliştirme İzinleri ve Veri Toplama Araçları (Devamı)

Ek-1

Sayın Veli;

Çocuğunuzun katılacağı bu çalışma, "Okulda Bulunma İstencileri" Sitem Anketi Etki Belirleyici adıyla, 21. Aralık 2021 tarihleri arasında yapılacak bir araştırma uygulamasıdır.

Araştırmanın Hedefi: Okulda Bulunma İstencileri Sitem Anketi Bilgi
Dinamikleri, Geliştirme ve Yeterlilik Ölçümü, Temel Bilgi, Akademi Bilgi

Araştırma Uygulaması: Anket / Görüşme / Gözlem şeklindedir.

Araştırma T.C. Milli Eğitim Bakanlığı'nın ve okul yönetiminin de izni ile gerçekleştirilmektedir. Araştırma uygulamasına katılım tamamıyla gönüllülük esasına dayalı olmaktadır. Çocuğunuz çalışmaya katılıp katılmamakta özgürdür. Araştırma çocuğunuz için herhangi bir istenmeyen etki ya da risk taşımamaktadır. Çocuğunuzun katılımı tamamen sizin isteğinize bağlıdır, reddedebilir ya da herhangi bir aşamasında geri çekilirsiniz. Araştırmaya katılmama veya araştırmadan ayrılma durumunda öğrencilerin akademik başarıları, okul ve öğretmenleriyle olan ilişkileri etkilemeyecektir.

Çalışmada öğrencilerden kimlik belirleyici hiçbir bilgi istenmemektedir. Cevaplar tamamıyla gizli tutulacak ve sadece araştırmacılar tarafından değerlendirilecektir.

Uygulamalar, genel olarak kişisel rahatsızlık vererek sorular ve durumlar içermemektedir. Ancak, katılım sırasında sorulardan ya da herhangi başka bir nedenden çocuğunuz kendisini rahatsız hissederse cevaplama işini yarıda bırakıp çıkarakta özgürdür. Bu durumda rahatsızlığın giderilmesi için gereken yardım sağlanacaktır. Çocuğunuz çalışmaya katıldıktan sonra istediği an vazgeçebilir. Böyle bir durumda veri toplama aracını uygulayan kişiye, çalışmayı tamamlamayacağıı söylemesi yeterli olacaktır. Anket çalışmasına katılmamak ya da katıldıktan sonra vazgeçmek çocuğunuzun hiçbir sorumluluk gerektirmeyecektir.

Onay vermeden önce sormak istediğiniz herhangi bir konu varsa sormaktan çekinmeyiniz. Çalışma bittikten sonra bizlere telefon veya e-posta ile ulaşarak soru sorabilir, soruları hakkında bilgi isteyebilirsiniz. Saygılarımızla,

Araştırmacı : Arat Gülhan
İletişim bilgileri : 0544 496 75 05 - Arat.gulhan@usb-pav.tr

Vefisi bulunduğum sınıfı numaranı öğrencisi
"in yukarıda açıklanan araştırmaya katılmasına izin veriyorum."
(İltiften formu imzalandıktan sonra çocuğunuzla okula geri gönderiniz*).

.....

İsim-Soyisim İmza:

Veli Adı-Soyadı :

Telefon Numarası :



Ek-3 Uygulama İzinleri ve Veri Toplama Araçları



T.C.
AMASYA VALİLİĞİ
İl Milli Eğitim Müdürlüğü



Sayı : E-47613789-44-64938701
Konu : Tez Çalışması Kapsamında
Araştırma/Anket İzni

02.12.2022

VALİLİK MAKAMINA

- İlgi : a) Amasya Üniversitesi Rektörlüğü Öğrenci İşleri Daire Başkanlığının 28.11.2022 tarih ve E-47526769-302.08.01-103196 sayılı yazısı.
b) Milli Eğitim Bakanlığının 21/01/2020 tarihli ve 1563890 (2020/2) Sayılı Genelgesi.

İlgi yazı (a) ile; Amasya Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar ve Öğretim Teknolojileri Anabilim Dalı Tezli Yüksek Lisans Programı 198113010 nolu öğrencisi Fırat YILMAZ tarafından uygulanması planlanan "Ortaokul Öğrencilerinin Siber Güvenlik Farkındalıklarının Belirlenmesi" konulu tez çalışması kapsamında, Dr. Öğr. Üyesi Aşlıhan İSTANBULLU'nun danışmanlığında, Müdürlüğümüze bağlı Merkez ilçede bulunan Ziyapaşa Ortaokulu ile Abdurrahman Kamil Ortaokulu öğrencilerine, belirtilen anketi uygulayabilmek için izin talep edilmektedir.

Bu bağlamda; söz konusu talebin, ilgi (b) 21/01/2020 tarihli ve 1563890 (2020/2) sayılı Genelge (Araştırma Uygulama İzinleri) de belirtilen hususlar doğrultusunda ve Türkiye Cumhuriyeti Anayasası ve insan hakları alanındaki uluslararası sözleşmeler başta olmak üzere 6698 sayılı Kişisel Verilerin Korunması Hakkındaki Kanun ile yürürlükte olan tüm yasal düzenlemeler ve politika belgelerine uygun, Türkiye Cumhuriyeti Anayasası, Milli Eğitim Temel Kanunu ile Türk Millî Eğitiminin genel amaçlarına uygun olarak ilgili yasal düzenlemelerde belirtilen ilke, esas ve amaçlara aykırılık teşkil etmeyecek şekilde, denetimleri ilgili okul müdürlükleri tarafından gerçekleştirilmek üzere, derslerin aksatılmaması ve gönüllülük esasına göre araştırma yapılması, araştırma ile ilgili sonuç raporlarını çalışmanın bitiş tarihinden itibaren 30 (otuz) gün içinde izin alınan kuruma ulaştırılması, uygulama sırasında da mühürlü ve imzalı örnekten çoğaltılan veri toplama araçlarının kullanılması Müdürlüğümüze uygun görülmektedir.

