



**T.C.**

**TOKAT GAZİOSMANPAŞA ÜNİVERSİTESİ**

**LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ**

**BİLGİSAYAR VE ÖĞRETİM TEKNOLOJİLERİ EĞİTİMİ ANABİLİM DALI**

**YÜKSEK LİSANS PROGRAMI**

**SİBER SUÇ FARKINDALIK ÖLÇEĞİ GELİŞTİRME:**

**GEÇERLİK VE GÜVENİRLİK ÇALIŞMASI**

**YÜKSEK LİSANS TEZİ**

**Ersin ATEŞ**

**Danışman: Doç. Dr. İbrahim ARPACI**

**TOKAT**

**Ekim, 2021**

## ETİK SÖZLEŞME

Bu belge ile bu tezdeki bütün bilgi toplama ve raporlaştırma sürecinin Tokat Gaziosmanpaşa Üniversitesi Lisansüstü Eğitim ve Öğretim Yönetmeliği'ne, Lisansüstü Eğitim Enstitüsü Tez Yazım Kılavuzuna, genel akademik kurallara ve etik ilkelere uygun olarak gerçekleştirildiğini; bu tez çalışmasının “intihal engelleme” programı ile tarandığını, bana ait olmayan tüm bilgi, düşünce ve bulgulara atıf yaptığımı ve kaynağını gösterdiğimi beyan eder, sorumluluğun tarafıma ait olduğunu kabul ederim.

Tarih: 12/ 10/ 2021

Tezi hazırlayan öğrencinin

Ersin ATEŞ

İmza

## Jüri Onay Sayfası

Lisansüstü Eğitim Enstitüsü Müdürlüğü'ne,

.....'nın.....

.....  
..... adlı çalışması ..... tarihinde jürimiz tarafından  
..... Anabilim / Ana Sanat Dalı'nda yüksek lisans  
tezi olarak kabul edilmiştir.

Adı Soyadı

İmza

Başkan: Doç. Dr. Kemal BAYTEMİR

.....

Üye (Tez Danışmanı): Doç. Dr. İbrahim ARPACI

.....

Üye: Doç. Dr. Kerem KILIÇER

.....

Onay

Yukarıdaki imzaların adı geçen öğretim üyelerine ait olduğunu onaylarım.

.../.../2021

.....

Enstitü Müdürü

## TEŞEKKÜR

Lisans ve yüksek lisans eğitim sürecinde bana yol gösteren, her zaman yanımda olan rahatça her problemi ve sorunlarımı paylaşabildiğim ve tüm sorunlarıma ortak olan aynı zamanda tezimin yazım sürecinde tecrübesi ve bilgi birikimiyle benimle sürekli fikirlerini paylaşan ilgisini hiçbir zaman esirgemeyen ve ölçeğin geliştirilmesi, ölçeğin uygulanması ve analiz aşamasında bana yardımcı olan, yol gösteren tez danışmanım Sn. Doç. Dr. İbrahim ARPACI hocama teşekkürlerimi sunarım.

Tokat Gaziosmanpaşa Üniversitesi BÖTE ve PDR bölümündeki hocalarıma da mesleki gelişimimde, iş arama sürecimde ve akademik anlamda bilgi birikimleriyle bana katkıda bulundukları için ve tez yazım ve veri toplama sürecinde yardımlarını esirgemedikleri için ayrı ayrı teşekkürlerimi sunarım. Ayrıca hazırlamış olduğum bu tezimde ölçek geliştirme ve veri toplama sürecinde bana yardımlarını hiç esirgemeyen değerli abim Kadir SEVİNÇ ve değerli arkadaşım Bilal ERDEM kardeşime ayrıca teşekkürlerimi sunarım. Sevgili kardeşim Taha ATEŞ, abim Halil ATEŞ ve yengem Fazilet ATEŞ veri toplama sürecinde ve tüm aşamalarında bana yardımcı oldukları için çok teşekkür ederim.

Tezimi yazmam konusunda bana sürekli yol gösteren, benim bugünlere gelmemde en büyük paya sahip, hayatımın her anında yanımda olan, bana hayat tecrübeleriyle rehberlik eden, arkamda dağ gibi duran Kemal ATEŞ babama sonsuz sevgi ve saygılarımı sunarım. Ayrıca sevgisini, merhametin desteğini bana karşı hiç eksik etmeyen, her zaman manevi olarak bana destek veren benim yanımda olan Fatma ATEŞ anneme de sevgi ve saygılarımı sunar, teşekkür ederim.

Ersin ATEŞ

## ÖZET

### SİBER SUÇ FARKINDALIK ÖLÇEĞİ GELİŞTİRME:

#### GEÇERLİK VE GÜVENİRLİK ÇALIŞMASI

Ateş, Ersin

Yüksek Lisans, Bilgisayar ve Öğretim Teknolojileri Eğitimi Ana Bilim Dalı

Tez Danışmanı: Doç. Dr. İbrahim Arpacı

Ekim 2021, x + 61 sayfa

Siber suçlar, siber saldırı ve tehditlere bağlı olarak günden güne artış göstermektedir. Böyle bir artıştan dolayı dışardan gelecek her türlü siber saldırı ve tehditlere karşı gereken güvenlik önlemleri hem bireysel hem de kurumsal olarak alınması gerekmektedir. Bu tez bireylerin siber suç farkındalık düzeylerini belirlemede kullanılacak geçerli ve güvenilir bir ölçme aracı geliştirmeyi amaçlamaktadır. Bu doğrultuda, bireylerin siber suç farkındalık düzeylerini belirlemeye yönelik “siber suç farkındalık ölçeği” adı verilen bir ölçme aracı geliştirilmiş ve psikometrik özellikleri test edilmiştir. Bu çalışmanın örneklemini Tokat Gaziosmanpaşa Üniversitesinde öğrenim gören 994 üniversite öğrencisi oluşturmaktadır. Birinci çalışma toplam 500 (294 kadın, 206 erkek) katılımcıdan oluşmaktadır. Birinci çalışmada ölçeğin faktör yapısı açıklayıcı faktör analizi (AFA) ile test edilmiştir. AFA sonuçları üç faktörlü bir yapı ortaya koymuştur ve ölçeğin tamamı için Cronbach alfa iç tutarlık kat sayısı .97 olarak bulunmuştur. İkinci çalışmanın örneklemini toplam 494 (281 kadın ve 213 erkek) katılımcıdan oluşmaktadır. İkinci çalışmada, doğrulayıcı faktör analizi gerçekleştirilerek üç faktörlü yapının (siber ortamda yer alan suçlar, siber ortama ve kişisel verilere yönelik suçlar ve gizlilik ve güvenlik) verilerle iyi uyum gösterip göstermediği incelenmiştir. Sonuçlar geliştirilen ölçme aracının bireylerin siber suç farkındalık düzeylerini ölçmede kullanılabilecek geçerli ve güvenilir bir ölçek olduğunu ortaya koymuştur.

Anahtar Kelimeler: Siber Suç, Siber Suç Farkındalık Ölçeği, Ölçek Geliştirme

## **ABSTRACT**

### **DEVELOPMENT OF CYBERCRIME AWARENESS SCALE (CAS):**

#### **VALIDITY AND RELIABILITY STUDY**

Ateş, Ersin

Master's Thesis, Department of Computer Education and Instructional Technology

Advisor: Assoc. Prof. Dr. İbrahim Arpacı

October 2021, x + 61 pages

Cybercrimes increase day by day based on cyber-attacks and threats. Due to such an increase, required security precautions against all kinds of cyber-attacks and threats should be taken by both individuals and organizations. This thesis aims to develop a valid and reliable measurement tool to be used in determining the cybercrime awareness level of individuals. Accordingly, a measurement tool named “cybercrime awareness scale” has been developed to determine the cybercrime awareness level of individuals and psychometric properties have been tested. The sample of this study consists of 994 undergraduate students studying at Tokat Gaziosmanpaşa University. The first study included a total of 500 respondents (294 female, 206 male). In the first study, factor structure of the scale has been tested with exploratory factor analysis (EFA). The EFA results revealed a three-factor structure, and the Cronbach alpha internal consistency coefficient of the total scale has been found as .97. The sample of the second study, consisted of 494 respondents (281 female and 213 male). In the second study, a confirmatory factor analysis was performed to investigate whether the three-factor structure (crimes in cyberspace, crimes against cyberspace and personal data, and privacy and security) has a good fit with the data or not. The results indicated that the developed measurement tool is a valid and reliable scale that can be used to measure individuals' cybercrime awareness level.

**Keywords:** Cybercrime, Cybercrime Awareness Scale, Scale Development

## İÇİNDEKİLER

|                                                                          | Sayfa |
|--------------------------------------------------------------------------|-------|
| ETİK SÖZLEŞME.....                                                       | i     |
| JÜRİ İMZA SAYFASI.....                                                   | ii    |
| TEŞEKKÜR.....                                                            | iii   |
| ÖZET .....                                                               | iv    |
| ABSTRACT.....                                                            | v     |
| İÇİNDEKİLER .....                                                        | vi    |
| TABLO LİSTESİ.....                                                       | viii  |
| ŞEKİL LİSTESİ.....                                                       | ix    |
| KISALTMALAR.....                                                         | x     |
| BÖLÜM I.....                                                             | 1     |
| GİRİŞ .....                                                              | 1     |
| Problem .....                                                            | 1     |
| Amaç .....                                                               | 4     |
| Önem.....                                                                | 4     |
| Sınırlılıklar .....                                                      | 7     |
| Tanımlar .....                                                           | 7     |
| BÖLÜM II .....                                                           | 10    |
| KAVRAMSAL ÇERÇEVE.....                                                   | 10    |
| Farkındalık .....                                                        | 10    |
| Siber Güvenlik, Bilgi Güvenliği Farkındalığı ve Yapılan Çalışmalar ..... | 13    |
| Siber Suç Farkındalığı ve Yapılan Çalışmalar .....                       | 21    |
| Ölçek Geliştirme Çalışmaları .....                                       | 25    |
| BÖLÜM III .....                                                          | 27    |
| YÖNTEM .....                                                             | 27    |
| Evren ve Örneklem .....                                                  | 27    |
| Veri Toplama Süreci .....                                                | 30    |
| Ölçme Araçları .....                                                     | 30    |

|                                                                           |    |
|---------------------------------------------------------------------------|----|
| BÖLÜM IV .....                                                            | 31 |
| BULGULAR.....                                                             | 31 |
| Çalışma I.....                                                            | 31 |
| Ölçeğin Formatı ve Madde Havuzunun Oluşturulması .....                    | 31 |
| Kapsam Geçerliliği .....                                                  | 31 |
| Açımlayıcı Faktör Analizi (AFA).....                                      | 31 |
| Yamaç-Birikinti Grafiği (Scree-Plot).....                                 | 33 |
| Güvenilirliğe İlişkin Bulgular .....                                      | 33 |
| Betimleyici İstatistikler, Normallik ve Madde Ayırt Edicilik Analizi..... | 34 |
| Çalışma II.....                                                           | 35 |
| Doğrulayıcı Faktör Analizi (DFA).....                                     | 35 |
| Ölçüt Bağıntılı Geçerlik .....                                            | 36 |
| BÖLÜM V .....                                                             | 38 |
| TARTIŞMA .....                                                            | 38 |
| BÖLÜM VI.....                                                             | 41 |
| SONUÇ VE ÖNERİLER.....                                                    | 41 |
| KAYNAKÇA.....                                                             | 44 |
| EKLER.....                                                                | 58 |
| Ek1. Bilgi Formu ve Ölçme Araçları SSFÖ Öğeleri ve Puanlama .....         | 58 |
| Ek2. İzinler .....                                                        | 60 |
| Ek3. Öz Geçmiş .....                                                      | 61 |

## TABLO LİSTESİ

|                                                                                                              | Sayfa |
|--------------------------------------------------------------------------------------------------------------|-------|
| Tablo 1. Ölçeğin Uygulandığı 1. Çalışma Grubundaki Öğrencilerin Demografik Bilgileri .....                   | 28    |
| Tablo 2. Ölçeğin Uygulandığı 2. Çalışma Grubundaki Öğrencilerin Demografik Bilgileri .....                   | 29    |
| Tablo 3. Döndürülmüş Bileşen Matrisi Sonuçları .....                                                         | 32    |
| Tablo 4. Betimleyici İstatistikler, Güvenirlilik, Normallik Testi ve %27 Alt Grup-%27 Üst Grup T-Testi ..... | 34    |
| Tablo 5. Model Uyum İndisleri .....                                                                          | 35    |

## ŞEKİL LİSTESİ

|                                                       | Sayfa |
|-------------------------------------------------------|-------|
| Şekil 1. Yamaç – Birikinti Grafiği (Scree-Plot) ..... | 33    |
| Şekil 2. Ölçüm Modeli .....                           | 36    |
| Şekil 3. Ölçüt Bağıntılı Geçerlik .....               | 37    |



## KISALTMALAR

AB: Avrupa Birliđi

AFA: Aımlayıcı Faktör Analizi

BTK: Bilgi Teknolojileri ve İletişim Kurumu

BÖTE: Bilgisayar ve Öğretim Teknolojileri Eğitimi

DFA: Doğrulayıcı Faktör Analizi

DVGÖ: Dijital Veri Güvenliđi Farkındalıđı Ölçeđi

EGM: Emniyet Genel Müdürlüğü

EİK: Elektronik İmza Kanunu

FSEK: Fikir ve Sanat Eserleri Kanunu

IP: İnternet Protokol Adresi

MEBS: Muharebe Elektronik Bilgi Sistemleri

SPSS: Sosyal Bilimler İçin İstatistik Programı

SSFÖ: Siber Su Farkındalık Ölçeđi

TCK: Türk Ceza Kanunu

UDHB: Ulaştırma, Denizcilik ve Haberleşme Bakanlığı

USOM: Ulusal Siber Olaylara Müdahale Merkezi

YEM: Yapısal Eşitlik Modellemesi

## BÖLÜM I

### GİRİŞ

#### Problem

Siber suçlar, bir bilişim sisteminin güvenliğini ve buna bağlı kullanıcı verilerini hedef alan suçlardır (EGM, 2020). Siber suçları diğer suçlardan ayıran en temel özellik bir bilişim sistemi olmadan işlenememesidir. Bundan dolayı bu suç türü bilgisayar ve internetle işlenen suçlar olarak da adlandırılmaktadır (EGM, 2020). Günümüzde çok fazla internet ve bilgisayar kullanıcısı olduğu bilinmektedir ve kullanıcı sayısı arttıkça da siber suç oranlarında artış gözlemlenmektedir. Geçmişten bu günümüze kadar insan yaşamını kolaylaştıran teknolojik gelişmeler günümüzde artmaya devam etmekte ve bu artan teknolojik gelişmeler işlerimizi kolaylaştırdığı kadar ciddi sorunlara da neden olabilmektedir. Bu sorunlarla başa çıkabilmek için öncelikle potansiyel sorunların farkında olmamız gerekmektedir. Siber suç vakaları son zamanlarda ülkemizde de çok fazla artış gösterdiği için Emniyet Genel Müdürlüğüne bağlı olarak Siber Suçlar Daire Başkanlıkları ve Müdürlükleri kurulmuştur.

İnsanoğlunun bulunduğu tüm alanlarda bilişim sistemlerinin kullanımı bilinmekte ve yaygın olarak her yerde kullanılmaktadır. Bundan dolayı, bilişim sistemleri daha çeşitli insan faaliyetlerini mümkün kılmaktadır. Örneğin, insanların günlük işlerinin hızını artırmakta, insanların yeni ve genellikle daha faydalı ilişkiler geliştirmesine ve sürdürmesine imkan tanımakta, kuruluşların yapısını ve işleyişini etkilemekte, satın alınan ürünlerin özelliklerini değiştirmekte ve işin tüm doğasını etkilemektedir. Bu anlamda bilişim sistemleri hayati ekonomik kaynaklar hâline getirmektedir. Bu durum sonuç olarak yeni fırsatlar doğurmakla birlikte, bilgi sistemlerinden sürekli yararlanma ihtiyacı, yeni tehdit ve sorunları da beraberinde getirmektedir. Bundan dolayı sıklıkla rastlanan sorunlardan birisi de siber saldırılar ve suçlardır. Siber saldırılar genellikle "bilgisayar korsanlarının bir bilgisayar ağına veya sistemine zarar verme veya yok etme girişimi" olarak tanımlanmaktadır ve bu tanımlamalar siber saldırılar arttıkça günden güne farklı tanımlamalarla artış göstermektedir (Cengiz,2021).

Bilişim sistemleri, hayatı ve insanların işini kolaylaştırma adına sağladıkları tüm olanakların yanında, güvenlik ve gizlilik boyutunda da yeni kaygı ve endişelerin gelişmesine sebep olmaktadır. Bu dijitalleşen dünyada, mağdur olan bireyle aynı yerde

bulunmaya gerek duymadan hırsızlık, dolandırıcılık, sahtekarlık, hakaret, özel hayatın gizliliğini ihlal, kişisel bilgilerin ele geçirilmesi gibi suç türleri mümkün hale gelmiştir. Bunun yanında bilişim sistemleri ile, suç gruplarının veya terör örgütlerinin iletişim imkanlarını artırmış olup, propaganda imkânlarını güçlendirmiş ve yeni durumların ve sorunların ortaya çıkmasına imkan sağlamıştır.

Siber suç olayları arttıkça yeni siber suç türleri de ortaya çıkmaktadır. Diğer taraftan, siber suçların diğer suçlara göre daha çok değişkenlik gösterdiği ve siber suç türlerinin sürekli kendini güncellediği görülmektedir. Bu durum yasal boşlukların ortaya çıkmasına neden olarak ekonomik, sosyal ve toplumsal, maddi zararlar açabilmektedir. Bu nedenle, siber suçlar ile ilgili yasaların ayrıntılı bir şekilde derlenip toparlanması ilerde çalışmacılara yol gösterici olacaktır (Budak, 2015). Bu kanuni düzenleme çalışmalarında hızlı bir şekilde hareket edilmesi, ülkelerin gelişmişlik düzeyi ile ilgili olduğu öne sürülmektedir. Siber uzay alanında yapılması gereken tüm hukuki düzenlemelerin çoğu ülkeler tarafından geç de olsa yapılmaya başlanmış olup ama yetersiz kaldığı ifade edilmektedir. Ülkemizde siber suç ile ilgili konu biraz daha geç ele alınmış olduğundan dolayı siber suç alanında çok büyük sorunlar ortaya çıkmaktadır.

Dünyada ve ülkemizde siber saldırı ve tehditler hatta siber savaşlar giderek artarken bireyler siber ortama daha bağımlı hale gelmektedir. Bu durum pek çok siber suçun habercisi olmaktadır. Bu nedenle bireylerin siber suç ve siber saldırılar konusunda farkındalıklarının geliştirilmesi gerekmektedir. Bireylerin bu konuda eğitilmesi ve siber suç farkındalıklarının arttırılması siber saldırı ve tehditlere karşı önlem almalarını sağlayacaktır. Siber suç farkındalığının oluşturulması ise bireyleri bilişim sistemi üzerinde yapılan işlemlerin hangilerinin mevcut siber suç mevzuatına göre suç kapsamına girdiği hangilerinin ise girmediği konusunda bilinç oluşturacaktır.

Dijitalleşmeye doğru giden bu dünyada toplumsal hayatımızda yer alan geleneksel suçlar da siber ve sanal ortama taşınarak siber suç başlığı altında değerlendirilmektedir. Siber suçlar, bilgisayar ve sistem casusluğu, casus yazılım ve diğer türlerle sürekli artışla birlikte artık büyük bir uluslararası sorun olarak kabul edilmekte ve bu sorun günden güne artış göstermektedir. Siber suçlarla ilgili kabul edilse de gerçekte ne anlama geldiği yeterince anlaşılmadığı için etik sorunları da beraberinde getirmektedir. İnternet bağlantılı bilişim sistemleri daha geniş coğrafyalara yayıldıkça, dünyadaki siber suç türleri ve olayları da artış göstereceği öne sürülmektedir.

Bilişim ortamında siber suçlarla ilgili karşılaşılan sorunlardan bir diğeri ise siber suç u işleyen kişilerin bulunmasına yönelik zorluklardır. Siber ortamda kişisel kimliğini saklayarak siber ortama erişimlerini ve etkileşimlerini arttırmaktadırlar ve kişilere kendilerini yeniden keşfetme imkânı sağlayarak onları gerçek kimliklerinden uzaklaştırarak yeni sanal kişilere dönüştürmektedirler. Bu durum siber ortamda yer alan suçlunun bulunmasını da zorlaştırmaktadır.

Siber saldırı girişiminde bulunanlar genel olarak siber suçları işledikleri zaman kişi, kurum ya da devletler gibi birçok kaynağa zarar verebilmektedirler. Bu zararları kısaca belirtecek olursak; kişilerin banka bilgilerine erişim, özel hayatın gizliliğini ihlal, dolandırıcılık, hakaret, kişisel bilgilerin ele geçirilmesi gibi durumlarda ortaya çıkabilecek risklere karşı siber güvenliğin sağlanmasının zorunlu hale gelmesi gerekmektedir.

Telif hakkı ihlalleri, müstehcenlik, hakaret, interaktif dolandırıcılık, kişisel verilerin çalınması, haberleşmenin engellenmesi, banka/kart bilgilerinin ele geçirilmesi gibi suçlar en sık rastlanan siber suçlar arasındadır (İlbaş ve Köksal, 2011). Bu suçlara maruz kalmamak için bilişim sistemleri ve bilgi güvenliği konusunda bireysel ve kurumsal düzeyde politikalar geliştirilmesi gerekmektedir (Whitman ve Mattord, 2012).

Ülkeler arasında ve ülke içinde gerçekleştirilen siber saldırılar, tehditler yaşamımızı ve ekonomik durumumuzu olumsuz yönde etkilemektedir. Bu durumdan dolayı dünya üzerinde yer alan ülkeler arasında ve ülkemizde gerçekleşen siber saldırı ve siber suç konusu hakkında duyarlı olunması, aynı zamanda ülkeler arasında ortaya çıkacak problemler karşısında birtakım önlemler alınmasını işaret etmektedir. Bu durumlardan dolayı siber saldırı, siber tehdit ve siber suç sorunu dünya çapında büyük sorunlardan biri olarak öngörülmektedir. Siber suç üzerine literatürde yapılmış çalışmalar incelendiğinde siber suçla ilgili literatürde birçok yapılmış çalışma bulunmasına rağmen bireylerin siber suç farkındalığını ölçmeye yarayan bir ölçek geliştirme çalışmasına rastlanılmamıştır. Bu nedenle bu çalışmada bireylerin siber suç farkındalığını ölçmeye yönelik bir ölçek geliştirme çalışmasına rastlanılmamıştır. Bu nedenle bu çalışmada bireylerin siber suç farkındalığını ölçmeye yönelik bir ölçek geliştirme çalışması yapılması planlanmıştır. Bu tez çalışması sonunda geliştirilen siber suç farkındalık ölçeği bireylerin siber suç hakkında ihtiyaçlarını ortaya koyarak siber suç farkındalığını

arttıracığı aynı zamanda yeni çalışmalar geliştirmek isteyen çalışmacılara yol gösterici olacağı düşünülmektedir.

