ANKARA ÜNİVERSİTESİ
EĞİTİM BİLİMLERİ ENSTİTÜSÜ

BİLGİSAYAR VE ÖĞRETİM TEKNOLOJİLERİ EĞİTİMİ
ANABİLİM DALI
BİLGİSAYAR VE ÖĞRETİM TEKNOLOJİLERİ EĞİTİMİ
PROGRAMI

ÖĞRETMENLERİN KİŞİSEL SİBER GÜVENLİK FARKINDALIK DÜZEYLERİNİN FARKLI DEĞİŞKENLERE GÖRE DEĞERLENDİRİLMESİ

YÜKSEK LİSANS TEZİ

İMREN ALTINER

ANKARA
EYLÜL, 2021


ANKARA ÜNİVERSİTESİ
1946

ANKARA ÜNİVERSİTESİ
EĞİTİM BİLİMLERİ ENSTİTÜSÜ

BİLGİSAYAR VE ÖĞRETİM TEKNOLOJİLERİ EĞİTİMİ
ANABİLİM DALI
BİLGİSAYAR VE ÖĞRETİM TEKNOLOJİLERİ EĞİTİMİ
PROGRAMI

ÖĞRETMENLERİN KİŞİSEL SİBER GÜVENLİK FARKINDALIK DÜZEYLERİNİN FARKLI DEĞİŞKENLERE GÖRE DEĞERLENDİRİLMESİ

YÜKSEK LİSANS TEZİ

İMREN ALTINER

DANIŞMAN: PROF. DR. HAFİZE KESER

ANKARA
EYLÜL, 2021

Ankara Üniversitesi Eğitim Bilimleri Enstitüsü Müdürlüğüne,

İmren ALTINER adlı öğrencinin hazırladığı "Öğretmenlerin Kişisel Siber Güvenlik Farkındalık Düzeylerinin Farklı Değişkenlere Göre Değerlendirilmesi" başlıklı bu çalışma Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı / Bilgisayar ve Öğretim Teknolojileri Eğitimi Yüksek Lisans Programı'nda jüri üyelerince oy birliği ile **Yüksek Lisans Tezi** olarak kabul edilmiştir.

	Jüri Üyeleri	İmza
Başkan	Prof. Dr. Hafize KESER	……..
Üye	Prof. Dr. Yasemin GÜLBAHAR GÜVEN	……..
Üye	Doç. Dr. Levent ÇETİNKAYA	……..

ONAY

Bu tez Ankara Üniversitesi Lisansüstü Eğitim Öğretim Yönetmeliği'nin ilgili maddeleri uyarınca, jüri üyeleri tarafından …/…/20... tarihinde, Enstitü Yönetim Kurulu tarafından ise …/…/20... tarihinde kabul edilmiştir.

……

Prof. Dr. Yasemin KARAMAN KEPENEKCİ

Eğitim Bilimleri Enstitüsü Müdürü

ETİK İLKELERE UYGUNLUK BİLDİRİMİ

Tez içindeki bütün bilgileri akademik yazım kurallarına uygun biçimde raporlaştırdığımı ve bunları etik ilkelere (atıfta bulunulan tüm yapıtlara kaynaklarda yer verilmesi, tezde kullanılan bilgi ve belgelere resmi yollarla ulaşılması ve bunların aslı bozulmadan kullanılması vb.) uygun olarak elde ettiğimi ve sunduğumu bildiririm.

İmren ALTINER

ÖZET

ÖĞRETMENLERİN KİŞİSEL SİBER GÜVENLİK FARKINDALIK DÜZEYLERİNİN FARKLI DEĞİŞKENLERE GÖRE DEĞERLENDİRİLMESİ

ALTINER, İmren
Yüksek Lisans Tezi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı
Tez Danışmanı: Prof. Dr. Hafize KESER
Eylül, 2021, xiii + 100 sayfa

Bu araştırmanın temel amacı ortaokul kademesinde görev yapan öğretmenlerin siber güvenlik farkındalık düzeylerini farklı değişkenler açısından değerlendirmektir. Bu amaç doğrultusunda öğretmenlerin demografik özellikleri ve konu ile ilgili eğitim alma durumları gibi bilgiler nicel olarak, siber güvenliği artırmaya yönelik önerileri ise nitel olarak toplanmış ve araştırmada karma yöntem çeşitlerinden eşzamanlı tasarım kullanılmıştır. Katılımcılardan veri toplama aşamasında siber güvenlik farkındalık durumları Kişisel Siber Güvenliği Sağlama Ölçeği kullanılarak, yaş, cinsiyet, kıdem yılı gibi demografik bilgiler ile konu ile ilgili eğitim alma, siber güvenlik farkındalığını artırmaya yönelik önerileri gibi bilgiler için Kişisel Bilgiler Formu kullanılmıştır. Ankara il merkezinde bulunan ilçelere (Altındağ, Çankaya, Etimesgut, Gölbaşı, Keçiören, Mamak, Pursaklar, Sincan, Yenimahalle) bağlı kamu ortaokullarında görev yapan 455 öğretmene veri toplama araçları uygulanmıştır. Elde edilen verilerin analizinde frekans, yüzde, ilişkisiz iki örneklem arasındaki farkın manidarlığına bakmak için bağımsız örneklem t testi ve ikiden fazla olması durumunda tek yönlü varyans analizi (ANOVA) yapılmıştır. Karşılaştırması yapılacak gruplar arasında gözlenen farkların istatistiksel olarak manidar olması durumunda ise oluşan farkın hangi grup ya da gruplardan kaynaklandığını belirlemek için ise post-hoc testi türü olan Scheffe metodu kullanılmıştır. Varyansların homojen olmadığı durumlarda ise gruplardaki gözlem sayılarının eşit olması durumunu göz önünde bulundurmayan post-hoc istatistiklerinden Tamhane's T2 metodu kullanılmıştır. Grupların puan ortalamaları arasındaki farkın manidarlığı .05 düzeyinde yorumlanmış ve veriler analiz edilirken SPSS programından faydalanılmıştır. Araştırma sonuçlarına göre öğretmenlerin, kişisel siber güvenliği sağlama düzeylerini

belirlemeye yönelik ölçekten ortalamanın üstünde puan aldıkları sonucuna ulaşılmıştır. Yine ölçeğin "Kişisel Gizliliği Koruma, Güvenilmeyenden Kaçınma, Önlem Alma, Ödeme Bilgilerini Koruma ve İz Bırakmama" alt faktörlerinden de alınan puanların ortalamanın üstünde olduğu görülmüştür. Katılımcıların, cinsiyet, kıdem yılı, ile siber güvenliğin sağlanma düzeyi arasında anlamlı bir ilişkinin olmadığı sonucuna ulaşılmıştır. Öğretmenlerin kişisel siber güvenliği sağlama düzeylerinin yaşlarına göre anlamlı bir farklılık göstermediği sonucuna ulaşılsa da özellikle 36-40 yaş aralığındaki öğretmenlerin ölçeğin tamamı ve alt faktörlerinin çoğunda puanlarının daha yüksek olduğu bulunmuştur. Ölçeğin bazı alt faktörlerinde ise yaşlarına göre anlamlı farklılık ortaya çıkmıştır. 50 yaş üstü bireylerin puanlarının düşük olduğu ve 40 yaş altı tüm guruplarla farklılık gösterdiği belirlenmiştir. Öğretmenlerin branşlarına, bilgi ve iletişim teknolojilerine yönelik eğitim alma, siber güvenlik alanına yönelik eğitim alma ve kullanılan teknolojik cihazlara göre siber güvenliği sağlama düzeyleri arasında anlamlı bir farklılık görüldüğü sonucuna ulaşılmıştır. Öğretmenlerin, siber güvenlik düzeyinin artırılmasına yönelik verdikleri cevapların ise yedi ayrı görüşte birleştiği ve kişisel bilgi gizliliğinin güvence altına alınması için konu ile ilgili yasal yaptırımların artırılması, kişisel bilgi iletişim teknoloji araçlarının daha güvenli hale getirilmesi, üniversiteler ve halk eğitim kurslarında eğitimlerin verilmesi önerilerinin en çok olduğu belirlenmiştir. Bu sonuçlar ışığında, siber güvenlik farkındalığının artırılmasına yönelik başta öğretmenler olmak üzere okuldaki tüm paydaşlara eğitim verilmesi ve üniversitelerdeki eğitim fakültelerinin öğretim programlarına siber güvenlik farkındalığının oluşmasına katkı sağlayacak derslerin yerleştirilmesi, yaş ile ilgili oluşan farklılığın sebebinin araştırılması önerilerinde bulunulmuştur.