Makamlarınızca da uygun görüldüğü takdirde Olurlarınıza arz ederim.

Alpaslan KANAR
Müdür a.
İl Milli Eğitim Şube Müdürü

OLUR
02.12.2022
Abdullah GÜRBÜZ
Vali a.
İl Milli Eğitim Müdür V.

Ekler:

- 1- İlgi (a) Yazı ve Ekleri (45 Sayfa)
- 2- Mühürlü ve İmzalı Veri Toplama Araçları (4 Sayfa)
- 3- (2020/2) Sayılı Genelge (3 Sayfa)

Bu belge güvenli elektronik imza ile imzalanmıştır.

Adres : Hızırpaşa Mah. İstasyon Cad. No: 72 Merkez/AMASYA

Belge Doğrulama Adresi : <https://www.turkiye.gov.tr/meb-ebys>

Telefon No : (0358) 212 29 93/2041

E-Posta : argu05@meb.gov.tr

Kep Adresi : meb@tr01.kep.tr

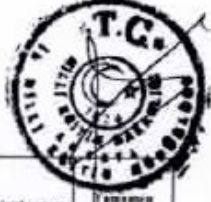
Bilgi için: Ahmet D.DURMUŞ

Unvan : Müdür

İnternet Adresi : Faks : (0358) 218 50 31

Bu evrak güvenli elektronik imza ile imzalanmıştır. <https://evraksorgu.meb.gov.tr> adresinden 80b4-0e72-3897-a059-c9ca koda ile teyit edilebilir.

Ek-3 Uygulama İzinleri ve Veri Toplama Araçları (Devamı)



9) GİRİŞ GÜVENLİK FARKINDALIĞI FORMU

Sıra No	Ölçek Maddeleri	Katılılıyla Katılmıyorum	Katılmıyorum	Ne Katılıyorum Ne Katılmıyorum	Katılıyorum	Hiçbir şekilde Katılmıyorum
1	Şifre oluştururken özel karakterler, rakam ve harf kullanılması gerektiğini bilirim.					Ek-2
2	Parolamı en az 8 karakterden oluşması gerektiğini bilirim.					
3	Kişisel bilgilerimin yer aldığı şifre oluşturmakla sakınca görmüyorum.					
4	Şifreimi kimseye paylaşmam.					
5	Şifrelerimi sık sık değiştiririm.					
6	İki (iki) farklı kimlik doğrulama ne olduğunu bilirim.					
7	Herhangi bir işlem yapmadığım halde e-postama gelen parola uyarılma (bilirlerini dikkate almam).					
8	Gelen e-postalarda isim ve e-posta adresini kontrol ederim.					
9	Tanımadığım kişilerden gelen e-postada sandiği (hacker varsa (sevgili boyefendi) barmefendi vb.) dikkatli olmam gerektiğini bilirim.					
10	Bir e-postadaki veya sosyal medya gönderisindeki bağlantılara tıklama konusunda dikkat ederim.					
11	Bir e-posta ekini açmadan önce, ekteki dosya adının anlamlı olup olmadığını kontrol ederim.					
12	Acil, önemli başlığıyla gelen e-postalara dikkatle yaklaşıyorum.					
13	Bağlantının güvenli olduğunu veya etmekte amacıyla bağlantı adresinin https:// olup olmadığını kontrol ederim.					
14	Bir e-postayı okumadan önce e-posta konusunun anlamlı ve gönderenin gerçek bir kişi olup olmadığını bakıyorum.					
15	Cihazlarımda gerekli yazılım güncellemelerini yapıyorum.					
16	Solucan ve virüsün farkını bilirim.					
17	Kötü amaçlı yazılım kullandıkları araçları ile bilgisayarımın ele geçirilebileceğini düşünürüm.					
18	Bilgisayarına saldırı olabileceğini kötü amaçlı yazılım türlerinin farkındayım.					
19	Kötü amaçlı yazılımına internete erişimene engel olabileceğini düşünürüm.					
20	Cihazlarım/cihazlarımda verilerimin yedek kopyalarını oluştururum.					
21	Sosyal medyada olma hesap açmadığım kimlik hususları olduğunu bilirim.					
22	Tanımadığım kişiden gelen e-postada kişisel bilgilerim istenirse paylaşırım.					
23	E-posta ile gelen kimlik bilgilerini doğrulama mesajlarına (parola, kredi kartı vb.) itibar edilmemesi gerektiğini bilirim.					
24	Sosyal medya servislerinde kişisel bilgilerimi koruyan özellikler olduğunu bilirim.					
25	Kimlik avına ne olduğunu bilirim.					

Not: 25 maddesi ce doldurduğunuzdan emin olunuz.

Sevgili öğrenciler, Katılılıyla Katılmıyorum için işaretler ediniz.

Bu belge güvenli elektronik imza ile imzalanmıştır.

Bu belge güvenli elektronik imza ile imzalanmıştır.

ÖZGEÇMİŞ

Adı-Soyadı : Fırat YILMAZ

Bilimsel Faaliyetler (Yayınlar, Bildiriler, Katıldığı Projeler)

1-) F Yılmaz ve A Istanbulu (2022). Uzaktan Eğitimde Kişisel Siber Güvenliğin Önemi ve Çözüm Önerileri *14th International Computer and Instructional Technologies Symposium*. 26-28.

2-) F Yılmaz ve A Istanbulu (2022). Internet Güvenliği Farkındalığında Oyunların Etkisi *14th International Computer and Instructional Technologies Symposium*. 162-171