### **Amaç**

Siber suçlar ile ilgili yapılmış çalışmalar incelendiğinde literatürde birçok çalışmaya rastlanmıştır olsa da bireylerin siber suç farkındalık düzeylerini ölçmeyi amaçlayan ölçek geliştirme çalışmalarının sınırlılık arz ettiği görülmektedir. Mevcut çalışmalardan farklı olarak bu çalışmada Türk Ceza Kanunu'nda belirtilen siber suçlar dikkate alarak bireylerin siber suç farkındalık düzeylerini ölçmeye yönelik bir ölçek geliştirme çalışması yapılması amaçlanmıştır. Bu tez çalışması sonunda geliştirilen siber suç farkındalık ölçeğinin bireylerin siber suç farkındalık düzeylerini belirleyerek yeni çalışmalar yapmak için çalışmacılara yol gösterici olması beklenmektedir.

Siber suçlar günümüzde teknolojik aletlerin ve internetin kullanıma bağlı olarak hızla yaygınlaşırken bireylerin siber suç farkındalık düzeylerini ölçen ölçeklere rastlansa da Türk Ceza Kanunu'nda belirtilen siber suçları dikkate alan bir ölçek aracına rastlanmamıştır. Bu çalışmanın literatürde yer alan bu boşluğa katkı sağlayacağı düşünülmektedir. Bu araştırmanın amacı bireylerin siber suç farkındalık düzeylerini ölçen bir ölçek geliştirilmesi, geliştirilen ölçek aracının geçerlik ve güvenirlik çalışmasının gerçekleştirilmesidir.

### **Önem**

İnternet kullanımının günden güne artmasından ötürü siber suç olaylarında da önemli bir artış yaşanmakta ve bu durumda siber suçlarla mücadelede ileri derecede zorluklar ortaya çıkarmaktadır (Bansal, 2018). Tüm bireysel ve kurumsal kullanıcıların dışardan gelecek her türlü siber saldırı ve tehditlere karşı gerekli güvenlik önlemlerini alabilmesi için öncelikle siber suçların neleri kapsadığı konusunda farkındalık sahibi olması gerekmektedir (Peker, 2010). Bu nedenle, siber suçlar konusuna farkındalık geliştirilerek gerekli önlemlerin alınması, siber saldırı ve tehditlerden zarar görmemek için son derece önemlidir (Özcan, 2004).

Siber suçlarla ilgili alınan yasal önlemlerin siber suçları önleme konusunda tek başına yeteri kadar etkili olmadıkları anlaşılmaktadır (Dülger, 2012). Alınan yasal önlemlerin yanı sıra kullanıcılar siber suçlar konusunda bilinçlendirilmeli ve detaylıca aydınlatılmalıdır. Siber suçlardaki artışının önüne geçebilmek için siber suçların kapsamı

hakkında kullanıcılara, özellikle gençlere, bilgilendirmeler yapılmalıdır (Bayram ve Saylı, 2013). İnternet ve bilgisayarla iç içe olan gençler siber ortama rahat bir şekilde uyum sağlarlar ve bilinçsiz kullanım siber suçlarla tanışmalarına neden olabilir, bu nedenle kullanıcılar siber suçlar konusunda bilinçlendirilmelidir (Budak, 2015). Siber suça daha çok kadınların maruz kaldığı ve bu nedenle kadınların siber suç türleri ve faaliyetleri konusunda daha çok bilinçlendirilmesi gerektiği ifade edilmektedir (Chel, 2018).

Siber suçlar, teknolojik ve bilişim sistemlerinin günden güne gelişmesiyle ve bilişim sistemleri ile çeşitlilik kazandığı düşünülürse yapılan bu araştırmanın güncelliği günümüz şartlarında yer alan tüm siber suçları gün yüzüne çıkararak bu konuda neler yapılması gerektiği hakkında bireysel ve devlet nezdinde alınacak tedbirler için fikir vermektedir (Budak, 2015).

Siber Suçlarla Mücadele Daire Başkanlığı web sayfasında yer alan siber suç türleri şunlardır: Verilere yönelik suçlar, online örgütlü kumar, zararlı yazılımlar (Bot-Net/ D-DOS saldırıları), bilişim sistemine girme, sistemi engelleme, bozma, haberleşmenin gizliliğini ihlal, verileri yok etme veya değiştirme, özel hayatın gizliliği, kişisel verilerin kaydedilmesi, nitelikli hırsızlık, nitelikli interaktif dolandırıcılık, banka ve kredi kartı suçları, hakaret, haberleşmenin engellenmesi, elektronik sertifikalarda sahtekarlık, e-imza verilerinin izinsiz kullanımı, telif hakkı ihlali, katalog suçlar ve erişimin engellenmesi ve hekleme siber suç türleridir (EGM, 2020). Bu siber suç türlerine göre ölçek maddeleri oluşturulmuş ve analizler yapılmıştır. Analiz sonuçlarına göre hangi siber suç türüne daha fazla ağırlık verileceği ve kurumlar çalışmalarını ona göre şekillendirmeleri ve fikir edinmeleri açısından bu çalışma büyük önem arz etmektedir. Aynı zamanda bireylerin ve araştırmacıların bilmedikleri siber suç türlerinin neler olduğunu öğrenmelerine katkı sağlayacaktır.

Siber saldırı ve tehditleri önleyebilmek için özel işletmeler (bankalar gibi) ve devlet kurumları (kolluk kuvvetleri (asker, polis), adli ve idari kuruluşlar) bilgi güvenliği uzmanı, siber güvenlik uzmanı, adli bilişim uzmanı ve yönetim bilişim sistemleri uzmanı istihdam etmektedir. Bu kişiler bilişim sistemleri ve teknoloji sürekli geliştiği için siber olayları ve tehditleri önlemek için yeni yazılımlar geliştirmekte ve verileri daha güvenli hale getirmeye çalışmaktadırlar. Aynı zamanda Emniyet Genel Müdürlüğü içerisinde yer alan Siber Suçlarla Mücadele Daire Başkanlığı ve Genelkurmay Başkanlığına bağlı

MEBS ve Siber Savunma Komutanlığı siber suçları önlemek için siber saldırı ve tehditlere karşı kurulan kurumlardır. Bu kurumlara istihdam edilen ve edilmekte olan bilişim uzmanları bu çalışmada çıkan analiz sonuçlarını inceleyerek siber olaylara ve hangi siber suç türüne yönelik yazılım geliştirmeleri konusunda kolaylık sağlayacağı yönünde yol gösterici bir çalışmadır. Aynı zamanda bu çalışma bu kurumlarda çalışan diğer personellerin ise siber suç konusu hakkında daha fazla fikir edinmelerine aracı olup bu çalışma baz alınarak bu kurumlardaki çalışanlara eğitim verilebilir. Bu çalışma siber suçla ilgilenen kurumların hangileri olduğunu bilmeyenler için fikir sahibi olmalarına katkı sağlayacaktır.

Türkiye’de siber suç ve türlerine yönelik çalışmalar yürütölmeye başlanmıştır. Ancak internet ağı ve bilişim sistemlerinin hızlı gelişimi teknolojiyle kıyaslandığında, bu yapılan çalışmaların az ve yetersiz kaldığını işaret etmektedir. Siber suçlarla mücadele noktasında özellikle genç neslin bilinçlendirilmesi yönünde adımlar atılmalıdır. İnternet kullanımının özellikle gençler arasında yaygın olması ve gençlerin kendini farklı gösterme çabası onları bilerek ya da bilmeyerek bilişim suçlarına karışmalarına neden olmaktadır. Bu noktadan hareketle gençlerin internet ve sosyal medya bağımlılığı, yapılan bilişim suçlarının neler olduğu, suçların hukuki yaptırımlarının ne gibi sonuçlar doğuracağı vb. konularda bilgilendirme çalışmalarının yapılması son derece önemlidir. Bu yapılan siber suç farkındalığı çalışması gençlere siber suç konusu hakkında yol gösterici olacağı düşünülmektedir (Lafvermez, 2018).

Bu çalışmada siber suç farkındalığı ile ilgili, bireylerin siber suçlara ilişkin yasal düzenlemeler ve işlemlere ilişkin algıları ve siber suç türleri konularını da içeren kapsamlı bir siber suç farkındalık ölçeğı hazırlanmıştır. Hazırlanmış olan bu ölçeğın sorularının siber suçlar konusunda daha sonra yapılacak olan çalışmalarda faydalanılabilecek olması açısından önemli olduğu söylenebilir (Yılmaz, 2018).

Siber suç farkındalığı konusunda yapılan bu çalışmanın birçok yönden önemli olduğu ifade edilebilir. Siber suç bireylerin günlük yaşamlarında ve bilişim ortamlarında herhangi bir endişe, korku, kaygı vb. hissetmeksizin ya da kendilerine karşı bir tehdit algılaması görmeksizin rahat bir biçimde davranabilmelerini engelleyen bir durumdur. Her an bir siber suçun mağduru olma ihtimali ile yaşayan bireylerin sosyal ya da bilişim ortamlarında yeterince özgür olabileceklerini söylemek çok da mümkün değildir. Bundan

dolayı bu çalışma bireylerin siber suç farkındalık düzeylerinin ortaya konulması açısından önemlidir (Yılmaz, 2018).

“Web of Science” veri tabanında 1975 yılından günümüze kadar olan yayınlar incelendiğinde başlığında “cyber crime” (siber suç) ve “cybercrime” ifadesi geçen toplam 1004 yayın (448 makale) bulunmaktadır. Diğer taraftan, “Google Akademik” veri tabanında ise 1996 yılından günümüze kadar makale başlığında “siber suç” ifadesi bulunduran 32 yayın (9 makale) mevcuttur. Alan yazında yer alan Türkçe çalışmaların siber suç farkındalığına odaklanılmadığı görülse de dijital veri güvenliği farkındalığı ve bilgi güvenliği farkındalığı konularında ölçek geliştirme çalışmalarına rastlanmaktadır. Siber suç farkındalığını ölçen Türkçe bir ölçek aracına rastlanılmamıştır. Bu nedenle bu ölçek geliştirme çalışması özgün bir çalışma olup literatürde bu alana önemli bir katkı sağlayacağı düşünülmektedir.

### **Sınırlılıklar**

- Bu çalışmanın örneklemi Tokat Gaziosmanpaşa Üniversitesinde 2020-2021 yıllarında öğrenim gören üniversite öğrencileri ile sınırlıdır.
- Araştırma geliştirilen veri toplama araçlarıyla elde edilen veriler ile sınırlıdır.
- Bu çalışmada geliştirilen ölçek aracının maddeleri ve alt boyutları Türk Ceza Kanunu’nda yer alan siber suç türleri ile sınırlıdır.

### **Tanımlar**

**Bilgi güvenliği:** Bilgi güvenliği siber ortamda kişiye ait bilgilerin ve verilerin korunması, saklanması vb. gibi durumları içermektedir. Bilgi güvenliği pek çok organizasyon için ise bilişim sistemlerinin korunması, bilgilerin saklanması, bilgilerin güvenliğinin sağlanması ve zararlı kullanımlara karşı korunması ifade edilmektedir (Eminağaoğlu ve Gökşen, 2009).

**Bilgi güvenliği farkındalığı:** Bilişim sistemi kullanıcıları tarafından bilgi güvenliğinin öneminin algılanması gerektiği, alınması gereken sorumluluklar, kurumlara uygun bilgi güvenliği seviyesi ve davranışları olarak ifade edilmektedir (Kruger ve Kearney, 2006).

**Bilişim sistemine yönelik suçlar:** Siber suç mevzuatında ve TCK’nda kabul edilen bilişim sistemine erişme, sistemi bozma, durdurma, engelleme, yok etme gibi suçların yer aldığı suç türleridir.

**Dijital veri güvenliği:** Siber ortamdaki bilgilerin ve verilerin taşınması ve saklanması sırasında verilerin bütünlüğü bozulmadan, izinsiz erişimlerden korunması için güvenli bir bilgi işleme ortama oluşturulması olarak ifade edilmektedir (Canbek ve Sağıroğlu, 2006).

**Kişisel verilere yönelik suçlar:** Kişisel verilere yönelik olarak kişisel bilgilerin yok edilmesi, silinmesi, üçüncü şahısların eline geçmesi vb. suç türleri yer almaktadır.

**Özel hayatın gizliliği ve nitelikli hırsızlık:** Özel hayatın gizliliği, telif hakkı, lisanssız programların kullanımı, web sitesi, e-posta vb. suç türlerini içermektedir.

**Siber güvenlik farkındalığı:** Siber ortamda yer alan kullanıcı, kurum ve kuruluş verilerini korumak amacıyla kullanılan elektronik araçların ve programların eğitim verilerek farkındalığının oluşturulması olarak ifade edilmektedir (Yılmaz ve Sağıroğlu, 2013).

**Siber güvenlik:** Bilgi sistemlerinde ve siber ortamda çalışmaların sürekliliğini sağlamak, kişisel verilerin korunması, gizliliğin güvence altına alınması, bilgi iletişim ve sistemlerinin yetkisiz ve kötüye kullanımını önlemek amacıyla teknik ve idari bir araçtır. Bunlar bireyleri ve kullanıcıları siber alandaki risklerden ve zararlı durumlardan korumak için alınan önlemlerdir. Siber güvenlik, devletlerin ve bireylerin elinde, özellikle siber savaşın teknolojik savaş taktikleri ve devletlerarası saldırı taktiklerinin ayrılmaz bir parçası haline geldiği için önemli bir silah olarak ifade edilmektedir (Idan, 2020).

**Siber saldırı:** Bilişim sistemlerinin güvenlik alt yapısına zarar vermek veya siber ortamda bulunan kişi veya kişilerce bilgisayar ve internet yani bilişim sistemleri kullanılarak gerçekleştirilen eylemler, saldırılar siber saldırı olarak ifade edilmektedir (UDHB, 2016).

**Siber:** Bilgisayar ve internet gibi bilişim sistemlerinde kullanılan her türlü aygıtın bir bütün olarak birleşiminden oluşan sistemlerin ağ (network) yardımıyla iletişimini sağlayan elektronik ortamdır (Sağıroğlu, 2018).

**Siber suç:** 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 (EGM, 2020).

**Siber tehdit:** Bilişim sistemlerine zarar vermek amacıyla bilgi ve iletişim teknolojileri kullanılarak gerçekleştirilen, bilişim dünyasındaki her türlü ağıta zarar vermek,

engellemek, bozmak, verileri ele geçirmek amacıyla gerçekleştirilen siber saldırıların siber ortamda kullanılması olarak adlandırılmaktadır (BTK, 2009).

Siber suç farkındalığı: Bireylerin siber suç hakkında bilinçlilik düzeyi olarak ifade edilmektedir (Budak, 2015).

Siber zorbalık: Başkalarına zarar vermeye yönelik saldırganca davranışların tekrarlayan biçimde ve kasıtlı olarak elektronik ve bilişim araçlarıyla elektronik ortamda gerçekleşmesidir (Tokunaga, 2010). Siber zorbalık kavramının yerine bazen e-zorbalık, elektronik zorbalık, siber şiddet, siber taciz, dijital şiddet, dijital zorbalık vb. gibi kavramların da eş anlamlı olarak kullanıldığı ifade edilmektedir (Hinduja ve Patchin, 2015; Pekşen Süslü, 2016).

## BÖLÜM II

### KAVRAMSAL ÇERÇEVE

#### Farkındalık

Farkındalık, sosyal grupların ve bireylerin çevreye karşı bilinçli ve duyarlı olmaları olarak ifade edilmektedir (Keleş, 2007). Farkındalık düzeyindeki artış ile bireyin kendine ve çevresine ilişkin bilinçli olma durumunda artış olur (Arpaci ve Gundogan, 2021). Bireyin davranışlarını yönlendiren düşünceleri ve duyguları ile ilgili farkındalık düzeylerinin arttırılması mümkündür (Engin ve Çam, 2005). Bir başka bir ifadeyle farkındalık, bireyin tüm duyu organlarıyla, başka birey veya çevresiyle temasa geçerken neyi, nasıl yaşadığının ayırında olmasıdır (Voltan-Acar, 2004).

Bir doğu felsefesi olan farkındalık ilk kez John Kabat-Zinn (1982) tarafından ortaya çıkarılan ve yaklaşık kırk yıla yakın süredir Batıda bir psikoterapi uygulama yöntemi olarak kullanılan bir kavramdır (Arpaci, 2021). Kökeni Doğunun kişisel gelişimin durumuna dayanan farkındalığı, psikolojik süreçler alanında açıklamaya çalışan birden fazla çalışma olduğu görülmektedir (Çatak ve Ögel, 2010). Farkındalık kavramını Doğunun gelenekleriyle yakın ilişkisinden ziyade psikolojik bir süreç olarak tanımlama çabaları da görülmektedir (Bishop vd., 2004; Shapiro vd., 2006).

Farkındalık konusu özellikle duygu ve düşüncelerin incelenmesi yönüyle ilgili olarak Gestalt psikolojisi ve bilişsel-davranışçı yaklaşım kapsamında detaylıca ele alınmıştır (Akkoyun, 2001; Dökmen, 2000). Farkındalık, “sağlıklı kişinin ayırt edici özelliği ve tedavi hedefi” olarak görüldüğü için Gestalt Terapisinin en önemli unsurlarından biridir (Seligman, 2006). Bireyler farkında oldukları zaman kendi davranışlarını düzenleyebilirler (Arpaci vd., 2019). Temaslı farkındalık, çevremizdeki kişilerle iletişim kurma durumuna temas halinde olma olarak ifade edilir. Ayrıca farkındalık duyuşsal, bilişsel (bilgi) ve duygusal olarak düşüncelerimizi duygularımızı ve hislerimizi kapsar ve bu durumdan dolayı Gestalt’ın alt yapısını oluşturan fenomenolojik-varoluşsal alanda birincil olarak yer alır (Intawa, 2011).

Farkındalıkla ilgili yapılan çalışmaların bir bölümünde üst biliş (bilgi), duygu düzenleme, dikkat düzenleme ve içsel maruz bırakma kavramları yer almaktadır (Çatak ve Ögel, 2010). Farkındalıkta yer alan üst biliş (bilgi) düşüncelerin gerçeklikle aynı olarak

değerlendirmeye alındığı nesnel bilgi işleme düzeyinden ayrılmayı sağlamakta ve üst bilişsel bilgi işlemeye geçildiği ifade edilmektedir (Çatak ve Ögel, 2010).

Farkındalık içerisinde incelenen bir diğer kavram ise duygu düzenlemedir. Farkındalıkta duygusal düzenlemelerin olumlu bir etkisinin bulunduğu ve duygusal alanda iyileşme sağlandığı şeklinde ifade edilmektedir (Lynch ve Bronner, 2006; Hayes ve Feldman, 2004; Coffey ve Hartman, 2008; Roemer vd., 2008; Mitmans-Gruber vd., 2009). Farkındalığın duygu düzenleme üzerindeki etkilerine ilişkin bir diğer ifade ise duygusal tolerans ile ilgili olduğu açıklanmıştır ve bu ifadeye göre ise farkındalık, istenmeyen durumları kabul etmeyi sağlamakta ve olumsuz olan duygulara karşı tolerans kapasitesini arttırdığı ifade edilmektedir (Çatak ve Ögel, 2010).

Farkındalıkta dikkat düzenleme kavramı da detaylıca incelenmiştir. Dikkatin istemli olarak anlık yaşantılara odaklandığı ifade edilmektedir. Bundan dolayı farkındalığın birden fazla tanımlarında dikkat, farkındalığın temel bir yapıtaşı olarak ifade edilmektedir (Teasdale vd., 1999; Bishop vd., 2004). Birkaç çalışmada farkındalığın dikkatin fiziksel ve duygusal iyi olma halleri ile olumlu, depresyon ve kaygı belirtileriyle ise olumsuz ilişkisinin olduğu ortaya çıkmıştır (Brown ve Ryan, 2003; Zvolensky vd., 2006). Farkındalığın birden fazla dikkat üzerindeki etkilerini inceleyen çalışmalarda literatürde mevcuttur (Anderson vd., 2007; Chambers vd., 2009; Schmertz vd., 2009). Bu çalışmalarda yer alan bölümlerde farkındalığın sürekli dikkati arttırdığı ifade edilmektedir (Chambers vd., 2009). Diğer taraftan, farkındalığın sürekli dikkat kapasitesini artırıcı bir etkisi olmadığını savunan çalışmalar da mevcuttur (Anderson vd., 2007; Schmertz vd., 2009).

Farkındalık, yargı veya hiçbir beklenti olmaksızın ortaya konan, bireyin dikkatini yaşanan zamana göre yönlendiren dikkat düzenleme işlemidir (Ford, 2016). Farkındalık, dikkatin istemli olarak ve yargısal olmayarak anlık deneyim ve tecrübelerin akışına yöneltilmesidir (Kabat – Zinn, 2003). Farkındalık teorisinde yer alan dikkat aynı zamanda içsel, dışsal ve uzlaşımsal farkındalık olarak tasnif edilmektedir (Psikosentez, 2018). İçsel farkındalık, bireyin kendi kendinin farkında olması ve kendi kendini algılaması olarak tanımlanmaktadır. İçsel farkındalığın seviyeleri ise şunlardır (Psikosentez, 2018); duyum ve davranışların farkına varma, duyguların farkına varma, isteklerin farkına varma ve değer yargılarının farkına varma.

Dışsal farkındalık, diğer bireylere ve dış çevreye ilişkin farkındalık olarak ifade edilmektedir (Psikosentez, 2018). Uzlaşımsal farkındalık, içsel ve dışsal farkındalığın bileşimidir. İçsel yaşantılar ve dışsal (çevresel) faktörlerle ilgili farkındalıklar bilişsel bilgi olarak biçimlendirilir ve anlamlı hale getirilir. Anıların, düşüncelerin ve hayallerin bu alanda yer aldığı ifade edilmektedir (Psikosentez, 2018).