Anahtar Sözcükler: Siber güvenlik, Siber tehditler, Bilgi ve iletişim teknolojileri

ABSTRACT

EVALUATION OF TEACHERS' PERSONAL CYBER SECURITY AWARENESS LEVELS ACCORDING TO DIFFERENT VARIABLES

ALTINER, Imren

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

Thesis Advisor: Prof. Dr. Hafize KESER

September, 2021, xiii + 100 Pages

The main purpose of this research is to evaluate the cyber security awareness levels of secondary school teachers in terms of different variables. For this purpose, information such as the demographic characteristics of teachers and their educational status on the subject were collected quantitatively, and their suggestions for increasing cyber security were collected qualitatively and mixed method was used in the research. During the data collection phase, the Personal Information Form was used for information such as demographic information such as age, gender, seniority year, and suggestions for increasing cyber security awareness. Data collection tools were applied to 455 teachers working in public secondary schools in the districts of Ankara city center (Altındağ, Çankaya, Etimesgut, Gölbaşı, Keçiören, Mamak, Pursaklar, Sincan, Yenimahalle). In the analysis of the data obtained, an independent sample t-test was used to examine frequency, percentage, and the significance of the difference between two unrelated samples, and in case of more than two, one-way analysis of variance (ANOVA). If the differences observed between the groups to be compared are statistically significant, the Scheffe method, which is a type of post-hoc test, was used to determine from which group or groups the difference occurred. In cases where the variances are not homogeneous, Tamhane's T2 method, which is one of the post-hoc statistics that does not take into account the equality of the number of observations in the groups, was used. The significance of the difference between the mean scores of the groups was interpreted at the .05 level and the SPSS program was used while analyzing the data.According to the results of the research, it was concluded that the teachers scored above the average from the scale to determine their level of providing personal cyber security. It was also seen

that the scores obtained from the sub-factors of the scale "Protection of Personal Privacy, Avoiding Untrusted, Taking Precautions, Protecting Payment Information and Leaving No Traces" were above the average. It was concluded that there was no significant relationship between the participants' gender, seniority, and the level of providing cyber security. Although it was concluded that the level of providing personal cyber security of the teachers did not show a significant difference according to their age, it was found that especially the teachers in the 36-40 age range had higher scores in the whole scale and in most of its sub-factors. In some sub-factors of the scale, there was a significant difference according to their age. It was determined that the scores of individuals over the age of 50 were low and differed with all groups under the age of 40. It has been concluded that there is a significant difference between the levels of teachers receiving training on information and communication technologies, getting training on cyber security, and providing cyber security according to the technological devices used. It was concluded that the answers given by the teachers to increase the level of cyber security are in seven different opinions and the suggestions are mostly to increase the legal sanctions on the subject to ensure the privacy of personal information, to make the personal information and communication technology tools more secure, and to provide trainings in universities and public education courses. In the light of these results, suggestions were made to provide training to all stakeholders in the school, especially teachers, in order to increase cyber security awareness and to place courses that will contribute to the formation of cyber security awareness in the curriculum of education faculties in universities and to investigate the reason for the difference in age.

Keywords: Cyber security, Cyber threats, Information and communication technologies

ÖN SÖZ

Bilgi ve iletişim teknolojileri ve internetin kullanımı yaygınlaştıkça içinde bulunduğumuz bilgi çağında bu teknolojileri güvenli kullanmanın önemi; siyasi, sosyal, ekonomik, sağlık ve eğitim gibi pek çok alanda oldukça artmaktadır. Bilgi ve iletişim teknolojileri ve internetin yaygınlaşması topluma sağladığı faydaların yanı sıra riskleri de beraberinde getirmektedir. Bu risklerin içinde en önemlilerinden biri de siber tehditlerdir. Bireysel anlamda siber güvenlik farkındalık düzeyinin artmasının, toplumda siber güvenliğin sağlanmasında en önemli faktörlerden biri olmaktadır. Bireysel farkındalığın oluşması için eğitim kurumlarının önemi yadsınamaz. Siber güvenlik farkındalık düzeyinin artırılmasında eğitim kurumlarında görev alan tüm öğretmenlerin yanı sıra Bilişim Teknolojileri ve Yazılım dersi ve Bilgisayar Bilimi dersi ile bu dersleri veren öğretmenlerin rolü büyüktür. Alan yazın incelendiğinde eğitim kurumlarında öğretmen olarak görev yapan bireylerin siber güvenlik farkındalığını ortaya koymaya ilişkin bir çalışmaya rastlanmamıştır.

Ortaokul kademesinde görev yapan öğretmenlerin siber güvenlik farkındalık düzeylerini farklı değişkenler açısından değerlendirmeyi amaçlayan bu araştırma beş bölümden oluşmaktadır. Birinci bölümde, araştırma kapsamındaki problem, amaç, önem, sınırlılıklar ve tanımlara ilişkin bilgilere yer verilmiştir. İkinci bölümde, bilgi çağı, Endüstri 4.0, bilgi ve iletişim teknolojileri ile internet, siber güvenlik, siber tehditler, Türkiye'de siber güvenlik, ilgili ulusal ve uluslararası araştırmalar, üçüncü bölümde araştırmanın modeli, çalışma grubu, verilerin toplanması, veri toplama araçları ve verilerin analizine ilişkin bilgiler bulunmaktadır. Dördüncü bölümde, öğretmenlerin kişisel siber güvenlik farkındalık durumlarına ilişkin bulgular ve yorumlar yer almaktadır. Beşinci bölümde araştırma kapsamında elde edilen sonuçlara ve sonuçlar göz önünde bulundurularak yapılan önerilere yer verilmiştir.

TEŞEKKÜR

Yüksek lisans eğitimim süreci boyunca bana her konuda destek veren, katkılarıyla çalışmalarımı yönlendirerek bu araştırmanın ortaya çıkmasında en büyük katkıyı sağlayan, lisans eğitimimde öğrencisi olabilme fırsatını yakaladığım ve bana her durumdaki davranışlarıyla örnek olan, her zaman öğrencisi olabilmekten büyük onur ve gurur duyduğum tez danışmanım Prof. Dr. Hafize Keser'e,

Bu süreçte değerli fikirlerine başvurduğum Doç. Dr. Levent ÇETİNKAYA' ya ve Prof.Dr. Yasemin GÜLBAHAR GÜVEN'e,

Araştırmam sırasında ölçek uygulaması yapmama izin veren tüm okul yöneticilerine ve ölçeği cevaplayan tüm öğretmenlere,

Verilerin elektronik ortama aktarılma sürecinde yardımlarını esirgemeyen kardeşim Hande Altıner'e

Bana inanan, güvenen, sevgi ve desteklerini her zaman hissettiğim aileme ve arkadaşlarıma sonsuz teşekkürler...

İÇİNDEKİLER

Sayfa

TABLOLAR DİZİNİ

Tablo **Sayfa**

KISALTMALAR/SİMGELER

BTK	Bilgi Teknolojileri Kurumu
BİT	Bilgi ve İletişim Teknolojileri
TÜİK	Türkiye İstatistik Kurumu
ITU	Uluslararası Telekomünikasyon Birliği
CISA	Siber Güvenlik ve Altyapı Güvenliği Ajansı
MEB	Milli Eğitim Bakanlığı
OECD	Ekonomik İşbirliği Kalkınma Örgütü
TCK	Türk Ceza Kanunu
TİB	Telekomünikasyon İletişim Başkanlığı
USOM	Ulusal Siber Olaylara Müdahale Merkezi
SOME	Siber Olaylara Müdahale Ekipleri
KMO	Kaiser Mayer Olkin
DFA	Doğrulayıcı Faktör Analizi
UNESCO	Birleşmiş Milletler Eğitim, Bilim ve Kültür Örgütü

BÖLÜM 1

GİRİŞ

Bu bölümde araştırmanın problemi, amacı, önemi, sınırlılıkları ile araştırmada kullanılmış olan terimlerin tanımları yer almaktadır.

Problem

İnsanlık tarihi boyunca, meydana gelen yenilikler ve değişimler sonucunda dünyada birçok farklı çağ yaşanmıştır. Bu çağlar sosyo-ekonomik açıdan bakıldığında; öncelikle ilkel toplum ardından tarım toplumu sonra da sanayi toplumu olarak süregelmiş, günümüze ise bilgi toplumuna geçiş yapılmıştır (Aktan ve Tunç, 1998). Teknolojide kaçınılmaz bir şekilde meydana gelen gelişmelerle birlikte, toplumlar birçok farklı sürecin içinde bulunmaktadırlar. Bu süreçler de genellikle dönemin en çok önem verdiği terimlerle anılmaktadırlar.