Farkındalık, duyuşsal yönden hissedilen duygunun ifade edilmesi, bu duyguların algılanmasındaki artış ile şekillenmektedir (Chambers, Gullone ve Allen, 2009). Farkında olma kavramı ise, bireyin kendi iç dünyasını (duygusal yönünü) ve dış dünyasını (davranışını) düzenli olarak gözlemleyen; farkındalığın arka plandaki yönlerin gelişmesini sağlayan bir görev olarak ifade edilmektedir (Brown ve Ryan, 2003).

Farkındalık, kişilerin içinde bulunduğu durumu özümsemesini ve anlamasını içermektedir (Baer, 2003; Bishop vd., 2004; Brown, Ryan ve Creswell, 2007; Leary ve Tate, 2007; Shapiro, Carlson, Astin ve Freedman, 2006; Verplanken ve Fisher, 2014). Farkındalık bireyin, bütün duyuşsal alanda yaşadığı anı anlamlandırması, bilgiden haberdar olması ve anlaması gereken duruma dikkat ederek özen göstermesi gerektiğini ifade etmektedir (İlhan ve Esentürk, 2015). Farkındalık, kişilerin tutumu ile davranışları arasındaki ilişkiyi etkileyen en önemli unsurlardan biri olarak görülmektedir (Demir ve Cicioğlu, 2020). Bu çalışmada, bireylerin siber suç farkındalık düzeylerini ölçmeyi amaçlayan ölçek maddeleri farkındalık teorisi dikkate alınarak geliştirilmiştir.

### **Siber Güvenlik, Bilgi Güvenliği Farkındalığı ve Yapılan Çalışmalar**

Literatür incelendiğinde bu alanda bilgi güvenliği, bilgi güvenliği farkındalığı, siber güvenlik ve siber güvenlik farkındalığı kavramlarının açıklamalarına ve bu kavramlarla ilgili literatürde yer alan çalışmalara yer verilmiştir.

Bilgi güvenliği, siber ortamda kişiye ait bilgilerin ve verilerin korunması, saklanması vb. gibi durumları içermektedir. Bu tanım kişisel olarak ele alınan güvenliği ifade etmektedir. Bilgi güvenliği pek çok organizasyon için ise bilişim sistemlerinin korunması, bilgilerin saklanması, bilgilerin güvenliğinin sağlanması ve zararlı kullanımlara karşı korunması ifade edilmektedir (Eminağaoğlu ve Gökşen, 2009). Bilgi güvenliği farkındalığı ise bilişim sistemi kullanıcıları tarafından bilgi güvenliğinin öneminin algılanması gerektiği, alınması gereken sorumluluklar, kurumlara uygun bilgi güvenliği seviyesi ve davranışları olarak ifade edilmektedir (Kruger ve Kearney, 2006). Diğer bir kavram olan siber güvenlik kavramını da değinecek olursak siber güvenlik, internetin yaygınlaşması ve gündelik veri iletişiminin hızlıca dijitalleşmesi neticesinde ortaya çıkmış bir kavram olarak ifade edilmektedir. 1991’de internetin sivil kullanıma yaygın olarak açılması ve gelişen bilgisayar teknolojisi bireylerin fiziksel dünyadaki bağlantılarına dijital ve sanal ortamı eklemiştir. Bugünlerde ‘siber uzay’ adını verdiğimiz bu alan 2000’li yıllarda gelişen telekomünikasyon teknolojisiyle birlikte etkili biçimde hayatımıza girmiştir (Bıçakcı, 2019). Bu çalışmada bir diğer önemli kavram ise siber güvenlik farkındalığıdır. Siber güvenlik farkındalığı, siber ortamda yer alan kullanıcı, kurum ve kuruluş verilerini korumak amacıyla kullanılan elektronik araçların ve programların eğitim verilerek farkındalığının oluşturulması olarak ifade edilmektedir (Yılmaz ve Sağıroğlu, 2013).

Cone vd. (2007) yaptıkları çalışmada siber güvenlik eğitimi ve farkındalığı için geliştirilen bir video oyununu incelemişlerdir. Betimleyici istatistiklerin sonuçları oyunun siber güvenlik eğitimi ve farkındalığı için çeşitli kuruluşlar tarafından kullanılabileceğini belirtmişlerdir ve temel farkındalık eğitim programlarına da katkısının olacağını ifade etmişlerdir. Diğer bir çalışmada Abawajy (2014) siber güvenlik farkındalığı sağlama yöntemlerini incelemiştir. Çalışmada metin tabanlı, oyun tabanlı ve video tabanlı yöntemler incelenmiştir. Çalışma sonuçları birleşik teslimat yöntemlerinin bireysel güvenlik farkındalığı oluşturmada daha etkili olduğunu ortaya koymuştur. Diğer bir çalışmada ise Kritzing ve von Solms (2010) yapmış oldukları çalışmada bireysel kullanıcılar için siber güvenlik farkındalık uygulaması yoluyla yeni bir koruma yöntemini

ele almışlardır. Çalışma sonuçlarına göre kullanıcıların siber güvenlik farkındalığı oluşturulmadan internet kullandıklarında birden fazla siber suça maruz kalabileceklerini ifade etmişlerdir. Başka bir çalışmada Yu vd. (2013) siber güvenlik farkındalığı için bulut bilişim tabanlı bir mimariyi ele alarak incelemiştir. Araştırma sonucunda siber güvenlik farkındalığını sağlayabilmek için izlenen cihazlardan gelen büyük verilerin depolanması ve işlenmesi gerektiğini ifade etmişlerdir. Siber güvenlik farkındalığı oluşturmak için bulut bilişim tabanlı bir mimari önermişlerdir. Korpela (2015) veri analitiği ile siber güvenlik farkındalığı ve eğitim programlarının geliştirilmesini incelemiştir. Farkındalık ve eğitimin siber suçlar konusunda geçerli önleyiciler olduğunu ve bu tür programları uygulamanın iyi ve kötü yönlerinin tartışılması gerektiğini ifade etmiştir. Başka bir çalışmada Al-Janabi ve Al-Shourbaji (2016) Orta Doğu'da eğitim ortamında siber güvenlik farkındalığı konusunu incelemiştir. Çalışmanın örneklemini lisans öğrencileri ve eğitim ortamında çalışan kişilerin oluşturduğunu ifade etmişlerdir. Bu çalışma sonucunda katılımcıların siber güvenlik farkındalığı konusunda gerekli niteliklere sahip olmadığını belirtmişlerdir. Benzer şekilde, Alotaibi vd. (2016) yaptıkları çalışmada Suudi Arabistan'daki siber güvenlik farkındalığını ele alarak incelemiştir. Çalışmanın amacı Suudi Arabistan'da internet ve mobil cihaz kullanımı arttığı için bu konuyu incelemiştir. Analiz sonucunda internet becerilerinin siber güvenlik uygulamaları üzerinde bir etkiye sahip olduğunu ve beceri düzeyi ile bölgedeki kuruluşlar tarafından uygulanan güvenlik önlemleri arasında bir ilişki olduğunu belirtmişlerdir. Siber suçla mücadelede yetersiz kaldıkları için ve siber güvenlik farkındalığı oluşturmak için bir model geliştirmeye ihtiyaç olduğuna değinmişlerdir.

Erol ve Sağıroğlu (2016) siber güvenlik farkındalığı için yetenek tabanlı bir model geliştirilmesini önermişlerdir. Bu modeli geliştirebilmek için farkındalığın ölçülmesine yönelik araştırmaların kişisel, kurumsal ve ulusal düzeyde yapılması gerektiğini ifade etmişlerdir. Diğer bir çalışmada Mokha (2017) siber suç ve siber güvenlik farkındalığı üzerine bir araştırma yapmıştır. Bu araştırmada günümüzde yaygınlaşan siber suç ve siber güvenlik konusunda farkındalık oluşturmayı amaçlanmıştır. Katılımcıların eğitim düzeyleri ile siber suç ve siber güvenlik farkındalık düzeyleri arasında anlamlı bir ilişki olduğu ortaya çıkmıştır.

Aksoğan vd. (2018) İletişim fakültesi öğrencilerinin siber güvenlik farkındalığını İnönü Üniversitesi örneğinde incelemiştir. Betimleyici istatistik sonucuna göre öğrencilerin çoğunluğunun siber güvenlik farkındalıklarının düşük çıktığını ifade

etmişlerdir. Cinsiyete, yaşa ve internette günlük geçirilen süreye göre verilen cevapların bazılarında anlamlı farklılıklar gözlemlendiğini, katılımcıların okudukları bölüme göre verilen cevaplar arasında ise anlamlı bir fark bulunmadığını belirtmişlerdir. Başka bir çalışmada Akgün ve Topal (2015) Sakarya Üniversitesi Eğitim Fakültesinde öğrenim gören son sınıf öğrencilerinin (n=259) bilişim güvenliği farkındalıklarını incelemişlerdir. Kesitsel tarama yöntemi ile yapılan bu çalışmada veri toplama aracı “Bilişim Güvenliği Anketi” kullanılmıştır. Katılımcıların bilişim güvenliği farkındalıklarının yeterli düzeyde olmadığı ifade edilmektedir. Cinsiyete ve ortalama bilgisayar-internet kullanım süresine göre anlamlı farklılıklar olduğunu gözlemlenmekle birlikte, bilişim güvenliği eğitimi aldığını belirten adaylar ile almayan adaylar arasında beklendiği gibi ciddi bir anlamlı farklılık gözlemlenmediğini ifade edilmektedir.

Aydaner (2019) genç tüketicilerin sosyal mühendislik ile siber güvenlik farkındalıklarının online alışveriş niyetleri üzerindeki etkisini incelemiştir. Bu çalışmanın örneklemini Bandırma On yedi Eylül Üniversitesinde okuyan 693 öğrenci oluşturmaktadır. Genç tüketicilerin sosyal mühendislik farkındalıklarındaki değişimin önemli bir kısmının siber güvenlik farkındalıklarında meydana gelen değişim tarafından açıklandığı tespit edilmiştir. Ayrıca öğrencilerinin bilgi güvenliği konusunda eğitimlere ihtiyaç duydukları ifade edilmiştir. Diğer bir çalışmada Tavlaş (2019) ortaöğretim kurumlarında uygulanan siber güvenlik farkındalık eğitiminin öğrenciler üzerinden etkisini incelemiştir. Bu çalışmanın örneklemini İstanbul’da yer alan ortaokullarda okuyan 211 öğrenci oluşturmaktadır. Sonuçlar uygulanan bilgi güvenliği farkındalık eğitiminin öğrencilerinin siber güvenlik ve siber zorbalık farkındalıklarına pozitif etkisi olduğunu göstermiştir. Başka bir çalışmada Özbek (2019) öğretmen adaylarının siber güvenlik farkındalıklarını incelemiştir. Sonuçlar öğretmen adaylarının kişisel siber güvenlik sağlama durumlarının orta düzeyde olduğunu göstermektedir. Ayrıca erkek öğretmen adaylarının kişisel siber güvenliği sağlama hususunda kadın öğretmen adaylardan daha duyarlı olduğu ifade edilmektedir. Öğretmen adaylarının akademik başarıları ve öğrenim gördükleri sınıf düzeylerine göre kişisel siber güvenliği sağlama durumları arasında anlamlı bir farklılık görülmediğini belirtilmiştir.

Hacımustafaoğlu (2019) ortaöğretim öğrencilerinin bilgi güvenliği farkındalık düzeyleri ile siber mağdur olma durumu arasındaki ilişkiyi İstanbul ili Üsküdar ilçesi örnekleminde incelemiştir (n=995). Çalışmada veri toplama aracı olarak “Bilgi Güvenliği Farkındalık Ölçeği, Siber Mağduriyet Ölçeği ve Kişisel Bilgi Formu” kullanılmıştır. Bu

çalışmanın sonuçlarına göre bilgi güvenliği farkındalık düzeyi ile siber mağdur olma durumu arasında herhangi bir ilişki olmadığı ifade edilmiştir. Diğer taraftan, siber mağduriyete maruz kalma durumunun cinsiyet ve internet kullanma süresi ile ilişkili olduğu ifade edilmiştir. Başka bir çalışmada Tekerek ve Tekerek (2013) öğrencilerin bilgi güvenliği farkındalık düzeylerini incelemişlerdir. Kahramanmaraş'ta öğrenim gören ilköğretim ve ortaöğretim öğrencilerinden oluşan 2449 kişiye Bilgi Güvenliği Farkındalık Ölçeği uygulanmıştır. Çalışmanın sonucuna göre katılımcıların bilgi güvenliği farkındalık seviyelerinin yetersiz olduğu tespit edilerek bu doğrultuda geliştirici çalışmalar yapılması gerektiği vurgulanmıştır. Benzer bir çalışmada Biber ve Biber (2018) ortaöğretim öğrencilerinin bilgi güvenliği farkındalıklarını incelemişlerdir. Bu çalışmanın örneklemini İzmir iline bağlı Mesleki ve Teknik Anadolu Liseleri, Anadolu Liseleri ve Temel Liselerde öğrenim gören 276 öğrenci oluşturmaktadır. Bilgi Güvenliği Farkındalık Ölçeği kullanılarak toplanan verinin bulgularına bakıldığında öğrencilerin bilgi güvenliği farkındalık düzeylerinin orta seviye altında olduğunu göstermektedir.

Gökçearslan, Günbatar ve Sarıtepeci (2021) ortaöğretim öğrencilerinin bilgi güvenliği farkındalıklarını incelemişlerdir. Çalışmanın örneklemini 359 kişiden oluşan 9-12. sınıf öğrencileri oluşturmaktadır. Öğrencilerin dijital okuryazarlık seviyeleri ile bilgi güvenliği farkındalıkları arasında pozitif bir ilişki olduğu tespit edilmiştir. Günlük internet kullanımı yedi saat ve üzeri olan öğrencilerin bilgi güvenliği farkındalığının diğerlerine göre daha yüksek olduğu bulunmuştur. Buna karşın sosyal medya kullanım süresinin öğrencilerin bilgi güvenliği farkındalık seviyelerinde anlamlı bir farklılık oluşturmadığı ifade edilmektedir. Ayrıca erkek öğrencilerin bilgi güvenliği farkındalık düzeylerinin kadın öğrencilerden daha yüksek olduğu belirtilmiştir.

Yılmaz, Şahin ve Akbulut (2016) öğretmenlerde dijital veri güvenliği farkındalığı konusunu incelemişlerdir. Bu çalışmanın örneklemini 2014-2015 eğitim öğretim yılında Balıkesir ilinde yer alan özel ve resmi okullarda görev yapan 870 öğretmen oluşturmaktadır. Veri toplama aracı olarak Yılmaz'ın (2015) yılında gerçekleştirdiği Dijital Veri Güvenliği Farkındalığı Ölçeğini (DVGFÖ) kullanılmıştır. Öğretmenlerin dijital veri güvenliği farkındalıklarının oldukça yüksek düzeyde olduğu ve farkındalık değerlerinin cinsiyet, günlük bilgisayar kullanım süresi, günlük İnternet kullanım süresi ve farklı teknolojilere sahip olma durumlarına göre farklılaştığı; ancak branş, öğrenim kademesi, öğrenim durumu ve mesleki kıdem bağlamında farklılık göstermediği bulunmuştur.

Bıkmaz (2017) sađlık ynetimi blm đrencilerinin mobil gvenlik farkındalıđı ve dijital veri gvenliđi farkındalıđını dzeylerini belirlemek istemiřtir. đrencilerin dijital veri gvenliđi farkındalıklarının kt amaçlı yazılımlar ve gvenlik yazılımlarından haberdar olma, uygulama yklerken gvenlik mesajlarına dikkat etme ve kiřisel verilere ulařılmak istenmesine dikkat etme durumlarına gre farklılařtıđı sonucuna ulařılmıřtır. Benzer bir alıřmada Korkmaz (2018) niversite đrencilerinin internet ve veri gvenliđi farkındalıklarını incelemiřtir. Seluk niversitesinde đrenim gren 400 đrenciden veri toplanmıřtır. Bu veriler baz alınarak yapılan analizlere gre kadın ve erkek đrencilerin verdiđi cevapların ortalaması arasında istatistiksel olarak anlamlı bir fark olduđu ortaya ıkıřtır. Diđer bir alıřmada Rezgui ve Marks (2008) yksekđretimde bilgi gvenliđi farkındalıđını incelemiřlerdir. Arařtırma sonularına bakıldıđında niversite alıřanlarının kiřilik zelliklerini, tutumlarını ve inan durumlarını ortaya koyarak bilgi gvenliđi farkındalıđını oluřturmak iin nerilerde bulunmuřlardır.

etin (2014) kullanıcıların bilgi gvenliđi farkındalık dzeylerini incelemiřtir. Kiřisel Veri Gvenliđi Farkındalıđı anketi ile Antalya ilinde yařayan 526 bireyden veri toplanmıřtır. Katılımcıların bilgi gvenliđi farkındalık dzeylerinin ortalamasının stnde olduđunu belirlenmiř, kiřisel veri paylařımı farkındalık dzeyinin diđer farkındalık dzeylerine gre daha yksek olduđu tespit edilmiřtir. Diđer bir alıřmada Lang vd. (2009) İrlanda'daki sosyal ađ ve kiřisel veri gvenliđini konusunda kamu bilincini incelemiřtir. alıřmanın sonucunda birok katılımcının veri yedekleme ve parola konusunda yeterli hassasiyeti gstermedikleri ortaya ıkmıřtır. Diđer bir alıřmada Nield vd. (2020) Avusturalya'daki tketicilerin veri gvenliđi farkındalıđını incelemiřlerdir. Arařtırma sonuları tketicilerin yksek dzeyde veri gvenliđi farkındalıđına sahip olduklarını ancak mevzuat konusunda dřk farkındalıđa sahip olduklarını ortaya koymuřtur. McCormac vd. (2017) bireysel farklılıklar ve bilgi gvenliđi farkındalıđını ele alarak incelemiřlerdir. rneklem olarak 505 Avusturyalı alıřandan veri toplamıřlardır. Sonular vicdanlılık ve anlařılabilirlik gibi faktrlerin bireylerin bilgi gvenliđi farkındalıđındaki varyansı anlamlı bir řekilde aıkladıđını fakat yař ve cinsiyete gre anlamlı bir fark olmadıđını gstermektedir.

Webb (2014) bilgi gvenliđi risk ynetimi iin bir farkındalık modeli geliřtirmiřlerdir. Bilgi gvenliđi risk deđerlendirmesi ve uygulamasında uygun olmayan gvenlik stratejilerine yol aan eksikliklerin tespit edilmesini sađlayan SA-ISRM modelini nerdiklerini ifade etmiřlerdir. Shaw vd. (2009) bilgi zenginliđinin bilgi

güvenliği farkındalık eğitiminin etkinliği üzerindeki etkisini incelemişlerdir. Araştırmada algılama, kavrama ve projeksiyon olmak üzere üç güvenlik farkındalığı düzeyi belirlemişlerdir. Bu üç bilgi güvenliği farkındalığı düzeyini arttırmak için multimedya ve hiper-metin tabanlı ortamlar kullanmışlardır. Deneysel çalışma sonucuna bakıldığında öğrencilerin multimedya materyali ile anlama ve projeksiyon düzeyinde daha iyi performans gösterdikleri söylenebilir. Başka bir çalışmada Avcı ve Arslan (2019) dijital veri güvenliği farkındalığı ve bilgi okuryazarlığı ile alınan hizmet içi eğitimin etkisini incelemişlerdir. Bu çalışmanın örneklemini ise 37 kadın ve 32 erkek personel oluşturmaktadır. 47 kişi daha önce bilgi ve dijital veri güvenliği eğitimi aldıklarını açıklamışlardır. Bu çalışmada veriler Bilgi Okuryazarlığı Ölçeği ve Dijital Veri Güvenliği Farkındalığı Ölçeği ile toplanmıştır. Analiz sonuçlarına göre bilgi okuryazarlığı ve dijital veri güvenliği farkındalığı arasında orta düzeyde bir ilişki çıktığını görülmüştür.

Şahinaslan, Kandemir ve Şahinaslan (2009) bilgi güvenliği farkındalık eğitimini ele almıştır. Kurumlarda bilgi güvenlik farkındalığı konusunda yöneticiden başlanarak en alt kademede çalışan personele kadar tüm çalışanlara eğitim ve seminerler verilmesi gerektiği ifade etmişlerdir. Kişisel ve kurumsal bilginin nasıl korunacağı hakkında tüm personelin fikir sahibi olması gerektiğini ifade etmişlerdir. Benzer bir çalışmada Bulgurcu vd. (2010) yapmış oldukları ampirik çalışmada bilgi güvenliği politikasına uygunluk, rasyonalite temelli inançlar ve bilgi güvenliği farkındalığını incelemişlerdir. Çalışma sonucunda bilgi güvenliği farkındalığının bilgi güvenliği politikasına uymaya yönelik tutum ve inançları pozitif etkilediğini bulmuşlardır. Şahinaslan vd. (2009) yapmış oldukları çalışmada kurumlarda bilgi güvenliği farkındalığı oluşturma yöntemlerini incelemişlerdir. Çalışanlara bilgi güvenliği hakkında rehberlik hizmeti, seminer ve eğitim verilmesi gerektiğini ifade etmişlerdir. Benzer bir çalışmada Yayla (2018) Fatih projesi uygulanan ve uygulanmayan okullardaki öğretmenlerin bilgi güvenliği farkındalık düzeylerini karşılaştırmıştır. 2024 öğretmenin katılımıyla gerçekleştirilen çalışmada “Bilgi Güvenliği Farkındalık Ölçeği” kullanmıştır. Sonuçlar Fatih projesinin uygulandığı okullarda bilgi güvenliği farkındalığının daha fazla olduğu ortaya çıkmıştır. Ayrıca, erkeklerde kadınlara göre bilgi güvenliği farkındalığının daha fazla olduğu ve genç yaşta olan öğretmenlerin bilgi güvenliği farkındalık düzeylerinin ileri yaşta olan öğretmenlere göre daha yüksek olduğunu ifade edilmiştir.

Yılmaz ve Ezin (2017) ülkemizdeki ebeveynlerin bilgi güvenliği konusundaki farkındalıkları incelemişlerdir. Nitel araştırma yöntemi kullanılarak yapılan bu

çalışmanın örneklemini 91 öğrenci ailesi oluşturmaktadır. Araştırma sonucunda ebeveynlerin bilgi güvenliği farkındalıklarının olduğu ancak verileri yedekleme ve yedekleme sıklığı konusundaki farkındalıklarının düşük olduğu anlaşılmıştır. Ailelerin çocuklarına bilgi güvenliği konusunda yardımcı olmada yetersiz kaldıkları ve çocuklarına bilgi güvenliği konusunda yeterli bilgi veremedikleri tespit edilmiştir. Benzer bir çalışmada Aslay, Çam ve Özen (2019) yükseköğretim kurumlarındaki bireylerin bilgi güvenliği farkındalık düzeylerini incelemişlerdir. Bu çalışmanın örneklemini Gümüşhane Üniversitesinde yer alan öğrenci, çalışan ve akademisyenlerden oluşan 350 katılımcı oluşturmaktadır. Veri toplamak için anket ve yüz yüze görüşme tekniği kullanılmıştır. Analiz sonuçlarına göre yükseköğretim kurumlarında bilgi güvenliği farkındalık düzeyinin artırılması için eğitimler verilmesi gerektiği vurgulanmıştır. Başka bir çalışmada Taner ve Kılıç (2019) güvenlik güçlerinin bilgi güvenliği farkındalığını belirlemeye yönelik bir çalışma yapmışlardır. Bu çalışmanın örneklemini ise Siirt'te görev yapan 207 jandarma ve 197 polis olmak üzere toplam 404 güvenlik personeli oluşturmaktadır. Sonuçlar emniyet personellerinin bilgi güvenliği farkındalık düzeylerinin düşük olduğunu göstermektedir. Bu çalışmanın sonucunda emniyet personellerinin bilgi güvenliği farkındalıklarının artırılmasına yönelik çalışmalar yapılması gerektiği ifade edilmektedir. Diğer bir çalışmada ise Öztemiz ve Yılmaz (2013) Ankara ilinde yer alan 14 kütüphaneyi ele alarak bilgi merkezlerinde bilgi güvenliği farkındalığı konusunu incelemişlerdir. Veri yüz yüze veya telefon görüşme ile toplanmıştır. Araştırmanın sonucu kütüphane çalışanlarının büyük bir kısmının bilgi güvenliği farkındalık seviyelerinin yetersiz olduğunu göstermektedir. Başka bir çalışmada Erdoğan (2017) üniversite öğrencilerinin bilgi güvenliği kazanımlarını ve bilgi güvenliği farkındalıklarını incelemiştir. Bu çalışmanın örneklemini Afyon Kocatepe Üniversitesi'nde okuyan ve rastgele seçilen 550 öğrenci oluşturmaktadır. Sonuçlar bilgi güvenliği kazanımlarının cinsiyet, yaş ve internet kullanım süresine göre; bilgi güvenliği farkındalıklarının ise yaş, bölüm, sınıf ve internet ortamını güvenli bulup bulmamalarına göre anlamlı bir farklılık gösterdiğini göstermektedir. Benzer bir çalışmada, Yılmaz, Yılmaz ve Sezer (2014) üniversite öğrencilerinin güvenli bilgi ve iletişim teknolojisi kullanım davranışlarını incelemişlerdir. Bu çalışmanın örneklemini üniversite birinci sınıfta okuyan 124 öğrencisi oluşturmaktadır. Sonuçların istenilen düzeyde çıktığı ifade edilmektedir.

Alemdaroğlu (2020) çalışanların bilgi güvenliği farkındalığına ilişkin algılarını bankacılık sektörünü ele alarak incelemiştir. Bu çalışmanın örneklemini Türkiye’de bulunan özel bir bankanın genel müdürü pozisyonunda çalışan toplam 321 kişi oluşturmaktadır. Bu verilere göre analiz sonuçlarına bakıldığında erkek çalışanların kadın çalışanlara göre daha fazla bilgi güvenliği farkındalığına sahip olduğu bulunmuştur. Lakin görev süresine göre anlamlı bir fark olmadığı sonucu ortaya çıkmıştır.

Okul vd. (2018) konaklama işletmesi yöneticilerinde bilgi güvenliği farkındalığı Kuşadası’ndaki beş yıldızlı otelleri ele alarak incelemiştir. Kuşadası’ndaki konaklama işletmesi yöneticilerinin bilgi güvenliği konusunda farkındalıklarının yüksek olduğu tespit edilmiştir. Lakin bilgi güvenliği ile ilgili bazı önemli hususlarda yeterli bilgiye sahip olmadıkları ifade edilmiştir. Çelik (2020) ise kalite yönetimi yöneticilerinin bilgi güvenliği farkındalığını incelemiştir. Bu çalışmanın örneklemini İstanbul ilinde yer alan Kamu Hastaneler Birliğine bağlı 67 hastanede çalışan 87 yönetici oluşturmaktadır. Sonuçlar erkek ve kadın yöneticilerin bilgi güvenliği farkındalığı düzeylerinde anlamlı bir fark olduğuna işaret etmektedir. Benzer bir çalışmada Mart (2012) çalışanlarda bilgi güvenliği farkındalığını incelemiştir. Bu çalışmanın örneklemini farklı meslek gruplarından 501 birey oluşturmaktadır. Sonuçlar çalışanların bilgi güvenliği farkındalık düzeylerinde cinsiyete göre anlamlı bir fark olduğu görülmüştür. Benzer şekilde Özdemir (2019) yaptığı çalışmada kamu kurum ve kuruluşlarında bilgi güvenliği farkındalığını incelemiştir. Bu çalışmanın örnekleminin 501 kişiden oluştuğu ifade edilmiştir. Sonuçlar üniversite mezunu bireylerin bilgi güvenliği farkındalığı düzeylerinin lise mezunu bireylere göre daha yüksek olduğunu göstermektedir. Diğer bir çalışmada Kapanoğlu (2016) yapmış olduğu çalışmada öğretmenlerin bilgi güvenliği farkındalığını incelemiştir. Bu çalışmanın örneklemini Türkiye’de 12 bölgeden 6 farklı branşta 1355 öğretmen oluşturmaktadır. Sonuçlar öğretmenlerin bilgi güvenliği farkındalık düzeylerinin orta düzeyde olduğunu göstermektedir. Bilgi güvenliği farkındalıklarının branşa, alınan bilgi güvenliği eğitime, öğrenim durumuna, yaşanılan bölgeye, internet kullanım süresine ve yaşa göre anlamlı farklılıklar gösterdiği belirtilmiştir. Başka bir çalışmada, Solmaz (2020) öğretmen adaylarının siber bilgi güvenliği farkındalıklarını ile dijital vatandaşlık düzeyleri arasındaki ilişkiyi incelemiştir. Bu çalışmanın örnekleminin bir devlet üniversitesinin Eğitim fakültesinde okuyan 1155 öğretmen adayı oluşturmaktadır. Verilerin analiz sonuçlarına bakıldığında öğretmen adaylarının siber bilgi güvenliği farkındalık düzeylerinin ortalamanın üstünde olduğunu göstermektedir.

Korelasyon analizi sonucu ise öğretmen adaylarının siber bilgi güvenliği farkındalıkları ile dijital vatandaşlık düzeylerini arasında pozitif yönde anlamlı bir ilişki olduğunu göstermektedir. Benzer bir çalışmada Dönmez (2019) lise öğrencilerinin bilgi güvenliği farkındalığı ile dijital okuryazarlık düzeyleri arasındaki ilişkiyi incelemiştir. Çalışmanın örneklemini lisede öğrenim gören 187 öğrenci oluşturmaktadır. Korelasyon analizi sonuçlarına göre bilgi güvenliği farkındalığı ile dijital okuryazarlık düzeyleri arasında anlamlı ve pozitif yönde bir ilişki olduğunu bulunmuştur. Başka bir çalışmada, Avcı ve Oruç (2020) üniversite öğrencilerinin kişisel siber güvenlik davranışları ile bilgi güvenliği farkındalıkları arasındaki ilişkiyi incelemiştir. Bu çalışmanın örneklemini özel bir üniversitenin mühendislik fakültelerinde okuyan 88 öğrenci oluşturmaktadır. Korelasyon analizi sonuçları öğrencilerinin kişisel siber güvenlik davranışları ile bilgi güvenliği farkındalık düzeyleri arasında pozitif yönde anlamlı bir ilişki olduğunu göstermektedir.

### **Siber Suç Farkındalığı ve Yapılan Çalışmalar**

Literatür incelendiğinde siber suç, siber suç farkındalığı, siber suç zorbalık kavramlarının açıklamalarına ve bu kavramlarla ilgili olan çalışmalara yer verilmiştir.

Siber Suç Farkındalığı, bireylerin siber suç konusu hakkında ne kadar fikir sahibi olduğu olarak ifade edilmektedir (Budak, 2015).

Bu çalışma da yer alan diğer önemli kavram ise siber zorbalık kavramıdır. Siber zorbalık kavramını açıklayacak olursak, başkalarına zarar vermeye yönelik saldırganca davranışların tekrarlayan biçimde ve kasıtlı olarak elektronik ve bilişim araçlarıyla elektronik ortamda gerçekleşmesidir (Tokunaga, 2010). Siber zorbalık kavramının yerine bazen e-zorbalık, elektronik zorbalık, siber şiddet, siber taciz, dijital şiddet, dijital zorbalık vb. gibi kavramların da eş anlamlı olarak kullanıldığı ifade edilmektedir (Hinduja ve Patchin, 2015; Pekşen Süslü, 2016).

Siber suç ise, bilgisayar ve bilgisayar ağı kullanılarak kullanıcı veya kullanıcı gruplarına yönelik, mağdur olan kişinin onurunu zedelemeye veya mağdura fiziksel veya zihinsel olarak doğrudan veya dolaylı olarak ağ üzerinden zarar verme suçu ile internet (görüşme odaları, e-postalar, ilan sayfaları ve gruplar) sosyal medya ve cep telefonu gibi iletişim araçları kullanarak zarar verme amaçlı saldırıların yapılması olarak ifade edilmektedir (Wikipedia, 2020).

Siber suçlar geniş bir edimler dizisini içermektedir. Genellikle, her ne kadar doğrudan bilgisayarı hedef alan suçlar ve bilgisayar ağları ve aygıtlarından faydalanarak işlenen suçlar, olarak iki temel kategoriye bölünmüş olsa da birincil hedef bilgisayar ağ veya aygıtının özgürlüğüdür (Wikipedia, 2020). Bilgisayar ağı ve aygıtlarını hedef alan suçlar ise şunlardır: Kötü amaçlı yazılım, hizmet-dışı bırakma saldırıları, bilgisayar virüsleri gibi vb. suçlardır (Wikipedia, 2020).

Bilgisayar ağları ve aygıtlarından faydalanarak işlenen suçlar ise şunlardır: bilgi çalma, dolandırıcılık ve kimlik hırsızlığı, siber izleme, kişisel ağ bilgilerinin çalınması (Kullanıcı adı, giriş şifresi, kredi kartı bilgileri vb.) (Wikipedia, 2020).

Siber suç işlenirken hedef, kişinin maddi mal varlığı veya kullandığı sistemler olabilir. Bu sistemlere kayıt eden, zarar veren, izinsiz erişen, özel hayata müdahale eden ve veri kopyalayan kişiler siber suçlu olarak tanımlanmaktadır (Siberay, 2020). Siber suçlarda kullanılan yöntemler ise şunlardır: kişilerin veya kurumların verilerine izinsiz erişim, saldırganlar, genel olarak siber suçları işlediklerinde birçok kaynağa zarar verebilmektedir. Bu noktada ortaya çıkabilecek risklerin siber güvenliği sağlanmalıdır. İtibarı zedeleme amaçlı girişimler, hedefleri belirleyerek sızmak veya erişebilmek için kötü amaçlı yazılım uygulamaları kullanmaktadır. Genel olarak kötü yazılımları tanımlayacak olursak virüs, trojan, malware gibi özel hazırlanmış uygulamalardır. Kişilerin banka hesaplarına erişim, illegal yollardan zedeleme amaçlı girişimler, sistemleri hizmet dışı bırakacak saldırılar gibi bir birçok noktada karşımıza gelmektedir. Saldırıya maruz kalan kişiler, siber suça ortak olabildikleri gibi habersiz olarak suçların işlenmesine yardımcı olmaktadır (Siberay, 2020). Siber saldırganlar tarafından ele geçirilen sistemler ise virüslerin veya zararlı uygulamaların dağıtılmasında yardımcı olmak, fidye yazılımları ve kripto sistemleri kullanmak, botnet ağlarının bir parçası olarak sıralanmaktadır (Siberay, 2020).

Tailor (2020) erkek ve kadın bireylerin siber suç bilinci/farkındalık düzeylerinin cinsiyete göre farklılaşıp farklılaşmadığını incelemiştir. Çalışmanın örneklemini toplam 360 kişiden oluşmaktadır. Bu çalışmada Rajasekar (2011) tarafından geliştirilen siber suç farkındalık ölçeğini kullanmıştır. Sonuçlar erkek ve kadın bireyler arasında siber suç bilinci/farkındalığı açısından anlamlı bir fark olduğu sonucunu ortaya koymuştur. Benzer bir çalışmada Bansal (2018) öğretmen adayları arasında siber suç farkındalığını kurumsal yönetim ve davranışsal türlerine göre incelemiştir. Örneklemini 132 öğretmen adayı oluşturmaktadır. Yönetimlerine göre üç farklı türden (devlet, devlet destekli ve kendi

kendini finanse eden) kuruluşun bu çalışmada yer aldığı ifade etmiştir. Çalışmasında Rajasekar (2011) tarafından geliştirilen siber suç farkındalık ölçeğin kullanılmıştır. Sonuçta öğretmen yetiştiren kurumların yönetim türlerinin ve öğretmen adaylarının davranış kalıplarının siber suç farkındalık düzeyi üzerinde önemli bir etkiye sahip olduğu ifade edilmiştir.

Karagiannopoulos, Sugiura ve Kirby (2019) Portsmouth Siber Suç Farkındalık Kliniği Projesini incelemişlerdir. Bu projenin amacı yerel topluluklar ve kuruluşlar arasında siber suçlara karşı farkındalık oluşturma ve direnç arttırmaya yardımcı olacak yenilikçi bir araştırma ve iş birliği geliştirmektir. Çalışmanın sonucunda toplum için siber suç farkındalığı üzerine genel konuşmalar, sunumlar ve atölye çalışmaları yapılarak siber suç farkındalığını arttırmaya çalışıldığı belirtilmiş ve bu çalışmaların sonuçlarının olumlu olduğu ve işe yaradığı gözlemlenmiştir. Benzer bir çalışmada Goel (2014) öğretmen eğitiminde siber suç farkındalığını incelemiştir. Bu çalışmasının örneklemini 120 öğretmen adayı oluşturmaktadır. Rajasekar (2011) tarafından geliştirilen siber suç farkındalık ölçeği kullanılmıştır. Çalışma sonucunda kadın ve erkek bireyler arasında siber suç farkındalığına yönelik anlamlı bir fark olmadığı sonucu ortaya çıkmıştır. Benzer bir çalışmada Solak ve Topaloğlu (2015) lisans öğrencilerinin siber suç algıları/farkındalıkları arasındaki farklılıkları incelemişlerdir. Çalışmanın örneklemini Trakya Üniversitesinde eğitim gören 182 öğrenci oluşturmaktadır. Sonuçlar öğrencilerin siber suç algılarına ilişkin hukuki ve ahlaki bakış açıları arasında cinsiyete göre anlamlı bir fark olmadığını göstermektedir. Diğer bir çalışmada, Topal vd. (2019) öğretmen adaylarının siber suçlarla ilgili bilgi ve farkındalık düzeylerini incelemiştir. Araştırmanın örneklemini Kocaeli Üniversitesinde okuyan 323 öğretmen adayı oluşturmaktadır. Sonuçlar öğretmen adaylarının siber suçlar konusunda bilgi düzeylerinin yeterli olmadığını göstermektedir. Cinsiyete göre ve ortalama günlük bilgisayar kullanım süresine göre anlamlı farklılıklar görülmüştür. Benzer bir çalışmada Budak (2015) mesleki ve teknik liselerdeki bilişim bölümü öğrencilerinin siber suç farkındalıklarını incelemiştir. 2013-2014 eğitim-öğretim yılında Erzurum'da Mesleki ve Teknik Liselerin bilişim bölümlerinde okuyan toplam 269 öğrenciye yerli-yabancı kaynaklardan yararlanılarak ve uzman görüşlerine başvurulak oluşturulan “Ortaöğretim Kurumlarında Siber Suç Farkındalık Anketi” uygulanmıştır. Çalışma sonucunda öğrencilerin siber farkındalık durumları, interneti kullanma süreleri ve internette saldırıya uğrama durumları ortaya konulmuştur.

Wang (2007) bilgisayar tabanlı siber suçları araştırmak için dijital kanıtları incelemeye çalışmıştır. Bu incelemede siber suçlarla mücadele etmek için sabıka delilleri toplanmıştır. Bu delillerin analizinde çıkan sonuçlar siber suçların günden güne arttığını ve değişik isimlerde ortaya çıktığını göstermektedir. Bu sonuca göre, bilgisayar tabanlı sistemler için yazılım kullanılarak siber suçlara karşı koruma sağlanabileceği ve siber suç işleyenlerin daha kolay yakalanabileceği ifade edilmiştir. Diğer bir çalışmada Küçükvardar (2018) içerik analizi yöntemini işe koşarak, bilişim teknolojilerinin kötüye kullanılmasıyla ortaya çıkan siber suç ve buna bağlı kavramlar ile bu suçun etkilerini incelemiştir. Literatür analizi sonucunda teknolojinin gelişmesiyle beraber siber suçlarında dünya çapında ve tüm alanda gün geçtikçe artış gösterdiğini ifade edilmiştir. Son zamanlarda farklı isimlerde siber suçlar ortaya çıktığı için toplumun bu konuda aydınlatılması gerektiği ve farklı isimlerde çıkan bu siber suçların yasal olarak düzenlenmesi gerektiği ifade edilmiştir. Bunun için siber suçlara yönelik uluslararası hukuk boyutunda daha kapsamlı düzenlemelerin yapılması gerektiği ve her geçen gün etkisini arttıran siber suç kavramı üzerine bilimsel araştırmaların yapılması gerektiği ifade edilmektedir.

Yılmaz (2018) bireylerin siber suç korkusunu ve önlem alma stratejilerini ele almıştır. Ankara’da bulunan 13095 dört Teknokent çalışanına anket uygulaması gerçekleştirilmiştir. Çalışmanın sonucu Teknokent çalışanlarında siber suç korkusu bulunduğu ve katılımcıların çoğunluğunun orta ve üst düzeyde önlem alma stratejileri geliştirdikleri görülmüştür.

Agatston vd. (2007) öğrencilerin siber zorbalığa bakış açısını incelemişlerdir. Bir devlet okulunda okuyan 148 ortaokul ve lise öğrencisiyle görüştiklerini ifade etmişlerdir. Kadın öğrencilerin çoğu, siber zorbalığın okullarında bir sorun olduğunu belirtse de erkek öğrencilerin bunun bir sorun olmadığını belirtmişlerdir. Diğer bir çalışmada, Mishna vd. (2010) ortaokul ve lise öğrencilerinde siber zorbalık davranışlarını incelemişlerdir. 2186 kişiden toplanan veri toplanmıştır. Toplanan bu verilerin analiz sonuçları incelendiğinde öğrencilerin yarısına yakın kısmını siber zorbalığa maruz kaldıklarını veya siber zorbalık yaptıkları anlaşılmaktadır. Benzer bir çalışmada Mishna vd. (2009) çocukların ve gençlerin siber zorbalıkla ilgili algılarını belirlemeyi amaçlamıştır. Örneklem olarak beşinci ve sekizinci sınıfta okuyan 38 öğrenci seçilmiştir. Katılımcılar siber zorbalığın önemli bir sorun olduğunu ifade etmişler ve siber zorbalığın çoğunlukla sosyal gruplar arasında arttığını belirtmişlerdir. Son olarak, Duman (2019) yapmış olduğu çalışmada

velilere yönelik geliştirilen siber zorbalık farkındalık eğitiminin etkisini incelemiştir. Bu çalışmada yöntem olarak zayıf deneysel modellerden tek grup ön test-son test yöntemini kullandığını ifade etmiştir. 80 veliden toplanan veri analiz edildiğinde programa katılan velilerin duyarlılık düzeyleri arasında istatistiksel olarak anlamlı bir fark olduğu görülmüştür.

### **Ölçek Geliştirme Çalışmaları**

Rajasekar (2011) tarafından geliştirilen siber suç farkındalık ölçeği 36 maddeden oluşan İngilizce bir ölçektir. Söz konusu ölçek beşli Likert tipinde bir ölçektir. Ölçek 21 olumlu ve 15 olumsuz maddeden oluşmaktadır. Bireysel puan 36 maddenin puanlarının toplamıdır ve 36 ile 180 arasında değişmektedir. Olumsuz maddeler ters çevrildiğinde toplamda ne kadar yüksek puan alınır o kadar yüksek düzeyde siber suç farkındalığına sahip olunacağı ifade edilmektedir.

Abuda, Rivera ve Norona (2020) geliştirdikleri siber suç farkındalık ölçeğinin geçerliliğini Filipinler’de yer alan lise son sınıf öğrencileri örnekleminde incelemişlerdir. Likert tipinde 18 maddeden oluşan siber suç farkındalık ölçeği toplam 200 öğrenciye uygulamışlardır. Açımlayıcı faktör analizi dört faktörlü bir yapı ortaya koymuştur. Siber suç farkındalık ölçeğinin dört faktörü; kimlik avı (phishing) farkındalığı, istenmeyen posta ile ilgili farkındalık, anti virüs yazılımının algılanan etkinliği ve Webde zorbalık olarak isimlendirilmiştir. Ölçeğin yeterli iç tutarlılık gösterdiği ifade edilmektedir (Cronbach alfa= 0,823). Benzer bir çalışmada Tibi, Hadeje ve Watted (2019) tarafından geliştirilen siber suç farkındalığı ölçeği beşli Likert ölçeğinde derecelendirilen toplam 23 kapalı uçlu ifadeden oluşmaktadır. İfadeler siber suçlar hakkında bilgi ve katılımcıların kendilerini siber suçtan korumaya çalışıp çalışmadığı ile ilgili ifadeleri ve katılımcıların bir siber suç mağduru olup olmadığını inceleyen ifadeleri içermektedir.