Sanayi toplumunun devamı niteliğinde ortaya çıkan bilgi toplumu, "bilgi ekonomisi", "sanayi-sonrası toplum", "bilişim toplumu", "bilgi çağı" ve buna benzer biçimlerde ifade edilmekte; yeni çıkan teknolojilerin gelişimiyle "bilgi üretiminin", "bilgi sermayesinin" ve "nitelikli insan faktörünün" önem kazandığı, yaşam boyu öğrenmenin öneminin arttığı, "iletişim teknolojileri", "bilgi otoyolları", "elektronik ticaret" ve buna benzer farklılıklarla toplumu "ekonomik", "sosyal", "kültürel" ve "siyasal" açıdan sanayi toplumunun ilerisine götüren gelişme aşaması şeklinde ifade edilebilmektedir (Aktan ve Tunç, 1998).

Tarım ve sanayi toplumlarında, insan gücü ve makine kaynağı güçlü toplumu temsil ederken, bilgi toplumlarında bilginin ve aklın gücünden yararlanmak güçlü toplumu temsil etmektedir (Tonta, 1999). Bilgi ve iletişim teknolojilerinin birlikte kullanılması ile yapılabilen üretimin, insan gücüyle ve makine kaynaklarıyla yapılabilen üretimin çok ötesinde olduğu söylenebilmektedir. Üretimde "nükleer enerji", "elektrik enerjisinin" yerini almış ve sermaye "bilgi" olmuş, iletişim teknolojilerinde yaşanan gelişmelerle, "ulaşım-erişim" çok daha kolay hale gelmiştir. Fazla nüfus ve gereksinimleri karşılayabilmek üzere, birçok alanda, bilgi ve iletişim teknolojilerinin

kullanılabilir olması önemli hale gelmiştir (Karasar, 2004). Böylece bilgi teknolojilerinde ortaya çıkan yenilikler ve gelişmeler yeni bir çağın kapılarını aralamış, bununla birlikte farklı bir toplum tarzının kuruluşuna kaynak olduğu fikri ortaya çıkmaktadır. Sonuç olarak bilgi ve iletişim teknolojilerindeki yaşanan değişim ve gelişmelerle başlayan çağ, "bilgi çağı"; değişen ve farklılaşan toplum ise, "bilgi toplumu" şeklinde isimlendirilmektedir (Yeşilorman ve Koç, 2014). Bilgi toplumunun en önemli göstergelerinden biri; bilginin üretilmesi ve işlenmesinde faydalanılan bilgi ve iletişim teknolojileridir (Tonta ve Küçük, 2005).

Galbraith'e (1967) göre teknoloji, bilimsel veya sistematik olan bilgilerin pratik alanlarda düzenli ve yöntemli bir biçimde uygulanması olarak tanımlamıştır (Akt. İşman, 2001). Alkan`a (1998) göre en genel ifadeyle teknoloji; "kazanılmış yeteneklerin işe koşulması ile birlikte doğaya hâkim olmak için gerekli işlevsel yapılar, yollar oluşturma" olarak tanımlanmaktadır.

Bilgi teknolojisi; "bilginin toplanması", "işlenmesi", "depolanması", "ağlar aracılığıyla bir yerden bir yere aktarılarak" bireylerin kullanımına sunulması, iletişim ve bilgisayarlı teknolojileri de kapsayan "tüm teknolojiler" olarak tanımlanabilir. İletişim teknolojisi mesajların bir yerden bir yere eskiden var olan yöntemlerden çok daha hızlı ulaştırılmasına imkan tanımakta, bilgisayar teknolojisi ise "hesaplama" ve "bilgi işleme" yeteneklerimizi çok daha yüksek düzeye ulaştırmaktadır. Bilgisayar ve iletişim teknolojilerinin bir araya gelmesiyle birlikte (bilgi teknolojisi) "insan yetenekleri ilk kez milyon kere milyon kat artmaktadır" (Tonta, 1999). Bir başka deyişle bilgi ve iletişim teknolojisi bilgiye erişilmesi ve bilgi üretilmesine imkan tanıyan bilgisayar ve iletişim teknolojilerinin beraber kullanılmasıyla meydana getirilmiş olan sistemler topluluğu olarak tanımlanabilir.

Bilgi çağı, var olan tüm bilgilerin (veri, görüntü, ses vb.) elektronik, optik veya manyetik ortamlar aracılığıyla depolanabilmesi, işlem görebilmesi ve bir yerden bir yere ulaştırılabilmesine fırsat sağlayan bilgi ve iletişim teknolojilerinin gelişimini ifade etmektedir (Ünver, Canbay ve Mirzaoğlu, 2009). Sürekli olarak büyük bir hızla gelişen, farklılaşan ve çoğalan bilgi ve iletişim teknolojileri, bilgi toplumuna küresel dönüşümün temel öğeleridir (Ünver vd., 2009). Bilgi toplumu olmak için harekete geçmenin ve ilerleyebilmenin formülü; bilişim teknolojilerini üretmekten, geliştirmekten ve dolayısıyla sahip olmaktan aynı zamanda etkili, verimli ve doğru bir biçimde kullanmaktan geçmektedir (Yeşilorman ve Koç, 2014).

Tüm dünyada küreselleşme süreci oldukça hızlanmış ve teknolojinin hayata entegre olması ile birlikte bilgi toplumunun oluşumu sağlanmıştır (H. Erkan ve C. Erkan, 2007; Akt. Bulut ve Akçacı, 2017). Bilgi toplumu günümüzde her an kendi vazifesini gerçekleştirerek, yapılanma aşamasını tamamlayan "son yeni sanayi devrimi", "4.Sanayi devrimi" ya da "Endüstri 4.0" olarak ortaya çıkmaktadır. Bu yeni sanayi devriminde; "Nesnelerin İnterneti", "Her Şeyin İnterneti" veya "Endüstriyel İnternet" kavramları toplumda önemli yer tutacaktır (Bulut ve Akçacı, 2017).

Farklı açılardan ele alınarak tartışılmaya başlanan Endüstri 4.0, sadece üretim sistemleri boyutuyla değil, tüm dünyada ekonomik, sosyal ve siyasal alanları kökten değiştirecek yenilikleri beraberinde getiriyor gibi algılanmaktadır (Soylu, 2018). Endüstri 4.0 fiziksel ve sanal unsurların birlikte kullanıldığı bir iş ve yaşam biçimini tarif eden bir değişim ve dönüşüm sürecidir (Bulu ve Keser, 2019). Endüstri 4.0, insan gücünün yerini makinelerin aldığı ve böylelikle üretim süreçlerinin de kendiliğinden yönetebilir hale ulaşması olarak tanımlanabilir. Bilgisayarlar ve internet teknolojilerinde ortaya çıkan bu yeni gelişmeler sayesinde, makinelerin düzen içerisinde çalışabilmesi yeni sanayi devrimini doğurmuştur (Ege Bölgesi Sanayi Odası, 2015).

21. yy başlarında bilişim ve iletişim teknolojileri alanında yaşanan kritik değişimler internetin daha yaygın kullanılmasını, bilgisayar programlarındaki gelişmeler ise akıllı sistemlerin ilerlemesini sağlamıştır. Bu yenilikler ve gelişmelerle dijital sistemler fiziksel alan ile bağlantı halinde olarak, insan faktörünü ortadan kaldırmak suretiyle üretimde bir çığır açmış, bu da 4. Sanayi Devrimi ya da daha yaygın adıyla Endüstri 4.0 olarak geçmeye başlamıştır (Soylu, 2018).

Teknolojilerdeki bu hızlı gelişmeler iş gücünün eğitim ihtiyaçlarını büyük ölçüde etkilemektedir. Endüstri 4.0 döneminde sadece döneme ayak uydurabilen, kendini geliştirmiş nitelikli çalışanlar dijital araçlar ve robotlarla birlikte çalışabileceklerdir. Günümüzde hızlı bir dönüşüm gerçekleşmektedir ve insanların makineleri kullandığı dönemden insanların makinelerle birlikte çalıştığı bir döneme geçilmektedir (Bulu ve Keser, 2019).