Güldüren, Çetinkaya ve Keser (2016) ortaöğretim öğrencilerine yönelik bilgi güvenliği farkındalık ölçeği geliştirmişlerdir. Toplam 407 kişiden toplanan veriyle açımlayıcı faktör analizi (AFA) yapmışlardır. Yapılan açımlayıcı faktör analizi sonucuna göre ölçeğin 36 madde ve üç alt boyuttan oluştuğu ifade edilmiştir. 200 kişiden toplanan veri ile doğrulayıcı faktör analizi yapılmış ve üç faktörlü yapının doğrulandığı ifade edilmiştir. Ayrıca, katılımcıların bilgi güvenliği farkındalık düzeylerinin cinsiyete göre anlamlı bir farklılık gösterdiği ortaya çıkmıştır. Benzer bir çalışmada Çetinkaya, Güldüren ve Keser (2017) yaptıkları çalışmada Yurdagül (2005) tarafından tanımlanan

kuramsal ölçek geliştirme modelini baz alınarak bilgi güvenliği farkındalık ölçeği geliştirmeyi amaçlamışlardır. Çalışma grubunun toplam 516 öğretmenden oluştuğu belirtilmiştir. Çalışmanın ilk aşamasında, 316 kişilik katılımcı grubu ile açımlayıcı faktör analizi (AFA) yapıldığı ifade edilmiştir. Ölçeğin üç alt boyut (“Mobil cihazlar, Mahremiyet ve İletişim: MMI,” “Saldırı ve Tehditler: ST” ve “Genel Güvenlik: GG”) ve 48 maddeden oluştuğu belirlenmiştir. Çalışmanın ikinci aşamasında, 200 kişilik katılımcı grubu ile gerçekleştirilen doğrulayıcı faktör analizi (DFA) sonucunda üç faktörlü yapı doğrulanmıştır. Bu çalışma sonucunda öğretmenlerin bilgi güvenliği farkındalık düzeylerini belirlemek için kullanılabilecek geçerli ve güvenilir bir ölçek geliştirildiği açıklanmıştır. Diğer bir çalışmada Keser ve Güldüren (2015) üniversitelerde çalışan öğretim elemanlarının bilgi güvenliği farkındalık düzeylerini belirlemeye yönelik bir ölçek geliştirme çalışması gerçekleştirmiştir. 363 öğretim elemanının yer aldığı ilk çalışmada açımlayıcı faktör analizi yapılarak ölçeğin 34 maddeden ve iki alt boyuttan oluştuğu ortaya konulmuştur. Doğrulayıcı faktör analizi 200 kişi ile yapılarak iki faktörlü yapı doğrulanmıştır. Son olarak, Çatuk (2018) siber riskler karşısında KOBİ’lerin bilgi güvenliği farkındalıklarını ölçen bir ölçek geliştirme çalışması gerçekleştirmiştir. Bu çalışmanın örneklemini Gaziantep ilinde yer alan 800 kişiden oluşan KOBİ çalışanları oluşturmaktadır. Güvenirlik analizi ve doğrulayıcı faktör analizi sonucuna bakıldığında ölçeğin geçerli ve güvenilir olduğu görülmektedir.

## BÖLÜM III

### YÖNTEM

Bu çalışma, nicel araştırma yönteminin kullanıldığı bir ölçek geliştirme çalışmasıdır. Bu ölçek geliştirme çalışmasında öncelikle kapsamlı bir literatür taraması ile TCK’nda yer alan bilişim suçlarına ve siber suç mevzuatına dayanılarak madde havuzu oluşturulmuştur. Maddeler tasarlanırken bir maddenin tek bir ifadeyi ölçmesine dikkat edilmiştir. Geliştirilen madde havuzu üç farklı uzman (adli bilişim uzmanı, bilişim sistemleri uzmanı, ölçme ve değerlendirme uzmanı) tarafından değerlendirilmiştir. Böylelikle, madde havuzu ve nihai ölçek formu alan uzmanlarından gelen değerlendirmeler dikkate alınarak oluşturulmuştur. Uzmanlar maddelerin değiştirilmesi ya da çıkarılması yönünde öneride bulunmuştur.

Uzman görüşüne göre nihai halini alan ölçek taslağı 500 kişiden oluşan ilk örneklem grubuna online olarak uygulanmıştır. SPSS yazılımı kullanılarak Cronbach Alpha güvenirlik katsayısı hesaplanmış ve Açıklayıcı Faktör Analizi (AFA) yapılmıştır. Alt boyutları belirlenen ölçek, 494 kişiden oluşan farklı bir örneklem grubuna online olarak uygulanmıştır. SPSS AMOS yazılımı kullanılarak doğrulayıcı faktör analizi, yapısal eşitlik modellemesi ile ölçüm modeli testi ve ölçüt bağıntılı geçerlik yapılmıştır.

### Evren ve Örneklem

Bu araştırmanın evrenini teknolojik cihaz (bilgisayar, akıllı telefon, tablet gibi) ve internet kullanan üniversite öğrencileri oluşturmaktadır. İlk çalışmanın örneklemini ise Tokat Gaziosmanpaşa Üniversitesinde öğrenim gören 500 üniversite öğrencisi oluşturmaktadır. Katılımcılar kolayda örnekleme yöntemi ile seçilmiştir. Tablo 1 incelendiğinde ilk çalışma ortalama yaşı 24,80 (SS= 2,60, 17-48 yaş arasında) olan 294 kadın (%58,8) ve 206 erkek (%41,2) katılımcıdan oluşmaktadır. Çalışmaya gönüllü olarak katılan katılımcılar devlet üniversitelerinde okuyan ön lisans, lisans, yüksek lisans ve doktora öğrencileridir. Katılımcıların %12,4’ü günde 1-2 saat, %37,8’i günde 3-4 saat, %32,6’sı günde 5-7 saat ve %17,2’si ise günde 8 saatten fazla internet kullanmaktadır. Sonuçlar katılımcıların çoğunun (%92,8) mobil internet kullandığını göstermektedir. Katılımcıların %74,6’sı E-devlet, %71,4’ü ise e-ticaret hizmetlerini kullanmaktadır. Katılımcıların %11,8’i siber suçlarla ilgili eğitim aldığını, %14,0’ü ise siber saldırıya maruz kaldığını belirtmektedir.

Tablo 1. Birinci Çalışma Grubuna Ait Katılımcıların Demografik Bilgileri

| Cinsiyet                                                 | Frekans | Yüzde (%) |
|----------------------------------------------------------|---------|-----------|
| Kadın                                                    | 294     | 58,8      |
| Erkek                                                    | 206     | 41,2      |
| İnternet Kullanım Süreniz                                |         |           |
| 1-2 Saat                                                 | 62      | 12,4      |
| 3-4 Saat                                                 | 189     | 37,8      |
| 5-7 Saat                                                 | 163     | 32,6      |
| 8 Saat ve üzeri                                          | 86      | 17,2      |
| Mobil Cihazınızda internet var mı                        |         |           |
| Evet                                                     | 446     | 92,8      |
| Hayır                                                    | 54      | 7,2       |
| İnternet hizmetleri kullanım amacı                       |         |           |
| İnternet/mobil bankacılık hizmetini kullanırım           | -       | -         |
| E-devlet hizmetlerini kullanırım                         | 376     | 74,6      |
| E-ticaret siteleri üzerinden İnternet alışverişi yaparım | 360     | 71,4      |
| Kullanmıyorum ve kullanmayı düşünmüyorum                 | -       | -         |
| Siber suçlarla ilgili eğitim aldınız mı?                 |         |           |
| Evet                                                     | 59      | 11,8      |
| Hayır                                                    | 441     | 88,2      |
| Siber saldırıya maruz kaldınız mı?                       |         |           |
| Evet                                                     | 70      | 14,0      |
| Hayır                                                    | 430     | 86,0      |
| Toplam                                                   | 500     | 100       |

İkinci çalışma ortalama yaşı 26,30 (SS=2,42, 18-47 yaş arasında) olan 494 katılımcıdan oluşmaktadır (281 kadın ve 213 erkek). Katılımcıların %11,7 si günde 1-2 saat, %40,5'i günde 3-4 saat, %33,4'ü günde 5-7 saat ve %14,4'ü günde 8 saatten fazla

internet kullanmaktadır. Tablo 2’de belirtildiği üzere katılımcıların %81,4’ü e-devlet, %62,1’i ise e-ticaret hizmetlerini kullanmaktadır. Katılımcıların %15’i siber suçlarla ilgili eğitim aldığını, %13,6’sı ise siber saldırıya maruz kaldığını belirtmektedir.

Tablo 2. İkinci Çalışma Grubuna Ait Katılımcıların Demografik Bilgileri

| Cinsiyet                                                 | Frekans | Yüzde (%) |
|----------------------------------------------------------|---------|-----------|
| Kadın                                                    | 281     | 56,9      |
| Erkek                                                    | 213     | 43,1      |
| İnternet Kullanım Süreniz                                |         |           |
| 1-2 Saat                                                 | 55      | 11,7      |
| 3-4 Saat                                                 | 200     | 40,5      |
| 5-7 Saat                                                 | 169     | 33,4      |
| 8 Saat ve üzeri                                          | 76      | 14,4      |
| Mobil Cihazınızda internet var mı                        |         |           |
| Evet                                                     |         |           |
| Hayır                                                    |         |           |
| İnternet hizmetleri kullanım amacı                       |         |           |
| İnternet/mobil bankacılık hizmetini kullanırım           | -       | -         |
| E-devlet hizmetlerini kullanırım                         | -       | 81,4      |
| E-ticaret siteleri üzerinden İnternet alışverişi yaparım | -       | 62,1      |
| Kullanmıyorum ve kullanmayı düşünmüyorum                 | -       | -         |
| Siber suçlarla ilgili eğitim aldınız mı                  |         |           |
| Evet                                                     | 74      | 15,0      |
| Hayır                                                    | 420     | 85,0      |
| Siber saldırıya maruz kaldınız mı                        |         |           |
| Evet                                                     | 67      | 13,6      |
| Hayır                                                    | 427     | 86,4      |
| Toplam                                                   | 494     | 100       |

### **Veri Toplama Süreci**

Tüm araştırma prosedürleri etik standartlara uygundur ve araştırma Tokat Gaziosmanpaşa Üniversitesi Sosyal ve Beşerî Bilimler Araştırmaları Etik Kurulu (17/11/2020-E.51622) tarafından onaylanmıştır. Katılımcılar araştırmanın amacı hakkında bilgilendirilmiş ve tüm katılımcılara online formda gönüllü katılım onay sorusu sorulmuştur. Ölçme aracı demografik sorular (ör. cinsiyet, yaş, internet kullanımı, siber suç, siber saldırı gibi) ve ölçek maddeleri bulunmaktadır. Bu çalışmada veriler online olarak Google Form üzerinden 2020-2021 yılları arasında Tokat Gaziosmanpaşa Üniversitesi öğrencilerinden elde edilmiştir.

### **Ölçme Araçları**

Bu çalışmada ölçme aracı olarak Demografik Bilgi Anketi, Dijital Veri Güvenliği Farkındalığı Ölçeği ve bu çalışmada geliştirilen Siber Suç Farkındalık Ölçeği kullanılmıştır. Siber Suç Farkındalık Ölçeği (SSFÖ) beşli likert tipinde 41 maddeden oluşan ve üç faktörlü olarak geliştirilmiş bir ölçektir. Ölçeğin katılma derecesi ise, Kesinlikle Katılmıyorum (1), Katılmıyorum (2), Kararsızım (3), Katılmıyorum (4), Kesinlikle Katılıyorum (5) şeklinde belirlenmiştir ve katılımcılar buna göre puanlamışlardır. Ölçüt bağıntılı geçerlik için kullanılan Dijital Veri Güvenliği Farkındalığı Ölçeği, beşli Likert tipinde 32 maddeden oluşan ve tek faktörlü olarak geliştirilmiş geçerli ve güvenilir bir ölçektir (Yılmaz, Şahin ve Akbulut, 2016).

## BÖLÜM IV

### BULGULAR

#### Çalışma I

##### Ölçeğin Formatı ve Madde Havuzunun Oluşturulması

Alanyazın incelemesi sonucu ölçeğin kavramsal çerçevesi belirlenmiş ve ölçeğin formatı oluşturulmuştur. Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı siber suç mevzuatı ve Türk Ceza Kanunu'nun bilişim suçları kapsamında değerlendirilen siber suç türleri dikkate alınarak 90 maddeden oluşan bir madde havuzu araştırmacı ve danışmanı tarafından oluşturulmuştur.

##### Kapsam Geçerliliği

Madde havuzunun kapsam geçerliliği alanında uzman üç kişi (Adli Bilişim Uzmanı, Bilişim Sistemleri Uzmanı, Ölçme ve Değerlendirme Uzmanı) tarafından değerlendirilmiştir. Alan uzmanları maddeleri 1'den 10'a kadar puanlamış, puanlamanın ortalaması alınarak 8 puanın yani %80'nin altında kalan maddeler çıkartılmış ve gelen önerilere göre kalan maddeler üzerinde düzeltmeler yapmıştır. Maddelerin değerlendirilmesinde Delphi tekniği kullanılmıştır. İlk değerlendirmenin ardından alan uzmanları 47 maddenin çıkarılması gerektiğini önermiştir. İlk revizyondan sonra madde havuzu uzmanlara ikinci kez sunulmuştur ve uzmanlardan onay alındıktan sonra 43 maddelik nihai form elde edilmiştir.

##### Açımlayıcı Faktör Analizi (AFA)

AFA ölçeğin faktör yapısını belirlemek için gerçekleştirilmiştir. Kaiser'in örneklem uygunluğu ölçümü .957 olarak bulunmuş ve Bartlett'in küresellik testi sonuçları değeri anlamlı çıkmıştır ( $\chi^2$  (df=903) = 15408.501). Bu da değişkenlerin faktör analizi için uygun olduğunu göstermektedir. İlk aşamada faktör yükü 0,30 un altında kalan iki madde çıkarılmıştır. AFA sonuçlarına göre bir maddenin belirlenen boyutta yer alması için faktör yükünün en az 0,30 ve üstü olması gerekmektedir (Seçer, 2013). Varimax rotasyonu sonucunda üç faktörlü bir yapı oluşmuş ve 41 madde kalmıştır. Üç faktörün öz değeri birden büyüktür (19.501, 2.168, 1.426). Açıklanan Varyans sırasıyla 45.352, 5.041, 3.316 olarak bulunmuştur. Açıklanan toplam varyans ise %53.709 olarak

bulunmuştur. Tablo 3 Varimax rotasyonu ile maksimum olasılık için oransal ortak etken varyans ve döndürülmüş bileşen matris değerlerini göstermektedir.

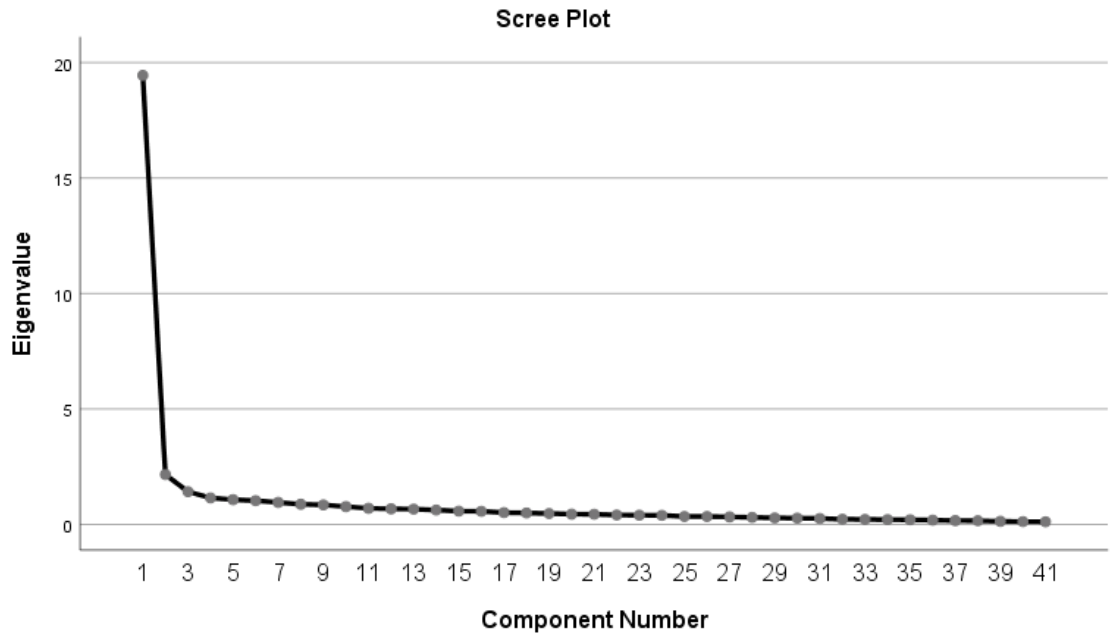
Tablo 3. Döndürülmüş Bileşen Matrisi Sonuçları

| Maddeler | Oransal Ortak Etken Varyans | 1    | 2    | 3    |
|----------|-----------------------------|------|------|------|
| Madde20  | ,603                        | ,542 |      |      |
| Madde21  | ,559                        | ,599 |      |      |
| Madde22  | ,549                        | ,467 |      |      |
| Madde23  | ,657                        | ,658 |      |      |
| Madde26  | ,663                        | ,584 |      |      |
| Madde27  | ,496                        | ,553 |      |      |
| Madde28  | ,669                        | ,748 |      |      |
| Madde29  | ,680                        | ,750 |      |      |
| Madde30  | ,746                        | ,782 |      |      |
| Madde31  | ,410                        | ,459 |      |      |
| Madde32  | ,560                        | ,695 |      |      |
| Madde33  | ,546                        | ,629 |      |      |
| Madde34  | ,633                        | ,713 |      |      |
| Madde36  | ,620                        | ,605 |      |      |
| Madde40  | ,635                        | ,673 |      |      |
| Madde41  | ,475                        | ,426 |      |      |
| Madde1   | ,570                        |      | ,732 |      |
| Madde2   | ,573                        |      | ,685 |      |
| Madde3   | ,505                        |      | ,639 |      |
| Madde4   | ,373                        |      | ,461 |      |
| Madde5   | ,706                        |      | ,741 |      |
| Madde6   | ,402                        |      | ,517 |      |
| Madde7   | ,572                        |      | ,672 |      |
| Madde8   | ,681                        |      | ,674 |      |
| Madde9   | ,606                        |      | ,643 |      |
| Madde10  | ,634                        |      | ,641 |      |
| Madde11  | ,690                        |      | ,640 |      |
| Madde13  | ,498                        |      | ,446 |      |
| Madde14  | ,715                        |      | ,661 |      |
| Madde17  | ,692                        |      | ,620 |      |
| Madde19  | ,559                        |      | ,459 |      |
| Madde24  | ,663                        |      | ,540 |      |
| Madde35  | ,546                        |      | ,509 |      |
| Madde12  | ,385                        |      |      | ,442 |
| Madde15  | ,350                        |      |      | ,522 |
| Madde16  | ,499                        |      |      | ,634 |
| Madde18  | ,487                        |      |      | ,646 |
| Madde25  | ,452                        |      |      | ,496 |
| Madde37  | ,493                        |      |      | ,552 |

|                          |        |       |        |
|--------------------------|--------|-------|--------|
| Madde38                  | ,544   |       | ,516   |
| Madde39                  | ,572   |       | ,463   |
| Öz Değerler              | 19,501 | 2,168 | 1,426  |
| Açıklanan Varyans        | 45,352 | 5,041 | 3,316  |
| Toplam Açıklanan Varyans |        |       | 53,709 |

### Yamaç-Birikinti Grafiği (Scree-Plot)

Yamaç-birikinti grafiği (scree-plot) Şekil 1 de verilmiştir. Şekilden de anlaşılacağı üzere ölçeğin üç faktörlü yapıda olduğu anlaşılmaktadır. Elde edilen üç alt faktör “siber ortamda yer alan suçlar, siber ortama ve kişisel verilere yönelik suçlar ve gizlilik ve güvenlik” olarak isimlendirilmiştir.



Şekil 1. Ölçeğin Üç Faktörlü Yapısını Gösteren Yamaç – Birikinti Grafiği (Scree-Plot)

### Güvenilirliğe İlişkin Bulgular

Ölçeğin iç tutarlılık katsayısının hesaplanması için Cronbach alfa ( $\alpha$ ) kullanılmıştır. Buna göre ilk çalışmada farkındalık ölçeğinin tamamı için güvenilirlik katsayısı .967 bulunmuştur. Her bir alt boyut için güvenilirlik katsayısı sırasıyla .947, .923, .896 olarak bulunmuştur. Buna göre toplam ölçek ve alt boyutların iç tutarlılığına ilişkin güvenilirlik katsayılarının yüksek düzeyde söylenebilir.

### Betimleyici İstatistikler, Normallik ve Madde Ayırt Edicilik Analizi

Yapısal Eşitlik Modellemesi (YEM) yapıldığında çarpıklık için kabul edilebilir değerler -3 ile +3 arasındadır. Basıklık için ise kabul edilebilir değerler -10 ile +10 arasında olmalıdır (Brown, 2006). Normallik analizi sonuçlarına göre verinin normal dağılıma sahip olduğu söylenebilir. Tablo 4 incelendiğinde, %27'lik alt ve üst dilimde yer alan öğrencilerin toplam puanları arasındaki farkların her bir madde için istatistiksel olarak anlamlı ( $p<.001$ ) olduğu görülmüştür. Böylece geliştirilen ölçekteki 41 sorunun, üst ve alt grupta yer alan öğrencileri anlamlı şekilde ayırt edebildiği belirlenmiştir (Büyüköztürk, 2004).

Tablo 4. Betimleyici İstatistikler, Normallik Testi ve Madde Analizi Sonuçları

| Maddeler | Ortalama | SS    | Çarpıklık<br>(SE=.109) | Basıklık<br>(SE=.218) | t         |
|----------|----------|-------|------------------------|-----------------------|-----------|
| Madde1   | 4,92     | 0,452 | -2,446                 | 4,102                 | 3,867***  |
| Madde2   | 4,87     | 0,505 | -1,186                 | 3,766                 | 5,473***  |
| Madde3   | 4,85     | 0,544 | -4,659                 | 5,948                 | 5,831***  |
| Madde4   | 4,71     | 0,700 | -6,493                 | 3,147                 | 8,375***  |
| Madde5   | 4,87     | 0,496 | -8,328                 | 6,316                 | 5,998***  |
| Madde6   | 4,77     | 0,678 | -5,621                 | 2,311                 | 7,277***  |
| Madde7   | 4,83     | 0,583 | -6,345                 | 2,977                 | 6,140***  |
| Madde8   | 4,84     | 0,581 | -4,425                 | 1,592                 | 6,922***  |
| Madde9   | 4,85     | 0,515 | -2,725                 | 5,392                 | 6,192***  |
| Madde10  | 4,87     | 0,510 | -3,139                 | 4,945                 | 5,824***  |
| Madde11  | 4,87     | 0,473 | -6,551                 | 3,232                 | 6,368***  |
| Madde12  | 4,50     | 1,000 | -1,526                 | 4,287                 | 9,758***  |
| Madde13  | 4,78     | 0,690 | -5,453                 | 7,522                 | 7,301***  |
| Madde14  | 4,88     | 0,487 | -7,299                 | 2,497                 | 5,793***  |
| Madde15  | 4,64     | 0,731 | -2,088                 | 1,726                 | 8,642***  |
| Madde16  | 4,65     | 0,781 | -3,528                 | 6,764                 | 10,213*** |
| Madde17  | 4,82     | 0,559 | -5,991                 | 8,046                 | 7,519***  |
| Madde18  | 4,63     | 0,798 | -6,246                 | 4,275                 | 9,222***  |
| Madde19  | 4,78     | 0,605 | -5,328                 | 1,218                 | 8,040***  |
| Madde20  | 4,85     | 0,503 | -8,789                 | 4,568                 | 6,991***  |
| Madde21  | 4,86     | 0,505 | -4,219                 | 8,478                 | 6,389***  |
| Madde22  | 4,87     | 0,459 | -6,871                 | 5,821                 | 6,268***  |
| Madde23  | 4,86     | 0,491 | -6,215                 | 3,547                 | 6,734***  |
| Madde24  | 4,87     | 0,497 | -2,872                 | 3,541                 | 6,255***  |
| Madde25  | 4,56     | 0,853 | -3,258                 | 6,523                 | 12,415*** |
| Madde26  | 4,85     | 0,501 | -8,823                 | 2,578                 | 7,100***  |
| Madde27  | 4,79     | 0,591 | -2,546                 | 4,137                 | 8,509***  |
| Madde28  | 4,85     | 0,506 | -6,264                 | 7,548                 | 7,337***  |
| Madde29  | 4,83     | 0,562 | -8,456                 | 1,547                 | 7,420***  |
| Madde30  | 4,84     | 0,556 | -2,521                 | 5,546                 | 6,877***  |

|         |      |       |        |       |           |
|---------|------|-------|--------|-------|-----------|
| Madde31 | 4,76 | 0,654 | -7,589 | 3,582 | 8,719***  |
| Madde32 | 4,77 | 0,598 | -8,523 | 4,571 | 10,373*** |
| Madde33 | 4,63 | 0,720 | -6,218 | 5,823 | 10,674*** |
| Madde34 | 4,84 | 0,532 | -8,457 | 2,423 | 7,117***  |
| Madde35 | 4,86 | 0,512 | -6,283 | 4,529 | 6,395***  |
| Madde36 | 4,80 | 0,577 | -4,243 | 6,221 | 8,448***  |
| Madde37 | 4,79 | 0,582 | -7,587 | 9,825 | 8,960***  |
| Madde38 | 4,78 | 0,567 | -3,254 | 1,548 | 8,887***  |
| Madde39 | 4,82 | 0,534 | -2,458 | 5,657 | 8,321***  |
| Madde40 | 4,86 | 0,469 | -2,897 | 7,568 | 7,715***  |
| Madde41 | 4,77 | 0,635 | -8,452 | 4,567 | 8,172***  |

\*\*\*  $p < .001$

## Çalışma II

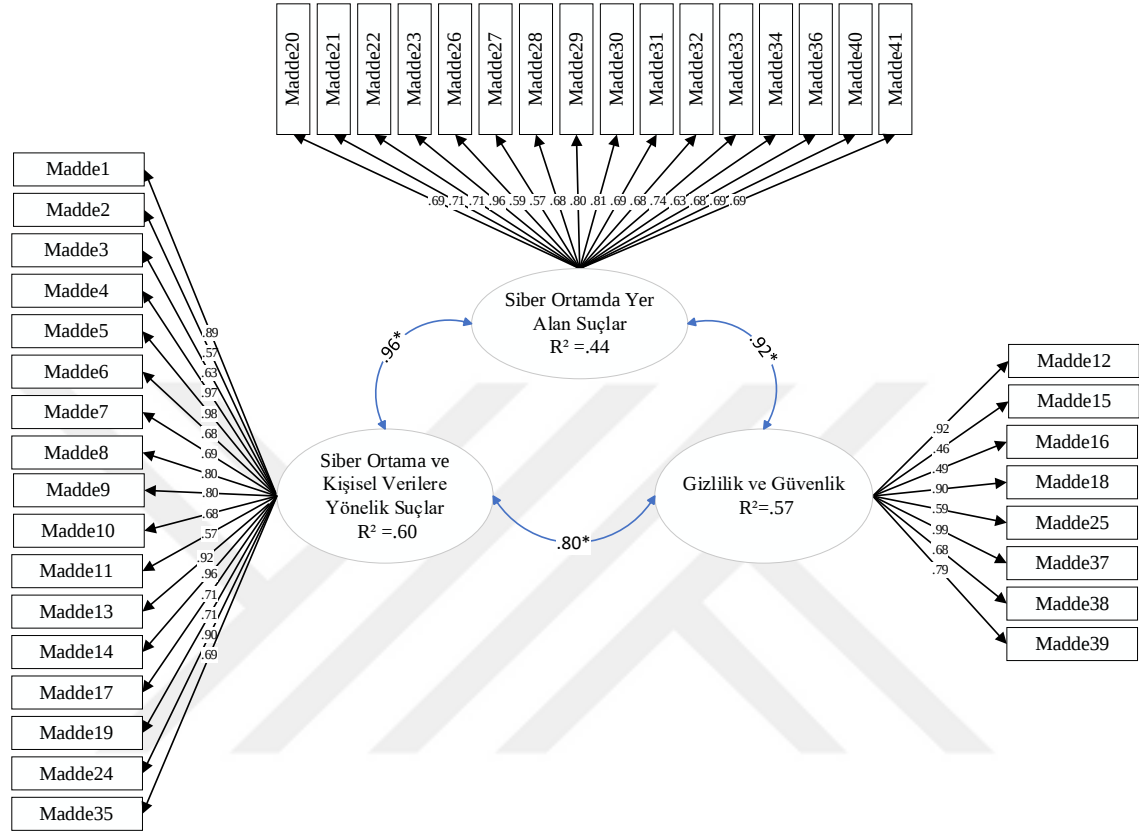
### Doğrulayıcı Faktör Analizi (DFA)

Şekil 2 de gösterilen ölçüm modelini SPSS AMOS (v.25) ile test etmek için DFA kullanılmıştır. Kline (2005) tarafından önerilen model uyum tahminleri ve referans değerleri incelendiğinde, ölçüm modeli için uyum indeks değerlerinin yeterli ve kabul edilebilir düzeyde olduğu söylenebilir: [ $\chi^2/df=2,87$ , GFI=.92, AGFI=.86, CFI=.92, TLI=.94, IFI=.93, RMSEA=.05]. Tablo 5 model uyum iyiliği değerlerini ve referans değerleri göstermektedir.

Tablo 5. Model Uyum İndisleri

| Uyum İndisleri | Ölçüm Modeli | Referans Değerler |
|----------------|--------------|-------------------|
| $\chi^2$       | 289,472      |                   |
| $p$ değeri     | < .001       |                   |
| $\chi^2/df$    | 2,872        | < 3               |
| GFI            | .924         | $\geq .90$        |
| AGFI           | .865         | $\geq .80$        |
| NFI            | .914         | $\geq .90$        |
| TLI            | .948         | $\geq .90$        |
| CFI            | .929         | $\geq .90$        |
| IFI            | .935         | $\geq .90$        |
| RMSEA          | .057         | $\leq .08$        |

SRMR .048  $\leq .08$

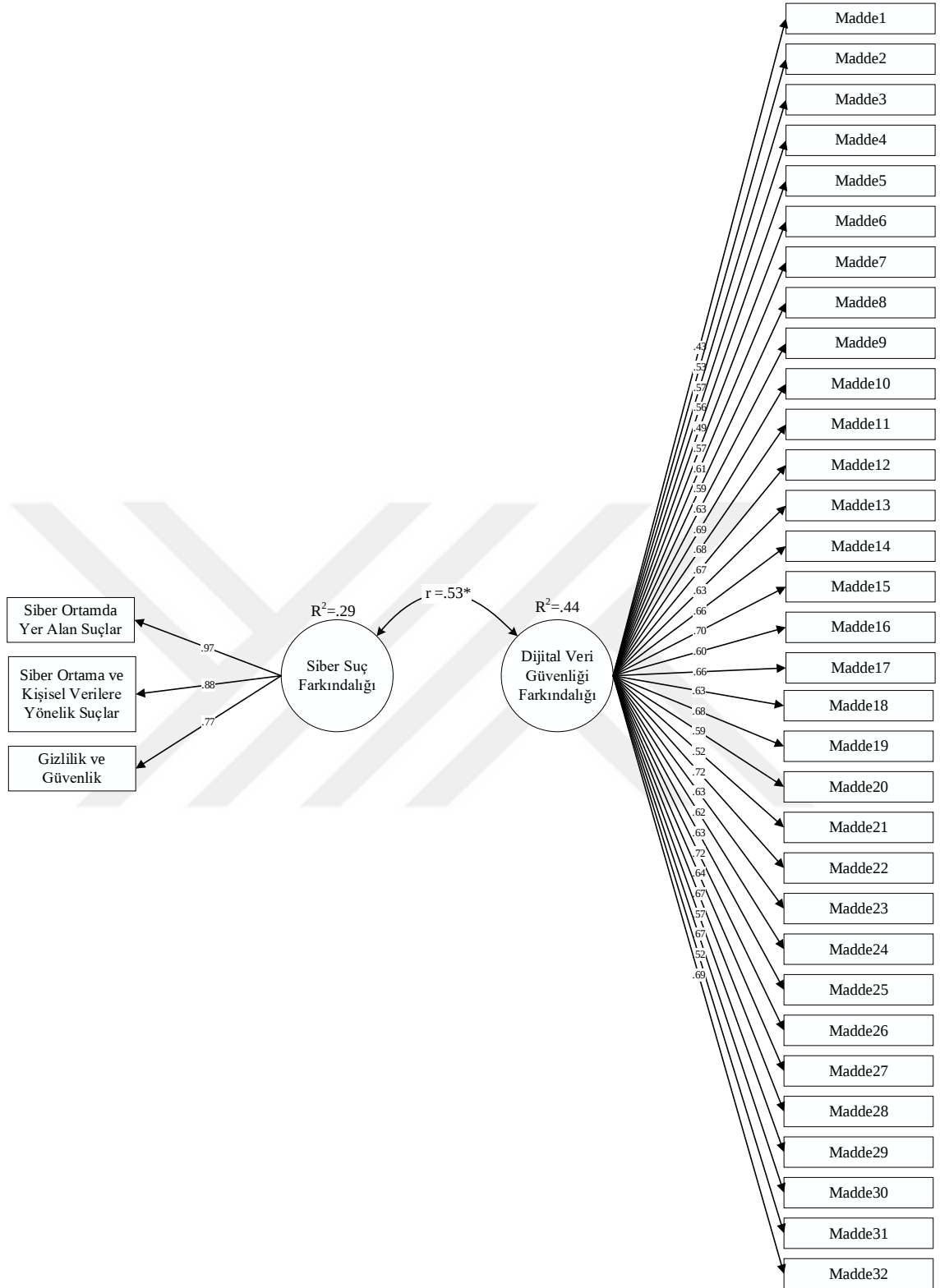


\* $p < .001$

Şekil 2. Ölçüm Modeli

### Ölçüt Bağıntılı Geçerlik

Siber Suç Farkındalık Ölçeği ile Dijital Veri Güvenliği Farkındalığı Ölçeği arasındaki benzerlik korelasyon analizi yapılarak test edilmiştir. Sonuçlar ölçekler arasında pozitif yönde ve anlamlı bir ilişki ( $r = 0,53$ ,  $p < 0,001$ ) olduğunu göstermektedir. Elde edilen bu sonuç iki ölçek arasındaki benzerliğin orta düzeyde olduğuna işaret etmektedir.



\* $p < .001$

Şekil 3. Ölçüt Bağıntılı Geçerlik

## BÖLÜM V

### TARTIŞMA

Teknolojinin gelişmesi ile günümüzde şahıslara, bankalara, şirketlere, hastanelere, okullara ve stratejik kurumlara ait bilgiler siber ortamda tutulmaktadır. Bilişim sistemlerinin herhangi bir siber saldırıya maruz kalamaması için sistemleri siber suçlara karşı korumak gerekmektedir (Gökçearslan, Nezgıtlı ve Çakır, 2020). Bu itibarla, kurumsal ve bireysel düzeyde siber saldırı ve risklere gereken önem verilmelidir. Günümüzde bilişim teknolojilerinin ve internet kullanımının artmasıyla birlikte siber saldırı ve tehditler de artış göstermekte siber suçlar ve suç türleri devamlı güncellenmektedir.

Ortaya çıkan siber suç türlerinin dünya çapında yer alan ülkelerin ilerleyen zamanlarda ekonomik ve sosyal olarak olumsuz yönde etkileyeceği aşıkardır. Bu nedenle, siber suçlarla mücadele için uluslararası iş birliklerine gidilmesi gerekmektedir (Erdoğan, 2012). Siber saldırı ve tehditler çok yüksek düzeyde artış göstermekte ve bu durum ise önlem alınmadığı takdirde başa çıkılmaz bir duruma dönüşebileceğine işaret etmektedir.

Siber suçlar toplum için çok büyük bir tehdit oluşturmakta ve dijitalleşmenin ardından siber suç daha çok artmaktadır bunun için siber suç türleri için yaş ve eğitim durumları ne olursa olsun kitle bilinci oluşturmak için bir strateji oluşturulmalıdır (Bansal vd., 2018). Siber suç artışına yönelik strateji oluşturulmadığı zaman daha fazla suç türleri ile karşılaşmamız kaçınılmaz olacaktır.

Bu çalışmada ayrıca siber suç farkındalık ölçeği ile dijital veri güvenliği farkındalığı ölçeği arasında yapılan ölçüt bağıntılı geçerlik analizi ile ortaya çıkan ( $r=.58$ ,  $p<0.01$ ) orta düzeyde pozitif yönde anlamlı ilişki, siber suç farkındalık ölçeğinin dijital veri güvenliği farkındalığı ölçeği ile bütünsel bir yaklaşım içinde olduğunu işaret etmektedir. Çalışmada DFA analizi sonuçlarına göre dijital veri güvenliği farkındalığı ölçeğinin tek boyutta oluşan ölçme modelinin bazı uyum indisleri iyi uyum gösterirken bazıları düşük düzeyde uyum göstermektedir (Yılmaz, Şahin ve Akbulut, 2016). Benzer olan dijital veri güvenliği farkındalığı ölçeğine göre siber suç farkındalık ölçeğindeki tüm uyum indisleri iyi uyum göstermektedir.

Siber suç farkındalık ölçeği özelliklerine ilişkin verileri özetlemek gerekirse siber suç ve türlerinin ölçülmesinde üç faktörlü yapının uygun olduğu görülmektedir. Benzer bir çalışma olan dijital veri güvenliği farkındalığı ölçeği ile aynı faktör sayısına sahip değildir ancak yapılan benzer diğer çalışmalarda (Budak, 2015) birden fazla faktör sayısının olduğu gözlemlenmiştir. Bu durum ise benzer yapılan çalışmalarda faktör sayısının aynı ya da farklı olarak değişkenlik gösterdiğini işaret etmektedir.

Ölçek geliştirme sürecinde güvenilirliğin test edilmesi mutlaka dikkat edilmesi gereken önemli bir nokta olarak ifade edilmektedir (Hinkin,1995). Daha önce yapılan çalışmalarda güvenilirliği belirlemede pek çok yöntem kullanılmasına rağmen bu çalışmada alanyazında sıklıkla tercih edilen ve en çok kabul gören Cronbach Alpha yöntemi kullanılmıştır (Gürbüz ve Karaküçük, 2007). Bu çalışmada güvenilirlik sonucu yüksek çıkmıştır. Benzer konularda yapılan çalışmalarda Cronbach Alpha katsayıları; (Dönmez vd., 2014) geliştirdiği Öğretmen Adaylarının Algılanan İnternet Riskleri Ölçeği'nde .856, (Tekerek ve Tekerek, 2013) tarafından geliştirilen Bilgi Güvenliği Farkındalığı Ölçeği'nde .720 ve (Mart, 2012) geliştirdiği Bilgi Güvenliği Farkındalığı Belirleme Anketi'nde .638 olarak hesaplanmıştır. Yapılan bu benzer çalışmalarda farklı güvenilirlik sonuçları ortaya çıkmıştır.

Bu çalışmada siber suç literatürüne katkı sağlamak amacıyla bireylerin siber suç farkındalık düzeylerini ölçmek için bir ölçek geliştirilmiştir. Literatür taraması yapıldığında bireylerin siber suç farkındalıklarını ölçen birçok ölçeğe rastlanmıştır. Örneğin Rajasekar (2011) tarafından geliştirilen siber suç farkındalık ölçeği 36 maddeden oluşan beşli Likert tipinde bir ölçektir. Ölçek 21 olumlu ve 15 olumsuz maddeden oluşmaktadır. Olumsuz maddeler ters çevrildiğinde elde edilen toplam puan ne kadar yüksekse o kadar yüksek düzeyde siber suç farkındalığına sahip olunacağı ifade edilmektedir.

Abuda, Rivera ve Norona (2020) tarafından geliştirilen siber suç farkındalık ölçeğinin geçerliliği Filipinler'de yer alan lise son sınıf öğrencileri örnekleminde incelemişlerdir. Likert tipinde 18 maddeden oluşan siber suç farkındalık ölçeği toplam 200 öğrenciye uygulamışlardır. Açıklayıcı faktör analizi dört faktörlü bir yapı ortaya koymuştur. Siber suç farkındalık ölçeğinin dört faktörü; kimlik avı (phishing) farkındalığı, istenmeyen posta ile ilgili farkındalık, anti virüs yazılımının algılanan

etkililiği ve Webde zorbalık olarak isimlendirilmiştir. Ölçeğin yeterli iç tutarlılık gösterdiği ifade edilmektedir (Cronbach alfa= 0,823).

Tibi, Hadeje ve Watted (2019) tarafından geliştirilen diğer bir siber suç farkındalığı ölçeği beşli Likert tipinde derecelendirilen toplam 23 ifadeden oluşmaktadır. İfadeler siber suçlar hakkında bilgi ve katılımcıların kendilerini siber suçtan korumaya çalışıp çalışmadığı ile ilgili ifadeleri ve katılımcıların bir siber suç mağduru olup olmadığını inceleyen ifadeleri içermektedir.

Bu çalışma ile geliştiren siber suç ölçeği mevcut ölçeklerle birçok yönden farklılıklar göstermektedir. Bu çalışmada geliştirilen ölçek Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı siber suç mevzuatı ve Türk Ceza Kanunu'nun bilişim suçları kapsamında değerlendirilen siber suç türleri dikkate alınarak Türkçe olarak geliştirilmiştir.

Diğer taraftan, mevcut ölçek diğer ölçekler ile kapsam olarak da farklılıklar göstermektedir. Abuda vd. (2020) tarafından geliştirilen siber suç farkındalık ölçeği kimlik avı (phishing) farkındalığı, istenmeyen posta ile ilgili farkındalık, anti virüs yazılımının algılanan etkililiği ve Webde zorbalık olmak üzere dört alt boyuttan oluşmaktadır. Tibi, Hadeje ve Watted (2019) tarafından geliştirilen siber suç farkındalığı ölçeği ise tek alt boyuttan oluşmaktadır. Ölçek “Siber suçun ne olduğunu bilirim, Kimlik avı hakkında bir şeyler duydum, Bir siber suçun sadece sanal bir suç olduğunu düşünüyorum, Bazı siber yasaları biliyorum” gibi genel ifadeler içermektedir.

## BÖLÜM VI

### SONUÇ VE ÖNERİLER

Bu tez çalışmasının amacı bireylerin siber suç farkındalık düzeylerini ölçmek için kullanılabilecek geçerli ve güvenilir bir siber suç farkındalık ölçeği geliştirmektir. Geliştirilen bu ölçeğin psikometrik özellikleri test edilmiştir. Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı siber suç mevzuatı ve Türk Ceza Kanunu'nun bilişim suçları kapsamında değerlendirilen siber suç türleri dikkate alınarak 90 maddeden oluşan bir madde havuzu araştırmacı ve danışmanı tarafından oluşturulmuştur. Uzman görüşleri sonucunda 43 maddelik bir nihai form oluşturulmuştur.

Çalışmanın birinci aşamasında güvenirlik analizi yapılmıştır. Ölçeğin tamamı için güvenirlik kat sayısı .97 olarak bulunmuştur. Dolayısıyla siber suç farkındalık ölçeğinin güvenirliği yüksek bir ölçek olduğu söylenebilir. Siber suç farkındalık ölçeğinin faktör yapısını belirlemek için ise Açıklayıcı Faktör Analizi (AFA) yapılmıştır. Kaiser'in örneklem uygunluğu ölçümü .957 olarak bulunmuş ve Bartlett'in küresellik testi sonuçları değeri anlamlı çıkmıştır ( $\chi^2$  (df=903) = 15408.501). Bu da değişkenlerin faktör analizi için uygun olduğunu göstermektedir. AFA sonuçlarına göre ölçek üç faktörlü bir yapıya sahiptir ve 41 maddeden oluşmaktadır. Açıklanan toplam varyans %53,71 olarak bulunmuştur. Normallik testi sonuçlarına bakıldığında ise verinin normal dağılıma sahip olduğu söylenebilir. Araştırmanın ikinci çalışmasında doğrulayıcı faktör analizi ile üç faktörlü yapının verilerle iyi uyum gösterip göstermediği incelenmiştir. DFA sonuçlarına göre üç faktörlü yapının verilerle iyi uyum gösterdiği sonucu ortaya çıkmıştır. Son olarak geliştirilen Siber Suç Farkındalık Ölçeği ile Dijital Veri Güvenliği Farkındalığı Ölçeği arasındaki benzerlik korelasyon analizi ile test edilmiştir. Sonuçlar iki ölçek arasında pozitif yönde ve anlamlı bir ilişki olduğunu göstermektedir ( $r= 0,53$ ,  $p<0,001$ ). Ölçeğin alt boyutları siber ortamda yer alan suçlar, siber ortama ve kişisel verilere yönelik suçlar ve gizlilik ve güvenlik olarak isimlendirilmiştir. Siber ortamda yer alan suçlar bilişim sistemi ile ilgili ifadeleri içermektedir. Bu alt boyutta bilişim sistemine girme, siber ortamda kumar oynama ve banka kartı ile kişisel bilgilerin ele geçirilmesi ile ilgili ifadeler yer almaktadır. İkinci alt boyut ise siber ortama ve kişisel verilere yönelik suçları içermektedir. Üçüncü alt boyutta ise gizlilik ve güvenlik ile ilgili ifadelere değinilmiştir. Bu alt boyutta ise özel hayatın gizliliği, haberleşmenin engellenmesi, dinlenilmesi ve kaydedilmesi ile ilgili ifadeler yer almaktadır.