Bilgi teknolojisi kavramını niteleyen ve bu kavram geçtiğinde ilk düşünülen modern teknolojinin ürünü "bilgisayarlar", bilginin tedvir edilmesi sürecinde bilgi ve iletişim teknolojilerinin öneminin artması denince ise akla "internet teknolojisinin gelişmesi" gelmektedir. İnternet kullanan kişi sayısının ve internet yolu ile kazanılan katma değerin ("bilgi, ticaret, pazarlama, tanıtım, telekomünikasyon trafiği") yükselmesi,

çoğu ülkenin son zamanlarda bilgi ve iletişim teknolojilerindeki ilk amaçlarından biri haline gelmiştir (Yeşilorman ve Koç, 2014).

Türkiye'de ve dünyada bilgisayar ve internet kullananların sayısının gün geçtikçe arttığı görülmektedir. Türkiye İstatistik Kurumu'nun 2014 yılında yayınladığı raporda 16-74 yaş grubundaki bireylerin bilgisayar kullanım oranı %53,5 iken 2020 yılında en son yayınlanan rapora göre, 2018 yılında bu oran %59,6'dır. Yine Türkiye İstatistik Kurumu'nun 2015 yılında yayınladığı raporda 16-74 yaş grubundaki bireylerin internet kullanım oranı %55,9 iken, bu oran 2020 yılında en son yayınlanan rapora göre %79,0'dır (TÜİK, 2020). Yaklaşık son 5 yılda bilgisayar kullanım oranında %6,1'lik bir artış, internet kullanım oranında ise %19,4'lük bir artış olmuştur.

Bilgi ve iletişim teknolojilerinin 1990 sonrası bu hızla gelişimi, 2000'li yıllarla birlikte kullanımının tüm dünyada yaygınlaşması, bununla birlikte hem kamu hem de özel sektörün hizmetlerini dijital ortama da taşımaları, insanların bilgi ve iletişim teknolojilerine bağımsız olarak yaşamlarını sürdürmelerini imkansız hale getirmiştir (Demiraslan ve Elaldı, 2017). Bilgi ve iletişim teknolojilerinin kullanımındaki bu artış tüm dünyada sosyal, politik, ekonomik ve askeri güvenliği riske atmış, suçlulara ve teröristlere siber alanda yasadışı ve zararlı amaçlarına ulaşmalarını sağlayan bazı güvenlik açıklarını da beraberinde getirmiştir (Beydoğan ve Canbay, 2008).

Toplum adına çok fazla fayda sağlayan yenilik ve gelişmelerin, bazı kesimler ve taraflarca kötüye kullanılması, siber alanın saldırılara uğrayarak tehdit edilmesi, kişilere ve kurumlara maddi manevi zararlar verilmesi, bireylerin ve toplumların siber saldırı yolu ile mağduriyetlerinin giderek artması güvenlik anlayışını kökünden değiştirmiştir (Demiraslan ve Elaldı, 2017). Bunun gibi yaşanan olumsuz gelişmeler siber güvenlik, kritik bilgi ve altyapı koruma ile ilgili konuları gündeme getirmiş; uluslararası örgütleri, hükümetleri, özel sektörü ve sivil toplumu bu konuda önlemler almaya zorlamış ve siber güvenlik en önemli gündem maddelerinden biri haline gelmiştir (Beydoğan ve Canbay, 2008).

İnternet teknolojisi kullanımında güvenlik konusu, tasarımından sonraki dönemlerde peyda olan bir kavram olmuştur. İnternetin, "kullanım kolaylığı", "düşük maliyet" ve "evrensellik" ilkeleri temel alınarak internet tasarlanmış, kullanıcıların bu teknolojiye zarar vermek isteyecekleri akla gelmemiştir (Goodman, 2008). Günümüzde internet kullanımının artması ve teknolojinin çok hızlı biçimde gelişmesi, etkili korunma uygulamalarının geliştirilmesi ve hızlı müdahale hazırlığı kritik bir önem arz etmiştir. Saldırıların yapıldığı o anda "tespit edilmesi", "sanal ya da fiziksel koruma inşa

edilmesi", "ulusal ve bölgesel siber güvenlik politikalarının geliştirilmesi" siber güvenliğin oluşabilmesi için mecburi bir durum haline gelmiştir (Goodman, 2008).

Bu çağda internet teknolojilerinin kullanımı, yaşamımızın her alanında neredeyse bir zorunluluk olmuş ancak teknoloji, yaşamımıza getirdiği kolaylıkların yanı sıra olumsuz etkileri ve problemleri de beraberinde getirmiştir. İnternet teknolojisinin geliştirilmesindeki amaç "iletişimi arttırmak" ve "bilgi paylaşımını kolaylaştırmak" olmasına rağmen beklenenden çok hızlı bir şekilde yaygınlaşması nedeniyle toplumu olumsuz etkileyebilecek önemli problemleri de doğurmuştur (Çelik, Çelen ve Seferoğlu,2014).

Bulut ve Akçacı (2017), Endüstri 4.0'ın yeni teknoloji kavramları arasında siber güvenlik kavramına da yer vermişlerdir. Cihazların rutin halde internette etkin biçimde yer almalarının veri hasarına ve bilgi güvenliğinin tehdidine yol açabildiğini, siber güvenliğin veri güvenliğinin kontrol altında tutulmasını sağladığını, siber güvenlik sistemlerinin, şirketlerin fiziksel iletişimin güvenli bir ortamda yürütülebilmesine olanak tanıdığını ifade etmişlerdir.

Benzer şekilde Soylu (2018), Endüstri 4.0 ile ilişkili kavramlar arasında siber güvenliğe yer vermiştir. Endüstri 4.0 ile birlikte dikey ve yatay entegrasyonun önemli bir boyutta artmasıyla birlikte, "kritik endüstriyel sistemleri" ve "üretim hatlarını" siber güvenlik risklerine karşı korumak için, cihazların kimliklerinin tespiti ve cihazlara ulaşımın kontrolü güvenli iletişim için önem kazanmaktadır (Rübmann vd., 2015). Başka bir deyişle siber güvenlik içinde bulunduğumuz ve ilerleyen teknolojilerle toplumun içinde bulanacağı öngörülen dönemlerde önemini git gide artırmaktadır.

Siber güvenlik birçok farklı şekillerde ifade edilse de, uluslararası alanda kabul görmüş tanımı; siber ortamda kurumların ve kullanıcıların yapılarını güvence altına almak için; "kullanılabilecek araçlar, politikalar, güvenlik kavramları, güvenlik önlemleri, yönergeler, risk yönetimi yaklaşımları, eylemler, eğitim, en iyi uygulamalar," teminat ve teknolojilerin toplamıdır (ITU, 2008a). Siber güvenliğin genel güvenlik hedefleri bilginin:

- Kullanılabilirlik
- Özgünlük ve bütünlük
- Gizlilik

özelliklerini korumayı içermektedir (ITU, 2008a).

Uluslararası terimler sözlüğünde ise siber güvenlik; elektronik bilgi ve iletişim sistemlerinin hasar görmesini, yetkisiz kullanımını, sömürülmesini ve gerekirse

elektronik bilgi ve iletişim sistemlerinin restorasyonunu ve içerdikleri bilgileri önleyerek bu sistemlerin gizliliğini, bütünlüğünü ve kullanılabilirliğini güçlendirmek, başka bir deyişle saldırıları önleyerek, tespit ederek ve bunlara yanıt vererek bilgiyi koruma süreci şeklinde tanımlanmaktadır (Computer Security Resource Center, 2021).

Schatz, Bashroush ve Wall'a (2017) göre siber güvenlik, siber alanda kullanılan verilerin ve varlıkların gizliliğini, bütünlüğünü ve kullanılabilirliğini korumak için kurum, kuruluş ve hükümetlerce izlenen güvenlik risk yönetiminin ilerlemesiyle ilgili yaklaşım ve aksiyonlardır. Bu yaklaşım; siber çevreye ve kullanıcılarına en iyi korumayı sağlamak için kuralları, politikaları, güvenlik önlemlerini, teknolojileri, araçları ve eğitim koleksiyonlarını içerir.