Sonuç olarak, bu çalışmada geliştirilen Siber Suç Farkındalık Ölçeğinin bireylerin siber suç farkındalık düzeylerini belirlemede kullanılabilecek geçerli ve güvenilir bir ölçek olduğu söylenebilir. Bu ölçek kullanılarak bireylerin siber suçlara yönelik farkındalık düzeyleri belirlenebilir ve bu farkındalıkların arttırılmasına yönelik çalışmalar yapılabilir.

Bu çalışma ile ilgili önerilere yer verecek olursak her geçen gün siber suçlara ilişkin yeni yöntemler geliştirilmektedir. Bundan dolayı siber saldırı ve tehditlere uğrayan mağdurlar gün be gün artmakta bu durum ise ülkenin sosyal ve ekonomik durumuna zarar vermektedir (Sönmez, 2017). Bu durumun azaltılması için adli bilişim uzmanları tarafından tüm kullanıcılara özellikle üniversite öğrencilerine siber suçlar konusunda bilgilendirme yapılması önerilmektedir.

Siber suçun olumsuz etkileri konusunda farkındalık oluşturmak gerekmektedir. Özellikle genç kullanıcıların siber suçların yanlış etkileri konusunda yeterli bilgiye sahip olmaları ifade edilmektedir (Chel, 2018). Geliştirilen ölçek bireylerin siber suçlar konusundaki farkındalık düzeylerini ölçerek alana önemli katkı sağlayabilir.

Siber suçlar konusundaki farkındalık eksikliği, siber suç işlemeye veya siber suça maruz kalmaya neden olabilecek en önemli faktörlerden birisidir. Geliştirilen ölçek kullanıcıların siber suçlara ve siber suç türlerine yönelik eksikliklerinin tespit edilmesi konusunda kolaylaştırıcı olabilir.

Bilgisayar ve internet kullanıcılarının birçoğunun siber riskler, tehditler ve suçlar konusunda bilgi düzeylerinin düşük olduğu ifade edilmektedir (Topal, Geçer, Akkaya, Güzel ve Of, 2019). Bu tez çalışmasında elde edilen bulgular ile siber suç konusunun önemine dikkat çekilerek bu konudaki farkındalık düzeyinin artmasına katkı sağlanabilir.

Siber suçlar internet ve bilgisayar kullanımına bağlı olarak gün geçtikçe artış göstermektedir. Bu nedenle kullanıcıların özellikle üniversite öğrencilerinin yeterince bilgilendirilmesi ve bu konu hakkında farkındalık oluşturulması gerekmektedir. Siber suçlar konusunda seçmeli dersler açılması ya da zorunlu olan bilişim teknolojileri dersi müfredatına siber suçlar konusunun dahil edilmesi önerilmektedir. Diğer taraftan üniversitede eğitim veren akademisyenlere de siber suçlar ve türleri konusunda hizmet içi eğitim ve seminerler verilmesi önerilmektedir.

Covid-19 pandemisiyle birlikte insanlar birçok ihtiyaçlarını siber ortamda karşılamak durumunda kalmıştır. Pandemi ile en çok artış gösteren davranışlardan biri de internet alışverişidir. İnternet kullanım oranlarındaki bir dramatik yükseliş siber saldırı ve tehditlerin sayısının ve niteliğinin artmasına neden olmuştur. Bu tez çalışmasında son zamanlarda artış gösteren siber suçlar konusuna odaklanılarak ve bu konuda bir ölçme aracı geliştirilerek alana katkı sağlanmıştır.

Ülkemizde Emniyet Genel Müdürlüğüne bağlı Siber Suçlarla Mücadele Daire Başkanlığı, Jandarma Genel Komutanlığına bağlı MEBS Başkanlığı ve Bilgi ve Teknoloji Kurumuna bağlı Siber Olaylara Müdahale Merkezi (USOM) kurulmuştur. Bu merkezlerde siber suçun tanımına, siber suç türlerine ve ülkemize yönelik siber saldırı ve tehditlerin nasıl gerçekleştiğine en çok hangi alanlara yönelik gerçekleştiğine dair bilgiler yer almaktadır. Bunların dışında Bilgi ve Teknoloji Kurumu Hazine ve Maliye Bakanlığıyla beraber bir milyon istihdam projesi başlatılmış olup siber suç ve siber olaylarla ilgili katılım sertifikalı eğitimler verilmektedir. Bu tür eğitimlere üniversite öğrencileri yönlendirilmeli ve katılım sağlamaları hususunda teşvik edilmelidir.

Demografik bulgulara katılımcıların çoğunluğu günde en az 3-4 saat İnternette vakit geçirmektedir. Ayrıca bulgular katılımcılarının çoğunun (%92,8) mobil internet kullandığını göstermektedir. Katılımcıların %74,6'sı e-devlet, %71,4'ü ise e-ticaret hizmetlerini kullanmaktadır. Bu bulgular siber suç ve tehditler konusunda farkındalık oluşturma'nın ne denli önem arz ettiğini göstermektedir.

Bu çalışmanın bulgularına göre katılımcıların çoğunluğunun (%88,2) siber suç eğitimi almadıkları sonucu ortaya çıkmıştır. Üniversiteler siber suçlar alanında çalışmalar yapan ilgili kuruluşlarla iş birliği yaparak tüm öğrencilere siber suçlar konusunda farkındalık eğitimleri sağlayabilir.

Literatür taraması yapıldığında siber suç alanında bilimsel birçok çalışma, yayın, makale ve tez hazırlandığı görülmüş fakat bireylerin siber suç farkındalık düzeyini belirlemeye yönelik hazırlanmış, ilgili mevzuata uygun Türkçe bir ölçek tespit edilememiştir. Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı siber suç mevzuatı ve Türk Ceza Kanunu'nun bilişim suçları kapsamında değerlendirilen siber suç türleri dikkate alınarak geliştirilmiş olan bu ölçeğin alana önemli katkı sağlayacağı düşünülmektedir. Geliştirilen ölçek banka, KOBİ, adliye gibi özel ve resmî kurumlarda çalışan personellere de uygulanabilir.

## KAYNAKÇA

- Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, 33(3), 237-248. DOI: 10.1080/0144929X.2012.708787.
- Abuda, B. F. Q., Rivera, K. D. ve Noroña, R. V. (2020). Predictive validity of a cybercrime awareness tool: The case of senior high school students in a philippine secondary school. *International Journal in Information Technology in Governance, Education and Business*, 2(1), 18-26.
- Agatston, P. W., Kowalski, R. ve Limber, S. (2007). Students' perspectives on cyber bullying. *Journal of Adolescent Health*, 41(6), 59-60. DOI: 10.1016/j.jadohealth.2007.09.003.
- Akgün, Ö. ve Topal, M. (2015). Eğitim fakültesi son sınıf öğrencilerinin bilişim güvenliği farkındalıkları: Sakarya Üniversitesi Eğitim Fakültesi örneği. *Sakarya University Journal of Education*, 5(2), 98-121. DOI: 10.19126/suje.73391.
- Akkoyun, F. (2001). *Gestalt terapi*. Ankara: Nobel Yayınları.
- Aksoğan, M., Bayer, H., Gülada, M. O. ve Çelik, E. (2018). İletişim fakültesi öğrencilerinin siber güvenlik farkındalığı: İnönü Üniversitesi örneği. *Kesit Akademi Dergisi*, 4(13), 271-288.
- Alemdaroglu, A. (2020). *Çalışanların bilgi güvenliği farkındalığına ilişkin algıları: bankacılık sektöründe bir araştırma*. Yayınlanmamış yüksek lisans tezi. İstinye Üniversitesi Sosyal Bilimler Enstitüsü İşletme, İstanbul.
- Al-Janabi, S. ve Al-Shourbaji, I. (2016). A study of cyber security awareness in educational environment in the middle east. *Journal of Information & Knowledge Management*, 15(01), 1650007. DOI: 10.1142/S0219649216500076.
- Alotaibi, F., Furnell, S., Stengel, I. ve Papadaki, M. (2016, December). A survey of cyber-security awareness in Saudi Arabia. In *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)* (pp. 154-158). IEEE. DOI: 10.1109 / ICITST.2016.7856687.

- Anderson, N. D., Lau M. A., Segal Z. V. ve ark. (2007). Mindfulnessbased stress reduction and attentional control. *Clin Psychol Psychother*, 14:449-463. DOI: 10.1002/cpp.544.
- Arpaci, I. (2021). Relationships between early maladaptive schemas and smartphone addiction: The moderating role of mindfulness. *International Journal of Mental Health and Addiction*, 11(1). <https://doi.org/10.1007/s11469-019-00186-y>.
- Arpaci, I., & Gundogan, S. (2021). Mediating role of psychological resilience in the relationship between mindfulness and nomophobia. *British Journal of Guidance and Counselling*. <https://doi.org/10.1080/03069885.2020.1856330>.
- Arpaci, I., Baloglu, M., & Kesici, Ş. (2019). A multi-group analysis of the effects of individual differences in mindfulness on nomophobia. *Information Development*, 35(2), 333-341. <https://doi.org/10.1177/0266666917745350>.
- Aslay, F., Handan, Ç. ve Üstün, Ö. (2019). Yükseköğretim kurumlarında bilgi güvenliği farkındalık düzeylerinin ölçülmesi. *Yönetim Bilişim Sistemleri Dergisi*, 5(2), 1-11.
- Avcı, Ü. ve Oruç, O. (2020). Üniversite Öğrencilerinin Kişisel Siber Güvenlik Davranışları ve Bilgi Güvenliği Farkındalıklarının İncelenmesi.
- Aydaner, G. (2019). *Genç tüketicilerin sosyal mühendislik ile siber güvenlik farkındalıklarının online alışveriş niyetleri üzerindeki etkisinin ölçülmesi*. Yayınlanmamış yüksek lisans tezi. Bandırma Onyediy Eylül Üniversitesi Sosyal Bilimler Enstitüsü, Bandırma.
- Baer, R. (2003). Mindfulness training as a clinical intervention: A conceptual and empirical review. *Clinical Psychology: Science and Practice*, 10(2), 125-143. DOI: <https://doi.org/10.1093/clipsy.bpg015>.
- Bansal, A. ve Simon, M. C. (2018). Glutathione metabolism in cancer progression and treatment resistance. *Journal of Cell Biology*, 217(7), 2291-2298.
- Bansal, P. (2018). Cybercrime awareness among prospective teachers in relation to institutional management and behavioural pattern types. *Online international*

*interdisciplinary research journal*, Volume-08, Issue-03, May-June 2018 issue, ISSN 2249-9598.

- Bayram, N. ve Saylı, M. (2013). Üniversite öğrencileri arasında siber zorbalık davranışı. *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, 71(1), 107-116.
- Bıçakcı, S. (2019). “Siber Güvenlik ve Savunma”, *Güvenlik Yazıları Serisi*, No.42, Kasım 2019.
- Bıkmaz, Z. (2017). Sağlık yönetimi bölümü öğrencilerinin mobil güvenlik farkındalığı ve dijital veri güvenliği farkındalıklarının belirlenmesi. *Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi*, 1(1), 22-30.
- Biber, S. K. ve Biber, M. (2018). Ortaöğretim öğrencilerinin bilişim kültüründe bilgi güvenliği farkındalıklarının incelenmesi. *Uluslararası Bilimsel Araştırmalar Dergisi (IBAD)*, 578-589. DOI: 10.21733/ibad.476506.
- Bishop, S. R., Lau, M., Shapiro, S., Carlson, L., Anderson, N. D., Carmody, J., ... Devins, G. (2004). Mindfulness: a proposed operational definition. *Clinical Psychology: Science and Practice*, 11(3), 230-241. <https://doi.org/10.1093/clipsy.bph077>.
- Brown, K. W. ve Ryan, R. M. (2003). The benefits of being present: Mindfulness and its role in psychological wellbeing. *Journal of Personality and Social Psychology*, 84(4), 822. <https://doi.org/10.1037/0022-3514.84.4.822>.
- Brown, K. W., Ryan, R. M. ve Creswell, J. D. (2007). Mindfulness: Theoretical foundations and evidence for its salutary effects. *Psychological Inquiry*, 18(4), 211-237. DOI: <https://doi.org/10.1037/0022-3514.84.4.822>.
- Brown, T. A. (2006). Confirmatory factor analysis for applied research. New York: Guilford Press.
- BTK (2009). Siber güvenliğin sağlanması: Türkiye’de Mevcut Durum ve Alınması Gereken Tedbirler. <https://www.btk.gov.tr/File/Documents/Sayfalar/SiberGuvencikFsg.pdf> adresinden alınmıştır.

- Budak, Ö. (2015). *Bilişim öğrencilerinin siber suç farkındalığı: Erzurum ili mesleki ve teknik liseler örneği*. Yayınlanmamış yüksek lisans tezi. Atatürk Üniversitesi Eğitim Bilimleri Enstitüsü, Erzurum.
- Bulgurcu, B., Cavusoglu, H. ve Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, 523-548.
- Büyüköztürk, Ş. (2004). *Veri analizi el kitabı*. Ankara: Pegem Yayıncılık.
- Canbek, G. ve Sağıroğlu, G. (2006). Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme. *Politeknik Dergisi*, 9(3), 165-174.
- Cengiz, G. (2021). Siber Suçlar, Sosyal Medya ve Siber Etik. *İletişim Çalışmaları Dergisi*, 7(3), 407-424.
- Chambers, R., Gullone, E. ve Allen, N. B. (2009). Mindful emotion regulation: An integrative review. *Clinical psychology review*, 29(6), 560-572. DOI: <https://doi.org/10.1016/j.cpr.2009.06.005>.
- Chambers, R., Lo, B.C.Y. ve Allen N.B. (2009). The impact of intensive mindfulness training on attentional control, cognitive style, and affect. *Cognitive Ther Res*, 32: 303-322. DOI: <https://doi.org/10.1007/s10608-007-9119-0>.
- Chel, M. M. (2018). A study on awareness among women in educational institutions towards cybercrime. *Research and development*, 3(1).
- Coffey, K.A. ve Hartman, M. (2008). Mechanisms of action in the inverse relationship between mindfulness and psychological distress. *Comp Health Prac Rev*, 13:79-91. DOI: <https://doi.org/10.1177/1533210108316307>.
- Cone, B. D., Irvine, C. E., Thompson, M. F. ve Nguyen, T. D. (2007). A video game for cyber security training and awareness. *Computers & security*, 26(1), 63-72. DOI: <https://doi.org/10.1016/j.cose.2006.10.005>.
- Çatak, P. D. ve Ögel, K. (2010). Farkındalık temelli terapiler ve terapötik süreçler. *Klinik Psikiyatri*, 13(1), 85-91.

- Çatuk, C. (2018). *Siber riskler karşısında KOBİ'lerin bilgi güvenliği farkındalıklarını ölçen bir ölçek geliştirme: Gaziantep örnekleme*. Yayınlanmamış doktora tezi. Hasan Kalyoncu Üniversitesi Sosyal Bilimler Enstitüsü, Gaziantep.
- Çelik, Ç. (2020). Kalite yönetim direktörlerinin bilgi güvenliği farkındalığı: İstanbul ili örneği. *Sağlıkta Performans ve Kalite Dergisi*, 17(2), 29-48.
- Çetin, H. (2014). Kişisel veri güvenliği ve kullanıcıların farkındalık düzeylerinin incelenmesi. *Akdeniz İİBF Dergisi*, 14(29), 86-105.
- Çetinkaya, L., Güldüren, C. ve Keser, H. (2017). Öğretmenler için bilgi güvenliği farkındalık ölçeği (bgfö) geliştirme çalışması. *Milli Eğitim Dergisi*, 46(216), 33-52.
- Demir, G. T., ve Cicioğlu, H. İ. (2020). Dijital oyun bağımlılığına ilişkin farkındalık ölçeği (Dobifö): Geçerlik ve güvenirlik çalışması. *Avrasya Spor Bilimleri ve Eğitim Dergisi*, 2(1), 1-17.
- Dökmen, Ü. (2000). *Farkına varmak: Yarına kim kalacak evrenle uyumlaşma sürecinde varolmak gelişmek uzlaşmak*. (1. Baskı). İstanbul: Sistem Yayıncılık, 122-139.
- Dönmez, G. (2019). *Lise öğrencilerinin bilgi güvenliği farkındalığı ile dijital okuryazarlığı arasındaki ilişkinin incelenmesi*. Yayınlanmamış yüksek lisans tezi. Hacettepe Üniversitesi Eğitim Bilimleri Enstitüsü, Ankara.
- Duman, E. (2019). *Velilere yönelik geliştirilen siber zorbalık farkındalık eğitiminin etkisinin incelenmesi*. Yayınlanmamış yüksek lisans tezi. Bursa Uludağ Üniversitesi Eğitim Bilimleri Enstitüsü, Bursa.
- Dülger, M. V. (2012). *Bilişim Suçları ve İnternet İletişim Hukuku*. (2. Baskı). Ankara: Seçkin Yayıncılık.
- EGM. (2020). Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı. <https://www.egm.gov.tr/siber/sibersucnedir> adresinden alınmıştır.
- Eminağaoğlu, M. ve Gökşen, Y. (2009). Bilgi güvenliği nedir, ne değildir? Türkiye'de bilgi güvenliği sorunları ve çözüm önerileri. *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 11(4), 01-15.

- Engin, E. ve am, O. (2005). Farkındalık ve psikiyatri hemřirelięi. *Ege niversitesi Hemřirelik Yksek Okulu Dergisi*, 21(2), 159-168.
- Erdoęan, Y. (2012). Biliřim sistemine girme ve kalma suu. *Dokuz Eyll niversitesi Hukuk Fakltesi Dergisi*, 12, 1363-1433.
- Erdoęmuř, A. (2017). *niversite ęrencilerinin bilgi gvenlięi kazanımlarının, farkındalıkları zerindeki etkilerinin analizi*. Yayınlanmamıř yksek lisans tezi. Afyon Kocatepe niversitesi Fen Bilimleri Enstits, Afyon.
- Erol, S. E. ve Saęiroęlu, ř. (2016). Siber gvenlik farkındalıęı iin yetenek tabanlı dinamik model. Yayınlanmamıř yksek lisans tezi. Gazi niversitesi Fen Bilimleri Enstits, Ankara.
- Ford, C. (2016). Does mindfulness reduce attentional negativity bias and depressive symptoms? (Doctoral Thesis). Available from ProQuest Dissertations & Theses Global. (1830450395).
- Goel, U. (2014). B. Ed ęretmen eęitiminde siber su-a arařtırmasına ynelik farkındalık. *Learning Community-An International Journal of Educational and Social Development*, 5 (2and3), 107-117. DOI: <https://doi.org/10.1016/j.sbspro.2015.04.787>.
- Gkearsan, ř., Gnbatar, M. S. ve Sarıtepeci, M. (2021). Ortaęretim ęrencilerinin bilgi gvenlięi farkındalıklarının incelenmesi. *Yznc Yıl niversitesi Eęitim Fakltesi Dergisi*, 18(1), 354-373. DOI: <https://doi.org/10.33711/yyuefd.867015>.
- Gkearsan, ř., Nezgıtlı, S. ve akır, H. (2020). Biliřim suu haberlerinin basında sunumu: 2009-2019 yılları arası evrimii gazete haberleri rneklemi. *Bilgi ve İletiřim Teknolojileri Dergisi*, 2(2), 149-160.
- Gldren, C., etinkaya, L. ve Keser, H. (2016). Ortaęretim ęrencilerine ynelik bilgi gvenlięi farkındalık lęi (BGF) geliřtirme alıřması. *Elementary Education Online*, 15(2).
- Grbz, B. ve Karakk, S. (2007). Boř zaman engelleri lęi-28: lek geliřtirme, geerlik ve gvenirlik alıřması. *Gazi Beden Eęitimi ve Spor Bilimleri Dergisi*, 12(1), 3-10.

- Hacımustafaoğlu, R. (2019). *Ortaöğretim öğrencilerinin bilgi güvenliği farkındalık düzeylerinin Siber mağdur olma durumlarına etkisinin incelenmesi*. Yayınlanmamış yüksek lisans tezi. Sakarya Üniversitesi Eğitim Bilimleri Enstitüsü, Sakarya.
- Hayes, A.M. ve Feldman, G. (2004). Clarifying the construct of mindfulness in the context of emotion regulation. *Clin Psychol Sci Pract*, 11:255-262. DOI: <https://doi.org/10.1093/clipsy.bph080>.
- Hinduja, S., ve Patchin, J. W. (2015). *Bullying beyond the schooyard: Preventing and responding to cyberbullying*. Second Edition. California: Corwin Press.
- Hinkin, T. R. (1995). A review of scale development practices in the study of organizations. *Journal of management*, 21(5), 967-988.
- Idan, A. (2020). *Ulusal ve uluslararası güvenliğin bileşeni olarak siber güvenlik: Irak örneği*. Yayınlanmamış doktora tezi. Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Konya.
- Intawa. (2011). Integrating Awareness. <https://www.intawa.com.au/gestalt-awareness-and-dialogue/> adresinden alınmıştır.
- İlbaş, Ç. ve Köksal, M. A. (2011). Türkiye Bilişim Suçları Raporu: 1990-2011 Temmuz. 2. Uluslararası Bilişim Hukuku Kurultayı Bildiriler Kitabı. İzmir.
- İlhan, E. L. ve Esentürk, O. K. (2015). Zihinsel engelli bireylerde sporun etkilerine yönelik farkındalık ölçeği (ZEBSEYFÖ) geliştirme çalışması. *CBÜ Beden Eğitimi ve Spor Bilimleri Dergisi*, 9(1), 19-36.
- Kabat-Zinn J. (2003). Mindfulness-based interventions in context: past, present, and future. *Clin Psychol Sci Pract*, 10(2):144- 156. DOI: <https://doi.org/10.1093/clipsy/bpg016>.
- Kapanoğlu, G. (2016). *Öğretmenlerin bilgi güvenliği farkındalığının incelenmesi*. Yayınlanmamış yüksek lisans tezi. Gazi Üniversitesi Eğitim Bilimleri Enstitüsü, Ankara.
- Karagiannopoulos, V., Sugiura, L. ve Kirby, A. L. (2019). The portsmouth cybercrime awareness clinic project: Key findings and recommendations.