Kaşıkcı, Çağıltay ve Karakuş (2014), "Avrupa Çevrimiçi Çocuklar" projesine katılan Türkiye'nin yanında ve 23 Avrupa ülkesinin bulgularını değerlendirerek, çocukların ve ailelerinin internet kullanımlarını, çocukların internet ortamındaki hareketlerini, karşılaştıkları riskleri inceledikleri çalışmalarında; ülkemizdeki çocukların yaşamlarında internetin önemli bir yerinin olduğunu tespit etmişlerdir. Araştırma sonuçları, çocukların "internet kullanımı konusunda kendilerine güvendiklerini" ancak "internet becerileri konusunda yeterli olmadıklarını" göstermiştir. Ebeveynlerin ise "üçte ikisi bilişim okur-yazarı" olmadığı için, evlatlarına internetin verebileceği zararlar konusunda destek sağlayamadığı görülmüştür. Bu sonuçlara dayanılarak ebeveynlerin ve çocukların "okul, internet servis sağlayıcıları, bilişim firmaları ve sivil toplum kuruluşlarınca" desteklenmesi ve haberdar edilmesi gerekliliğini vurgulamışlardır (Kaşıkcı vd., 2014). Bu nedenle okullarda hizmet veren öğretmenlere büyük görev ve sorumluluklar düşecektir. Bu sebeplerle öğretmen adaylarına, bilişim güvenliği ile ilgili bilinçlerini ve bilgilerini artıracak, almaları gereken güvenlik tedbirlerini sağlayacak bilişim güvenliği eğitimleri verilmesinin faydalı olacağı ve büyük bir ihtiyaca çözüm getireceği düşünülmektedir (Gökmen ve Akgün, 2016). Bilişim Etiği ve Güvenliği bilişim teknolojileri öğretmen adaylarına zorunlu ders olarak, birçok üniversitede ise tüm öğrencilere seçmeli ders olarak verilmesi bu kapsamda değerlendirebilecek olumlu gelişmelerdir.

Siber güvenlik konusunun büyük oranda teknik olarak değerlendirilmesi ve teknik çözümler getirilmeye çalışılması; "yasal", "idari", "ekonomik ve sosyal" anlamda siber güvenliğin değerlendirilmesinin önüne geçmektedir. Sosyal olarak, interneti kullanan bireylerin birbirinden çeşitli "bilinç ve güvenlik farkındalığı düzeylerine" sahip oldukları görülmektedir. Bu duruma örnek olarak, bireyler siber tehlikeleri fark etmeden kişisel

bilgilerini güvenli olmayan internet sitelerine girebilmekte hatta alışveriş dahi yapabilmektedirler. Buna benzer olayların sıklıkla yaşanması, Türkiye'de siber güvenlik konusunda farkındalığın arttırılmasına yönelik toplumun tüm kesimlerinde bilinçlendirme çalışmalarına ihtiyaç duyulmaktadır. Farkındalığın arttırılması konusunda en önemli roller kamu kurum ile kuruluşlarına, özel sektör kuruluşlarına ve sivil toplum kuruluşlarına düşmektedir. Bir örnek olarak, Milli Eğitim Bakanlığı öğretim programlarına siber ortamda güvenliğin sağlanmasına yönelik farkındalık bilinç gelişmesine katkı sağlayacak dersler eklenebilir (Ünver vd., 2009).

Milli Eğitim Bakanlığı'nın Ortaokul 5 ve 6. sınıflar için Bilişim Teknolojileri ve Yazılım Dersi Öğretim Programı (2018) incelendiğinde; "Etik ve Güvenlik" başlıklı bir ünite yer almaktadır. Ünite konuları; "Etik Değerler", "Dijital Vatandaşlık", "Gizlilik ve Güvenlik" olmak üzere üç başlık altında toplanmıştır. 5.sınıf için

- Gizlilik ve Güvenlik konu kazanımları;
    - BT.5.2.3.1. Gizlilik açısından önemli olan bileşenleri belirler (Şifre güvenliği, kişisel bilgilerin güvenliği, mahremiyet gibi kavramlar üzerinde durulur),
    - BT.5.2.3.2. Gizli kalması gereken bilgi ile paylaşılabilecek bilgiyi ayırt eder (Öğrenciler paylaştıkları bilgilerin niteliği konusunda sorumlu davranmaya teşvik edilir)

şeklinde sıralanmıştır (MEB, 2018).

6.sınıf için ise yine ünite konuları; Etik Değerler, Dijital Vatandaşlık, Gizlilik ve Güvenlik olmak üzere üç başlık altında toplanmıştır,

- BT.6.2.1. Etik Değerler başlığı altında konu kazanımları;
    - BT.6.2.1.6. Bilişim suçlarının neler olduğunu açıklayarak ilgili kanunları özetler,
    - BT.6.2.1.7. Bilişim suçlarına karşı alınabilecek önlemler ve stratejiler geliştirir**, (**İnternet Bilgi İhbar Merkezi hakkında bilgi verilir)

şeklinde sıralanmıştır.

- BT.6.2.3. Gizlilik ve Güvenlik başlığı altında;
- BT.6.2.3.1. Bilişim teknolojilerinin kullanımında gizlilik ve güvenlik boyutlarının önemini tartışır (Gizlilik, bütünlük, erişilebilirlik gibi kavramlara değinilir),
- BT.6.2.3.2. Güvenlik açıklarının oluşumu konusunda yorum yapar,
- BT.6.2.3.3. Bilgi koruma yöntemlerini ifade eder,

- BT.6.2.3.4. Bilgi paylaşımı sürecinde olası riskleri değerlendirerek alınabilecek önlemleri tartışır,
- BT.6.2.3.5. Zararlı yazılımları kavrar (Virüs, spam, truva atı vb. zararlı yazılımlardan bahsedilir),
- BT.6.2.3.6. Güvenlik yazılımlarının kullanım amaçlarını açıklar

şeklinde sıralanmıştır (MEB, 2018).

Ünver ve diğerleri (2009) siber güvenliğin sağlanması ve kritik altyapıların korunması ile ilgili yaptıkları çalışmada, yaşanan teknolojik değişimler beraberinde "siber saldırı araçları ve yöntemleri" geliştirdiği için kullanıcılara "siber tehditler, riskler, saldırılar ve güvenlik önlemleri" konularında bilinçlendirme ve farkındalık çalışmalarının yapılması gerektiği ve teknolojilerin doğru biçimde kullanılmasına ilişkin bu çalışmaların da eğitim kurumlarınca gerçekleştirilmesi gerektiği önerisinde bulunmuşlardır.

Yılmaz, Şahin ve Akbulut (2016), Milli Eğitim Bakanlığı'na bağlı kurumlarda çalışan öğretmenlerin "dijital veri güvenliği farkındalıklarını" irdeledikleri çalışmalarında, katılımcıların "dijital veri güvenliği farkındalıklarının" oldukça yüksek olarak belirlemişlerdir. Öğretmenlerin "dijital veri güvenliği farkındalıklarının" branş, öğretmenlerin görev aldığı öğrenim kademesi, meslekteki görev yılları ve öğrenim durumuna göre farklılaşmadığını, fakat; cinsiyet, bir günde bilgisayarda geçirdikleri süre, bir günde internette geçirdikleri süre ve teknolojik aletlere sahip olma durumlarına göre dijital veri güvenliği farkındalığına olumlu bir etkisi olduğu sonucuna ulaşılmıştır (Yılmaz vd., 2016).

Gökmen ve Akgün (2016) tarafından, öğretmen adayları tarafından tecrübe edilen bilişim suçu olaylarının, "bilişim güvenliğini" konusunda öğrenmek istedikleri temaların tespit edilmesi için bir çalışma gerçekleştirilmiştir. Çalışmada, öğretmen adaylarından bir kısmının "bilişim suçlarına maruz kaldıkları", bir kısmının "bilişim suçunu bilerek veya bilmeyerek işledikleri", diğer bir kısmının ise "bilişim suçunun ne olduğu konusunda herhangi bir fikirlerinin olmadığı" ve "bilişim suçlarına maruz kaldıklarında bu durumu gerekli mercilere iletme konusunda bilgi sahibi olmadıkları" bulgularına ulaşılmıştır. Bunun yanı sıra katılımcıların bilişim güvenliğinin ne ifade ettiği ve neyi kapsadığı ile ilgili bilgilerinin eksik olduğu görülerek, "bilişim güvenliği" hakkında eğitim alma gereksinimleri olduğu sonucuna ulaşılmıştır (Gökmen ve Akgün, 2016).

Öğretmen yetiştirme lisans programlarının 25'i, 2018 yılında Yükseköğretim Kurulu Başkanlığında düzenlenen toplantı ile güncellenmiştir. Bu bağlamda Bilgisayar ve Öğretim Teknolojileri Öğretmenliği Lisans Programına, 4.yarıyılda Bilişim Etiği ve

Güvenliği dersi eklenmiştir. Programda ders içeriği; "Etik kavramı; bilgisayar güvenliğinin tarihsel gelişimi; etik-meslek ilişkisi ve profesyonel etik; etik ilkelerin doğası; dijital vatandaşlık ve bilgi toplumu bireyinin etik sorumlulukları; bilişim kaynaklarının kullanımında etik sorunlar; bilginin doğruluğu; bilgiye erişim; mahremiyet; veri koruma; fikrî mülkiyet, telifler, patentler ve lisans anlaşmaları; bilişim hukuku; bilişim suçları; bilişim suçlarının toplumsal etkileri; siber uzay ve siber güvenlik ile ilgili temel kavramlar; siber aktörler ve saldırı yöntemleri; siber savunma yöntemleri; mobil ve sosyal medya ortamlarında güvenlik; ağ güvenliği; kişisel ve kurumsal veri güvenliği yönetimi; bilişim mevzuatı ve hukuku" şeklinde oluşturulmuştur (https://www.memurlar.net/haber/749268/25-ogretmenlik-lisans-programi-guncellendi.html). Bilindiği gibi Bilgisayar ve Öğretim Teknolojileri Öğretmenliği Lisans Programını tamamlayan mezunlar ağırlıklı olarak ortaokullarda Bilişim Teknolojileri ve Yazılım dersi, liselerde ise Bilgisayar Bilimi dersi öğretmeni olarak atanmaktadırlar.

İçinde bulunduğumuz dönemde bilgi ve iletişim teknolojileri ve interneti güvenli kullanmanın önemi oldukça artmaktadır. Bireysel anlamda siber güvenlik farkındalık düzeyinin artmasının, toplumda siber güvenliğin sağlanmasında en önemli faktörlerden biri haline geldiği görülmektedir. Bireysel farkındalığın oluşması için eğitim kurumlarının önemi yadsınamaz. Siber güvenlik farkındalık düzeyinin artırılmasında Bilişim Teknolojileri ve Yazılım dersi ve Bilgisayar Bilimi dersleri ile bu dersleri veren öğretmenlerin rolü büyüktür. Bu bağlamda, araştırmanın problem durumunu "Ortaokul öğretmenlerinin siber güvenlik farkındalık düzeyleri nedir?" sorusu oluşturmaktadır.

Amaç

Bu araştırmanın temel amacı ortaokul kademesinde görev yapan öğretmenlerin siber güvenlik farkındalık düzeylerini farklı değişkenler açısından değerlendirmektir.

Bu genel amaca ulaşmak için aşağıdaki sorulara cevap aranmıştır:

1. Ortaokul kademesinde görev yapan öğretmenlerin siber güvenlik farkındalık düzeyleri nasıldır?
2. Ortaokul kademesinde görev yapan öğretmenlerin siber güvenlik farkındalık düzeyleri;
   a. Cinsiyet,

b. Yaş,
c. Görev yılı,
d. Branşı,
e. Bilişim teknolojileri konusunda eğitim alma (ders ya da kurs) durumu,
f. Siber güvenlik konusunda eğitim alma (ders ya da kurs) durumu,
g. Sahip olduğu bilgi ve iletişim teknolojileri,

3. Ortaokul kademesinde görev yapan öğretmenlerin siber güvenlik farkındalık düzeylerinin artırılmasına yönelik önerileri nelerdir?

Önem

Siber güvenlik konusu ile ilgili gerçekleştirilen araştırmalar ve çalışmalar incelendiğinde, çok büyük bir kısmının bu konuyu teknik açıdan ele aldığı, sistem ve ağ yöneticilerine dönük olduğu görülmektedir. Bu konuyu kullanıcılara yönelik veya farkındalık ve bilinç kazandırmak üzere eğitim temeline dayandırarak yapan çalışma sayısının oldukça az olduğu söylenebilir. Bu doğrultuda siber güvenlik konusunun bu açılarıyla incelendiği araştırmalara duyulan ihtiyaç artmaktadır (Öğün ve Kaya, 2013).

Alp (2018) akıllı şehirlerle ilgili yaptığı siber güvenlik çalışmasında, akıllı şehirlerde siber güvenlik yol haritası önerisinde bulunmuştur**.** Akıllı şehirde yaşayan tüm bireylerin güvenlik farkındalık seviyesinin artmasını sağlayacak eğitimler, afişler ve konferanslar düzenlenmeli, ilkokul veya ortaokul kademelerinden itibaren siber, siber alan, siber tehdit, siber güvenlik ve siber farkındalık gibi kavramlar hakkında bilinç kazandırılmalıdır önerilerinde bulunmuştur. Ayrıca, uğranabilecek siber saldırılara karşı tüm bireylerin farkındalık düzeylerinin artırılması, bu konuda çalışacak insan gücünü yetiştirmek üzere üniversitelerde "siber güvenlik programları" açılması ve ilgili bireylere gerekli yönlendirmelerin yapılması önerilmektedir.

Siber güvenlik ile ilgili yapılan çalışmalara bakıldığında farkındalık ile ilgili boyuta dikkat çekildiği görülmektedir. Bu doğrultuda yapılacak olan bu çalışma öğretmenlerin siber güvenlik farkındalık düzeylerinin belirleyeceği için literatürdeki bu eksikliğe bir cevap niteliğinde olacaktır. Yine siber güvenlik ile ilgili literatürdeki çalışmalara bakıldığında, çalışma grubu olarak kamu kurumlarında görev yapan öğretmenlerin seçildiği bir çalışmaya rastlanmamıştır. Bu yönüyle yapılacak olan bu çalışmanın kamu kurumlarında siber güvenlik farkındalık seviyesinin artması ile ilgili fayda sağlayacağı düşünülmektedir.

Elde edilen bulgular öğretmen yetiştirme programlarında öğretmen adaylarının siber güvenlik farkındalık düzeyini artırmaya yönelik kazanım ve etkinliklerin belirlenmesine ışık tutabilir.

Sınırlılıklar

Araştırma, veri toplama aracı olarak Kişisel Siber Güvenliği Sağlama Ölçeği ile ortaokul kademesinde görev yapan öğretmenlerin siber güvenlik farkındalık düzeylerinin değerlendirilmesi ile Ankara il merkezinde örnekleme dahil edilen ilçelerde görev yapan ortaokul öğretmenleri ile sınırlıdır.

Tanımlar

Bilgi Toplumu: Bilgi ve iletişim teknolojilerinin gelişimiyle; bilgi birikiminin sermayeye dönüştüğü ve "nitelikli insan" faktörünün önem kazandığı, yaşam boyu öğrenmenin öneminin arttığı, "iletişim teknolojileri", "bilgi otoyolları", "elektronik ticaret" ve buna benzer farklılıklarla beraber toplumu "ekonomik", "sosyal", "kültürel" ve "siyasal" açıdan sanayi toplumunun ilerisine götüren bir gelişme aşaması (Aktan ve Tunç, 1998; Ünver vd., 2009).

Bilgi ve İletişim Teknolojileri: Bilgiye erişilmesi ve bilgi üretilmesine olanak sağlayan, bilgisayar ve iletişim teknolojilerinin birlikte kullanılarak meydana çıkan sistemler topluluğu.

Endüstri 4.0: Fiziksel ve sanal unsurların birlikte kullanıldığı bir iş ve yaşam biçimini tarif eden bir değişim ve dönüşüm süreci olarak; insan gücünün yerini makinelerin aldığı, makinelerin düzen içinde çalışması ve böylelikle üretim süreçlerinin de kendiliğinden yönetebilir duruma gelmesi (Bulu ve Keser, 2019; Ege Bölgesi Sanayi Odası, 2015).

Siber Güvenlik: Siber ortamda kurumların ve kullanıcıların varlıklarını korumak için kullanılabilecek araçlar, politikalar, güvenlik kavramları, güvenlik önlemleri, yönergeler, risk yönetimi yaklaşımları, eylemler, eğitim, en iyi uygulamalar, güvence ve teknolojilerin toplamı. Saldırıları önleyerek, tespit ederek ve bunlara yanıt vererek bilgiyi koruma sürecidir (ITU, 2008a; Computer Security Resource Center, 2021).

BÖLÜM 2

KAVRAMSAL ÇERÇEVE VE İLGİLİ ARAŞTIRMALAR

Bu bölümde bilgi ve iletişim teknolojilerinin gelişimi ile ortaya çıkan bilgi çağı ve Endüstri 4.0 ortaya konularak, çağın gereği siber güvenlik ve siber güvenlik farkındalığına yönelik kavramsal bilgiler ve ilgili araştırmalar yer almaktadır.