- Keleş, Ö. (2007). *Sürdürülebilir yaşama yönelik çevre eğitimi aracı olarak ekolojik ayak izinin uygulanması ve değerlendirilmesi*. Yayınlanmamış Doktora Tezi, Gazi Üniversitesi, Eğitim Bilimleri Enstitüsü, Ankara.
- Keser, H. ve Güldüren, C. (2015). Bilgi güvenliği farkındalık ölçeği (bgfö) geliştirme. *Kastamonu Eğitim Dergisi*, 23(3), 1167-1184.
- Kline, R. B. (2005). *Principles and practice of structural equation modeling* (2nd ed). New York: Guilford.
- Korkmaz, Ö. (2018). Üniversite öğrencilerinin internet ve veri güvenliği farkındalıkları internet and data security awareness of university students. *Journal of Social And Humanities Sciences Research (JSHSR)*, 5(25), 2222-2229.
- Korpela, K. (2015). Improving cyber security awareness and training programs with data analytics. *Information Security Journal: A Global Perspective*, 24(1-3), 72-77. DOI: <https://doi.org/10.1080/19393555.2015.1051676>.
- Kritzinger, E. ve von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security*, 29(8), 840-847.
- Kruger, H. A. ve Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security*, 25(4), 289-296. DOI: <https://doi.org/10.1016/j.cose.2006.02.008>.
- Küçükvardar, M. (2018). Suç olgusunun değişen yüzü: Siber suçlar. *International Journal of Information, Technology and Philosophy*, 1(2), 1-18.
- Lafvermez, E. (2018). *Lise Öğrencilerinin Siber Suç Algı Düzeylerinin Farklı Değişkenler Açısından İncelenmesi (Kırşehir İli Örneği)*. Yayınlanmamış yüksek lisans tezi. Selçuk Üniversitesi Eğitim Bilimleri Enstitüsü, Konya.
- Lang, M., Devitt, J., Kelly, S., Kinneen, A., O'Malley, J. ve Prunty, D. (2009, September). Social networking and personal data security: a study of attitudes and public awareness in Ireland. In *2009 International Conference on Management of e-Commerce and e-Government* (pp. 486-490). IEEE.

- Leary, M. R. ve Tate, E. B. (2007). The multi-faceted nature of mindfulness. *Psychological Inquiry*, 18 (4), 251- 255. DOI: <https://doi.org/10.1080/10478400701598355>.
- Lynch, T. R. ve Bronner, L. L. (2006). Mindfulness and dialectical behaviour therapy: application with depressed older adults with personality disorders. *Mindfulness and Acceptance Based Treatment Approaches*, 1. Baský, R. Baer (Ed), USA, Academic Press, s.217-236. DOI: <https://doi.org/10.1016/B978-012088519-0/50011-3>.
- Mart, C. T. (2012). Developing speaking skills through reading. *International Journal of English Linguistics*, 2(6), 91.
- Mart, İ. (2012). *Bilişim kültüründe bilgi güvenliği farkındalığı*. Yayınlanmamış yüksek lisans tezi. Kahramanmaraş Sütçü İmam Üniversitesi Fen Bilimleri Enstitüsü, Kahramanmaraş.
- McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M. ve Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior*, 69, 151-156. DOI: <https://doi.org/10.1016/j.chb.2016.11.065>.
- Mishna, F., Cook, C., Gadalla, T., Daciuk, J. ve Solomon, S. (2010). Cyber bullying behaviors among middle and high school students. *American journal of orthopsychiatry*, 80(3), 362-374. DOI: <https://doi.org/10.1111/j.1939-0025.2010.01040.x>.
- Mishna, F., Saini, M. ve Solomon, S. (2009). Ongoing and online: Children and youth's perceptions of cyber bullying. *Children and Youth Services Review*, 31(12), 1222-1228. DOI: <https://doi.org/10.1016/j.childyouth.2009.05.004>.
- Mitmansgruber, H., Beck T.N., Höfer S. ve ark. (2009). When you don't like what you feel: experiential avoidance, mindfulness and meta-emotion in emotion regulation. *Pers Indiv Differ*, 46: 448- 453. DOI: <https://doi.org/10.1016/j.paid.2008.11.013>.
- Mokha, A.K. (2017). Siber suç ve güvenlik farkındalığı üzerine bir araştırma. *Beşerî ve Sosyal Bilimler Araştırma Dergisi*, 8 (4), 459-464. DOI: <https://doi.org/10.5958/2321-5828.2017.00067.5>.

- Nield, J., Scanlan, J. ve Roehrer, E. (2020). Exploring consumer information-security awareness and preparedness of data-breach events. *Library Trends*, 68(4), 611-635. DOI: <https://doi.org/10.1353 / lib.2020.0014>.
- Okul, T., Şimşek, G., Hafçı, B. ve Barış, Z. (2018). Bilgi güvenliği farkındalığı: Kuşadası'ndaki konaklama işletmesi yöneticileri üzerine bir uygulama. *Uluslararası Türk Dünyası Turizm Araştırmaları Dergisi*, 3(2), 189-201.
- Özbek, Y. (2019). *Öğretmen adaylarının siber güvenlik farkındalıklarının incelenmesi*. Yayınlanmamış yüksek lisans tezi. Necmettin Erbakan Üniversitesi Eğitim Bilimleri Enstitüsü, Konya.
- Özcan, M. (2004). Yeni Milenyum'da yeni tehdit: Siber terör. *Türk Harb-İş Dergisi*, (210), s.36-42.
- Özdemir, A. (2019) *Kamu kurum ve kuruluşlarında bilgi güvenliği farkındalığı*. Yayınlanmamış Yüksek Lisans Tezi. Gazi Üniversitesi Bilişim Enstitüsü, Ankara.
- Öztemiz, S. ve Yılmaz, B. (2013). Bilgi merkezlerinde bilgi güvenliği farkındalığı: Ankara'daki üniversite kütüphaneleri örneği. *Bilgi Dünyası*, 14(1), 87-100.
- Peker, B. (2010). *Bilişim suçları ve bilişim güvenliğinin ulusal ve uluslararası boyutu*. Yayınlanmamış yüksek lisans tezi. Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Konya.
- Pekşen Süslü, D. (2016). *Lise öğrencilerinde siber zorbalık ve siber mağduriyetin benlik saygısı, anne, baba ve akran ilişkiler açısından incelenmesi*. Yayınlanmamış doktora tezi. Maltepe Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.
- Psikosentez. (2018). Gestalt terapi ve farkındalık nedir? <https://www.psikosentez.com/gestalt-terapi-ve-farkindalik-nedir> adresinden alınmıştır.
- Rajasekar S. (2011). Cyber Crime Awareness Scale. KacheriGhat: National Psychological Corporation.

- Rezgui, Y. ve Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security*, 27(7-8), 241-253. DOI: <https://doi.org/10.1016/j.cose.2008.07.008>.
- Roemer, L., Lee, J. K., Salters-Pedneault, K. ve ark. (2008). Mindfulness and emotion regulation difficulties in generalized anxiety disorder: Preliminary evidence for independent and overlapping contributions. *Behav Ther*, 40:142-154. DOI: <https://doi.org/10.1016/j.beth.2008.04.001>.
- Sağıroğlu, Ş. (2018). *Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık*. Ankara: Grafiker Yayınları.
- Schmertz, S. K., Anderson, P. L. ve Robins D. L. (2009). The relation between self-report mindfulness and performance on tasks of sustained attention. *J Psychopathol Behav Assess*, 31: 60-66.
- Seçer, D. (2013). *SPSS ve LISREL ile pratik veri analizi*. Ankara: Anı Yayıncılık.
- Seligman, L. (2006). *Danışmanlık ve psikoterapi teorileri: Sistemler, stratejiler ve beceriler*. (2. Baskı). Upper Saddle Nehri, New Jersey: Pearson Education, Ltd.
- Shapiro, S. L., Carlson, L., Astin, J. A. ve Freedman, B. (2006). Mechanisms of mindfulness. *Journal of Clinical Psychology*, 62, 373e386. DOI: <https://doi.org/10.1002/jclp.20237>.
- Shaw, R. S., Chen, C. C., Harris, A. L. ve Huang, H. J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education*, 52(1), 92-100. DOI: <https://doi.org/10.1016/j.compedu.2008.06.011>.
- Siberay (2020). Siber Suçlar. <https://www.siberay.com/siber-suclar> adresinden alınmıştır.
- Solak, D. ve Topaloglu, M. (2015). The perception analysis of cyber crimes in view of computer science students. *Procedia-Social and Behavioral Sciences*, 182, 590-595. DOI: <https://doi.org/10.1016/j.sbspro.2015.04.787>.
- Solmaz, M. (2020) *Öğretmen adaylarının siber bilgi güvenliği farkındalıklarının ve dijital vatandaşlık düzeylerinin farklı değişkenler açısından incelenmesi*. Yayınlanmamış Yüksek Lisans Tezi. Mersin Üniversitesi Eğitim Bilimleri Enstitüsü, Mersin.

- Sönmez, Ü. (2017). Bilişim sistemleri aracılığıyla dolandırıcılık suçu. *Dicle Üniversitesi Adalet Meslek Yüksekokulu Dicle Adalet Dergisi*, 1(2), 47-68.
- Şahinaslan, E., Kandemir, R. ve Şahinaslan, Ö. (2009). *Bilgi güvenliği farkındalık eğitimi örneği*. XI. Akademik Bilişim Konferansı Bildirilerinde sunuldu, Şanlıurfa.
- Şahinaslan, E., Kantürk, A., Şahinaslan, Ö. ve Borandağ, E. (2009). Kurumlarda bilgi güvenliği farkındalığı, önemi ve oluşturma yöntemleri. *Akademik Bilişim*, 9, 11-13.
- Taylor, P. R. (2020). Cyber crime awareness: a comparative study of male and female b. ed. trainees.
- Taner, E. ve Kılıç, İ. (2019). Güvenlik güçlerinin bilgi güvenliği farkındalığını belirlemeye yönelik bir araştırma. *Güvenlik Bilimleri Dergisi*, 8(2), 253-269. DOI: <https://doi.org/10.28956/gbd.646321>.
- Tavlaş, H. (2019). *Ortaöğretim kurumlarında uygulanan siber güvenlik farkındalık eğitiminin öğrenciler üzerinden etkisi*. Yayınlanmamış yüksek lisans tezi. İstanbul Şehir Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.
- Teasdale, J. D. (1999). Metacognition, mindfulness and modification of mood disorders. *Clin Psychol Psychother*, 6: 146-155. DOI: [https://doi.org/10.1002/\(SICI\)1099-0879\(199905\)6:2<146::AID-CPP195>3.0.CO;2-E](https://doi.org/10.1002/(SICI)1099-0879(199905)6:2<146::AID-CPP195>3.0.CO;2-E).
- Tekerek, M. ve Tekerek, A. (2013). Öğrencilerin bilgi güvenliği farkındalığı üzerine bir araştırma. *Turkish Journal of Education*, 2(3), 61-70.
- Tibi, M. H., Hadeje, K., & Watted, B. (2019). Cybercrime awareness among students at a teacher training college. *Int. J. Comput. Trends Technol*, 67(6), 11-17.
- Tokunaga, R. S. (2010). Following you home from school: A critical review and synthesis of research on cyberbullying victimization. *Computers in Human Behavior*, 26(3), 277–287. DOI: 10.1016/j.chb.2009.11.014.
- Topal, A. D., Geçer, A. K., Akkaya, O., Güzel, Y. E., ve Mustafa, O. F. (2019). Öğretmen adaylarının bilişim suçları ile ilgili tutum ve bilgi düzeylerinin

incelenmesi. *Pamukkale Üniversitesi Eğitim Fakültesi Dergisi*, 45(45), 159-174. DOI: <https://doi.org/10.9779/puje.2018.227>.

UDHB (2016).2016-2019 Ulusal Siber Güvenlik Stratejisi. <http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf> adresinden alınmıştır.

Ümmühan, A. V. C. I. ve Arslan, E. (2019). Dijital veri güvenliği farkındalığı ve bilgi okuryazarlığı ile alınan hizmet içi eğitimin etkisi. *Ankara University Journal of Faculty of Educational Sciences (JFES)*, 52(3), 891-914.

Verplanken, B. ve Fisher, N. (2014). Habitual worrying and benefits of mindfulness. *Mindfulness*, 5(5), 566-573. DOI: <https://doi.org/10.1007/s12671-013-0211-0>.

Voltan-Acar, N. (2004). *Ne kadar farkındayım? Gestalt Terapi*. Ankara: Babil Yayıncılık.

Wang, S. J. (2007). Measures of retaining digital evidence to prosecute computer-based cyber-crimes. *Computer standards & interfaces*, 29(2), 216-223. DOI: <http://doi.org/10.1016/j.csi.2006.03.008>.

Webb, J., Ahmad, A., Maynard, S. B. ve Shanks, G. (2014). A situation awareness model for information security risk management. *Computers & security*, 44, 1-15. DOI: <https://doi.org/10.1016/j.cose.2014.04.005>.

Whitman, M. E. ve Mattord, H. J. (2012). *Principles of Information Security (Fourth Edition)*. Boston, USA: Course Technology.

Wikipedia (2020). Bilişim Suçları. [https://tr.wikipedia.org/wiki/Bilişim\\_suçları](https://tr.wikipedia.org/wiki/Bilişim_suçları) adresinden alınmıştır.

Yayla, H. G. (2018). *Fatih projesi uygulanan ve uygulanmayan okullardaki öğretmenlerin bilgi güvenliği farkındalığının incelenmesi*. Yayınlanmamış Yüksek Lisans Tezi. Ankara Üniversitesi Eğitim Bilimleri Enstitüsü, Ankara.

Yılmaz, E., Şahin, Y. L. ve Akbulut, Y. (2016). Öğretmenlerin dijital veri güvenliği farkındalığı. *Sakarya University Journal of Education*, 6(2), 26-45. DOI: <https://doi.org/10.19126/suje.29650>.

- Yılmaz, F. G. K., Yılmaz, R. ve Sezer, B. (2014). Üniversite öğrencilerinin güvenli bilgi ve iletişim teknolojisi kullanım davranışları ve bilgi güvenliği eğitimine genel bir bakış. *Bartın Üniversitesi Eğitim Fakültesi Dergisi*, 3(1), 176-199. DOI: <https://doi.org/10.14686/BUEFAD.201416213>.
- Yılmaz, F. ve Ezin, Ç. Ç. (2017). Ebeveynlerin bilgi güvenliği farkındalıklarının incelenmesi. *Eğitim Teknolojisi Kuram ve Uygulama*, 7(2), 41-57. DOI: <https://doi.org/10.17943/etku.288874>.
- Yılmaz, S. ve Sağıroğlu, Ş. (2013). Siber Güvenlik Risk Analizi, Tehdit ve Hazırlık Seviyeleri, 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, 20-21 Eylül, Ankara, 158-166.
- Yılmaz, Y. (2018). *Siber suç korkusu ve önlem alma stratejileri: Ankara'daki teknokentler örneği*. Yayınlanmamış Yüksek Lisans Tezi. Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.
- Yu, W., Xu, G., Chen, Z. ve Moulema, P. (2013, October). A cloud computing based architecture for cyber security situation awareness. *In 2013 IEEE conference on communications and network security (cNS)* (pp. 488-492). IEEE. DOI: <https://doi.org/10.1109/CNS.2013.6682765>.
- Zvolensky, M.J., Sondra. E.S., Alison, C.M. ve ark. (2006). Incremental validity of mindfulness based attention in relation to the concurrent prediction of anxiety and depressive symptomology and perceptions of health. *Cognit Behav Ther*, 35:145-158. DOI: <https://doi.org/10.1080/16506070600674087>.

## EKLER

### Ek1. Bilgi Formu ve Ölçme Araçları SSFÖ Öğeleri ve Puanlama

|                                                                    |                                                                                                     |
|--------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| 1.Alt Boyut: Siber Ortamda Yer Alan Suçlar                         |                                                                                                     |
| Madde20:                                                           | Siber ortamda yasak cihaz veya program (şifre kırıcı, e-imza oluşturma aracı vb.) kullanmak suçtur. |
| Madde21:                                                           | Bilişim sistemlerini kullanarak nitelikli hırsızlık yapmak suçtur.                                  |
| Madde22:                                                           | Siber ortamda nitelikli interaktif dolandırıcılık yapmanın suç olduğunu bilirim.                    |
| Madde23:                                                           | Bir başkasının e- mail hesabına izinsiz girmek suçtur.                                              |
| Madde26:                                                           | Kullanıcının bilgisi olmadan iletişim verisini (e-posta, adres, telefon numarası) kullanmak suçtur. |
| Madde27:                                                           | Siber ortamda soruşturma gizliliğini ihlal etmenin cezası vardır.                                   |
| Madde28:                                                           | Siber ortamda uyuşturucu madde kullanımını teşvik etmek suçtur.                                     |
| Madde29:                                                           | Siber ortamda Türk milletini, T.C. devletini, devletin kurum ve organların aşağılamak suçtur.       |
| Madde30:                                                           | Terör içerikli paylaşımların siber suç oluşturduğunun farkındayım.                                  |
| Madde31:                                                           | Donanım ve yazılımları korumaya yönelik programları etkisiz kılmak suçtur.                          |
| Madde32:                                                           | Siber ortamda asılsız siyasi ve askeri paylaşımlar yapmak suçtur.                                   |
| Madde33:                                                           | Siber ortamda çalışan bilgisayar sistemini engellemek/durdurmak suçtur.                             |
| Madde34:                                                           | Siber ortamda yasa dışı (çalıntı, sahte) ürünleri satmak suçtur.                                    |
| Madde36:                                                           | Siber ortamda bireyleri link aracılığıyla yasal olmayan sitelere yönlendirmek suçtur.               |
| Madde40:                                                           | Siber ortamda siber suç işlemeye yönelik yer ve imkan sağlamak suçtur.                              |
| Madde41:                                                           | Güvenilir olmayan borsalarda kripto para yatırımı yaparken dolandırılabilirim farkındayım.          |
| 2.Alt Boyut: Siber Ortama ve Kişisel Verilere Yönelik Siber Suçlar |                                                                                                     |
| Madde1:                                                            | Açık olan bilişim sistemine izinsiz girilmesi hukuki işlem gerektirir.                              |
| Madde2:                                                            | Kişiler arasındaki haberleşme gizliliğini ihlal etmek suçtur.                                       |
| Madde3:                                                            | Kişisel bilgilerin siber ortamda üçüncü şahıslarla paylaşılması suçtur.                             |
| Madde4:                                                            | Siber ortamda yasadışı bahis/kumar oynamak suçtur.                                                  |
| Madde5:                                                            | Siber ortamda şantaj yapmak suçtur.                                                                 |
| Madde6:                                                            | Siber ortamda hakaret içeren ifadeler kullanmanın suç olduğunu bilirim.                             |
| Madde7:                                                            | Siber ortamda izinsiz olarak ses veya görüntü kaydı yapılması suçtur.                               |
| Madde8:                                                            | Siber ortamda yasa dışı işlemlerle haksız çıkar sağlamanın suç olduğunu bilirim.                    |
| Madde9:                                                            | Bilişim sistemlerinin heklenmesi suçtur.                                                            |
| Madde10:                                                           | Siber taciz ve zorbalığın suç olduğunu bilirim.                                                     |
| Madde11:                                                           | E-imza verilerinin bir başkası tarafından kullanılmasının suç olduğunu bilirim.                     |
| Madde13:                                                           | Siber ortamda cinsel içerikli paylaşımlar yapılmayacağını farkındayım.                              |
| Madde14:                                                           | Bir başkasının sosyal medya hesap şifresini ele geçirerek işlem yapmak suçtur.                      |
| Madde17:                                                           | Siber ortamda sabotaj içerikli ifadelerin paylaşılması suçtur.                                      |

|                                   |                                                                                                                  |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------|
| Madde19:                          | Kötü amaçlı yazılımlar (virüs, Truva atı, solucan vb.) yoluyla bilişim sistemleri bozmanın suç olduğunu bilirim. |
| Madde24:                          | Bir web sitesine izinsiz girip bilgileri değiştirmek suçtur.                                                     |
| Madde35:                          | Siber ortamda fidye yazılımı (siber gasp) kullanarak para ve değerli eşya istemenin suç olduğunu bilirim.        |
| 3.Alt Boyut: Gizlilik ve Güvenlik |                                                                                                                  |
| Madde12:                          | Siber ortamda alıntı yaptığım eserleri telif hakkı ihlali yapmamak için kaynak olarak gösteririm.                |
| Madde15:                          | Siber ortamda özel hayatın gizliliği ihlal edenler hakkında suç duyurusunda bulunurum.                           |
| Madde16:                          | Siber ortamda kamu kuruluşları tarafından verilen web sitesi erişim engelleme kararlarına uyarım.                |
| Madde18:                          | Bilişim sistemindeki verilerin yok edilmesi suçtur.                                                              |
| Madde25:                          | Asılsız gönderilen spam maillerin suç oluşturduğunun farkındayım.                                                |
| Madde37:                          | Kripto paralar aracılığıyla yasa dışı işlemler yapmak suçtur.                                                    |
| Madde38:                          | Siber ortamda lisans sözleşmesine aykırı yazılım kullanmanın suç olduğunu bilirim.                               |
| Madde39:                          | Siber ortamda gizli olan görevlere ilişkin sırların açıklanması suçtur.                                          |

**Puanlama:** SSFÖ, 41 maddeden oluşturan siber suç farkındalığını değerlendiren “beş puanlı Likert tipi bir ölçektir. Tüm öğeler 5 puanlı ölçekle “kesinlikle katılmıyorum (1) ile “kesinlikle katılıyorum (5) arasında puanlanmaktadır. Ölçek puanları 41 ile 205 arasında değişmektedir. Yüksek puan, yüksek düzeyde siber suç farkındalığını işaret etmektedir.



**Ek3. Öz Geçmiş****ÖZ GEÇMİŞ**