2.1 Kavramsal Çerçeve

Bu bölümde araştırmanın kavramsal çerçevesini oluşturan, içinde bulunduğumuz bilgi çağına ve toplumsal etkilerine, Endüstri 4.0 ve getirdiği yeni sistemlere, bilgi ve iletişim teknolojilerinin gelişimine, siber güvenlik tanımlarına ve siber güvenlik ile ilgili kavramlara, siber tehditler ve yöntemlerine, ülkemizde siber güvenlik ile ilgili yapılan gelişmelere, yasal düzenlemelere, kurum ve kuruluşlara, siber güvenlikle ilgili araştırmalara yer verilmiştir.

Bilgi Çağı

İnsanlık tarihi boyunca tarım toplumu, endüstri toplumu ve ardından bilgi toplumuna doğru üç aşamalı bir geçiş yaşamıştır (Yüksel, 2014). Endüstri devrimi, üretim şekliyle, sosyo-ekonomik yapılaşmasıyla birlikte kendi kültürünü oluşturmuş ve sürecini tamamlayarak yeni bir döneminin kapılarını aralamıştır (Bölükoğlu, 2002). Tüm Dünyada 1970'lerden itibaren bilgi iletişim teknolojilerinde yaşanan çarpıcı gelişmeler bu yeni dönemin "Bilgi Çağı" olarak isimlendirilmesini sağlamıştır (Bölükoğlu, 2002).

Dönem, aynı zamanda "kapitalist-ötesi toplum", (Drucker,1993.) "bilişim toplumu", "bilgi çağı" "bilgi ekonomisi" gibi tabirlerle de nitelendirilmektedir (Aktan ve Vural, 2016). Bunların içinde en çok tercih edilen, tüm toplumlarda kabul gören kavram "bilgi çağı", aynı anlamı ifade eden "bilgi toplumu" olmaktadır (Yılmaz, 1998). Bilgi çağı, yeni değişim sürecinin gittiği yolu ve niteliğini ifade eden bilgi toplumu kavramını beraberinde getirmiştir (Ünal, 2009). 21.yy'ın ise bilgi çağı, bilgi toplumu olarak

nitelendirilmesi gerektiği konusunda bilim insanları ve neredeyse bütün toplumlar hem fikir olmuştur (İşman, 2011).

20.yy'ın ikinci yarısından sonra bilgi ve iletişim teknolojilerinin gelişme hızıyla birlikte, endüstri çağı sona ererek, yeni bir dönem olan bilgi çağının ortaya çıkmıştır. Bu yeni dönemde bilgi ve teknoloji kavramlarının önemini artırması sebebiyle bu kavramlarla örtüşen nitelikte isimlerle anılmış, aralarında bilgi çağı ve bu çağın özelliklerini anlatmak için de bilgi toplumu ifadeleri tüm çevrelerce kabul görmüştür.

Bilgi çağı, bilginin birincil kaynak haline geldiği, bilgi üretimi ve iletiminin yaygınlaştığı, bilgisiyle çalışanların daha fazla olduğu, yeni bilgi araştırma ve öğrenmenin çok mühim bir hal aldığı toplumsal ekonomik döneme karşılık gelmektedir (Bedük ve Balcılar, 2009). Bilgi toplumu, bilginin insan yaşamı için önemini artırdığı, bilgi için çalışan kişi sayısının fazlalaştığı, yaşam boyu öğrenme farkındalığının oluşmaya başladığı, öğrenen birey, örenen organizasyon ve öğrenen toplum arasındaki bağın kurulduğu bir dönemi ifade etmektedir (Bölükoğlu, 2002). Aynı zamanda dinamikliğini insan zihninden alan, sermayesi insani gelişmişlik olan elektronik bir çağdır (Meder, 2001). Yani bilgi çağı; bilginin en önemli sermaye haline geldiği, bilgiye ulaşma yollarının yeni teknolojiler ile sınırsızlaştığı toplumsal bir dönem, bilgi toplumu ise; insanların bilgisini artırmaya çalıştıkları, her topluluk ve her yapılanma için bilgi düzeyini yukarılara taşımanın çok mühim hale geldiği bir dönem olarak ifade edilebilir. Bu çağda bilgi teknolojileri her geçen gün gelişmekte, bu gelişmeler dünyayı bilginin önemini git gide arttırdığı bir yer haline dönüştürmektedir (İşman, 2011).

Bilgi toplumu kavramına hem kuramsal hem de ifade etmeye çalıştığı gerçeklik açısından bakıldığında ana ögenin "bilgi" olduğu anlaşılmaktadır (Yılmaz, 1998). Bilgi sözcüğü ana hatlarıyla, gözlem, deney, araştırma ve düşünme ile ulaşılan gerçek, zekâ ve akıl yürütme sonucu ortaya çıkan zihin ürünü şeklinde ifade edilmektedir (Ünal, 2009). Türk Dil Kurumu Sözlükleri' ne göre ise öğrenme, araştırma veya gözlem yolu elde edilen gerçek, olarak tanımlanmaktadır (Türk Dil Kurumu, 2019). Bilgi, bilgi ve iletişim teknolojilerinin gelişmesi ile birlikte sınırsız bir kaynak olarak görülmektedir (Barutçugil, 2002; Öğüt, 2003).

Bilgi çağında bilgi, bir yerden bir yere aktarılan, değişen, gelişen ve bilgi iletişim teknolojileri ile işlenen bir sermayeye dönüşmüştür (Yüksel 2014; Erkan, 1998). Bilginin bu denli önem kazanması insanları bilgiyi öğrenmeye, araştırmaya, sorgulamaya, eleştirmeye ve doğru bilgiyi bulmaya itmiştir. Bu durum bilgiyi fazlaca kullanan insanlardan oluşan bilgi toplumu olarak karşımıza çıkmaktadır (Yüksel, 2014). Biraz

daha somut bir açıdan bakıldığında, "bilgi, bu toplumda/çağda çok önemlidir" önermesine ulaşmak olası görünmektedir (Yılmaz, 1998).

Erkan'a (1993) göre, bilişim teknolojilerinin yapı taşı olan bilgisayar aracılığı ile bilgi toplumuna geçiş gerçekleşmiştir. Yüksel (2014) ise benzer şekilde bilgisayarın keşfinin ve kullanım yaygınlığının, bu yeni dönemin en belirgin özelliği olduğunu ifade etmiştir. Beraberinde birçok materyal geliştirilmiş, teknoloji hızla ilerlemiş ve bunun sonucu olarak insanlar bilmeye, bilgiyi araştırmaya ve öğrenmeye yönelmişlerdir (Yüksel, 2014).

Bilgi ve iletişim teknolojilerinin en önemli unsuru olan bilgisayarlar ve beraberinde gelişen teknolojileri toplumun her kesiminden insanın kullanması sayesinde, bilgiye ulaşma yolları çok çeşitlenmiş ve bilginin önemi fark edilerek bilgi çağına geçişin adımları atılmaya başlanmıştır.

20.yy'ın ikinci yarısından itibaren, merkezinde bilişim teknolojilerindeki gelişmelerin bulunduğu bilgi çağı; ürettiği araçlarla, ortaya koyduğu verilerin kullanımına bağlı olarak geliştirdiği dinamik toplum yapısıyla ve iletişim teknolojisindeki sonuçlarıyla, sürekli olarak kendini yenileyen bir ivme kazanmıştır (Bölükoğlu, 2002).

Bu dönemin önceki toplum türlerinden en önemli farkı bilgiyle güçlenen teknolojinin getirdiği yeni bir anlayış biçimine ayak uydurmaktır. Bilgi toplumu düzeyine erişebilmek dönemin en önemli hedeflerinden biri haline gelmiştir (Taşbaşı ve Altınbaşak, 2006). Ülkemizde ise 2003 yılında Türkiye'nin bilgi toplumu seviyesine erişebilmesi adına devlet planlama teşkilatı bünyesinde bilgi toplumu dairesi kurulmuştur (http://www.bilgitoplumu.gov.tr). Yani, teknolojinin gelişmesi ile artan bilgi düzeyi, yeni teknolojilerin de oluşmasına da yol açarak bir döngü oluşturmuştur.

Bilgi ve uzay teknolojileri gelişip toplumlarda yaygınlaşarak gündelik yaşamdaki makine kullanımının atmasına sebep olmuş, insanlar ile makineler arasındaki ilişkiyi farklı seviyeye taşıyarak bilgi toplumunda siber içeriğin önem kazandığı görülmüştür (Meder, 2001). Tüm dünyada ve ülkemizde de bilgi toplumuna geçiş sürecinde, ticari ve politik motivasyonlarla ortaya çıkan zararlı yazılımlar büyük artış göstermiş, ülkeler siber saldırıların hedefi haline gelmiştir (Yılmaz, Ulus ve Gönen, 2015).

Bilgi toplumlarında gelişen yeni teknolojiler sadece insanların değil aynı zamanda makinelerin iletişimini de farklı bir boyuta taşımıştır. Bu iletişimin ise sağladığı faydaların yanı sıra siber güvenlik gibi riskleri de beraberinde getirdiği söylenebilmektedir.

Endüstri 4.0

İçinde bulunduğumuz dönem; üretimde mekanik teknolojilerin yerlerini programlanabilir dijital teknolojiye bırakmasıyla ortaya çıkan üçüncü endüstriyel devrim olarak nitelenmekte ve dünyada bilgi iletişim teknolojilerinin büyük bir hızla gelişmesi ile kullanımının yaygınlaştığı "informatik" devir olarak da kabul edilebilmektedir (Çeliktaş, Sonlu, Özgel ve Atalay, 2015). Bilgi çağı, bilgi toplumu veya bilgi teknolojisi olarak adlandırılan bu dönem; bilgisayar, fiber-optik, çipler, atom enerjisi kullanım teknolojisi gibi mikro elektronik teknolojiler üzerine kurulmuştur (Yücel, 2003).

Bilgi toplumlarında gelişen bilgi iletişim teknolojileri ve bilişim sistemleri bazı konularda henüz istenilen düzeyde olamasa da, makinelerin birbiri ile bağlantı kurabileceğini, yorumlar yapabileceğini, karmaşık problemlere çözümler üretebileceğini, olayları öncelik sırasına sokabileceğini, birbirine olayları öğreterek destek olabileceğini net bir şekilde ortaya koymuş, bu çarpıcı gelişmeler dördüncü endüstriyel devrim olarak tanımlanmıştır (Öztemel, 2018). Yani bilgi çağında bilgi ve iletişim teknolojilerinin gelişiminin hızla devam etmesi sonucu, makinelerin birbirleri ile iletişime geçerek çeşitli sorunlarla baş edebileceği görülmeye başlanmıştır.

Endüstri 4.0 kavramı ilk defa Almanya'da Hannover Fuarı'nda ortaya atılmıştır. Alman Hükümeti'nin talebiyle, uzmanlar tarafından hazırlanan çalışma büyük dikkat çekmiştir (Ege Bölgesi Sanayi Odası, 2015). MacDougall (2014) ise, ilk defa 2011 yılı Hannover Fuarında, resmî belgelerle ortaya çıkan Endüstri 4.0'ın, dördüncü yeni sanayi devriminin habercisi olduğunu söylemiştir.

Endüstri 4.0, bilgisayar, internet ve bilgi iletişim teknolojilerinin gelişmesi ve birlikte kullanılarak ortaya çıkan ileri teknolojilerin sanayide üretimi, insan gücüne gerek kalmadan yönetebilmesi olarak tanımlanmıştır (Ege Bölgesi Sanayi Odası, 2015). Önceki endüstriyel devrimlere göre çok daha hızlı ilerleyen Endüstri 4.0 neredeyse her ülkede yönetim ve üretim sistemlerinde büyük bir dönüşüm getirmektedir (Schwab, 2015).

Günümüzde teknolojide yaşanan bu gelişmelerle birlikte Endüstri 4.0 olarak tanımlanan yeni bir endüstriyel devrime doğru ilerlenmektedir. Bu yeni devrim, siber-fiziksel sistemlere dayalı üretim üzerinde yoğunlaşmakta olup, bulut bilişim gibi üretimde verimliliği artıran yenilikçi bilgi iletişim teknolojileri kullanabilenlere avantaj sağlayacaktır (Çeliktaş vd., 2015). Bilgi ve iletişim teknolojilerindeki ilerleme bilgi çağında o kadar hızlı devam etmektedir ki, makinelerin "akıllı" hale gelmesiyle bazı

üretim sistemlerinde insanların yerini makinelerin almasıyla sonuçlanan yeni sanayi devrimi Endüstri 4.0 kavramı ortaya çıkmıştır.

Pamuk ve Soysal (2018) Endüstri 4.0'ın amaçlarını gerçekleştirebilmesi için birtakım araçlara ihtiyacı olduğunu belirtmiş, nesnelerin interneti ve siber-fiziksel sistemleri bu araçların arasında saymıştır. Ege Bölgesi Sanayi Odası (2015) ise raporunda, Endüstri 4.0'ın temel amacının akıllı fabrikaların kurulması olduğunu ve bu yeni yapılanma için siber fiziksel sistemlerin ve nesnelerin internetinin çok önemli rol oynadığını belirtmiştir. Öztemel (2018) de benzer şekilde, Endüstri 4.0'ın temel yapı taşları arasında siber fiziksel sistemler ve siber güvenlik sistemlerini saymıştır.

Buradan hareketle, gelişen bilgi ve iletişim teknolojilerinin Endüstri 4.0'ı oluşturabilmesi için çeşitli gereklilikleri olduğu ortaya çıkmıştır. Bu gereklilikler arasında; siber fiziksel ortamlar, siber fiziksel sistemler ve siber güvenlik alanlarının başı çektiği söylenebilmektedir.

Endüstri 4.0'ın temelini oluşturan internet teknolojisinin, günümüzde olduğundan çok daha fazla kullanılması ile birlikte siber güvenlik sistemlerinin önemini artıracak, kamu ve devletin kullandığı sistemlerin siber güvenliğini ve siber güvenliği konu edinecek olan teknolojik yeterliliği sağlamak da çok daha önemli bir hale gelecektir (Özer ve Turhan, 2019).

Bilgi İletişim Teknolojileri ve İnternet

Teknoloji, bilimsel bilgiyi uygulamaya koyma yani teknik bilim olarak nitelenmekte, insan-makine sistemlerinin tasarlanması, organizasyonu ve yürütülmesi süreçlerini sağlamaktadır (Alkan, 1987). MEB'in 2017 yılında yayımladığı 5.Sınıflar Bilişim Teknolojileri ve Yazılım Dersi Öğretmen Rehber Kitabı'nda ise teknoloji, insan yaşamını daha kolay hale getirmek için geliştirilen araç gereçler ve bunlara ilişkin bilgilerin tamamı olarak açıklanmıştır (Güven vd., 2017). Yalın (2012) ise bilgi ve teknoloji arasındaki ilişkiyi, insanların günlük hayatlarında yaşadığı; ulaşım haberleşme, beslenme, iletişim gibi sorunlarına bilimsel bilgilerden yararlanılarak, bilgisayar, televizyon, telefon, otomobil gibi araçların icat edilmesi ile örneklendirmiştir.

Tosun ve diğerleri (2006) bilgi ve iletişim teknolojilerini, her türlü bilginin elde edilmesini sağlayan, insanların kendi arasında, insanlarla elektronik sistemler arasında ve de elektronik sistemlerin birbiri ile, çok farklı iletişim tarzlarını kolaylaştıran tüm teknolojiler olarak tanımlarken, Blurton (1999); iletişim kurmak ve bilgi oluşturarak

bunları yaymak, depolamak, yönetmek için kullanılan çeşitli teknolojik aygıtlar ve kaynaklar olarak, Olakulehin (2007) ise bilgi ve iletişim teknolojisi kavramını, farklı şekillerde bilgilerin toplanması, depolanması, geri alınması ve aktarılması sürecinde yer alan teknolojiler olarak tanımlamıştır. 5.Sınıflar Bilişim Teknolojileri ve Yazılım Dersi Öğretmen Rehber Kitabı'nda bu kavram, bilgiye ulaşılması ve depolanması, saklanması, işlenmesi, taşınması aşamalarını gerçekleştiren tüm teknolojiler olarak tanımlanmıştır (Güven vd., 2017). Yani bilgi ve iletişim teknolojilerinin birçok farklı kaynakta tanımı yapılarak, bilgi ile iletişim ve teknoloji arasındaki köprü veya araç gereç; depolama, yayma, saklama, iletme ve geri alma gibi kavramlar kullanılarak benzer şekillerde ifade edilmiştir.

UNESCO 2003 yılında eğitimde bilgi ve iletişim teknolojilerinin kullanımı ile ilgili yayımladığı kılavuzda ise, bilgi ve iletişim teknolojilerini; bilgiye erişmek, depolamak, saklamak, işlemek, düzenlemek, üretmek, sunmak ve elektronik ortamda bilgiyi ileterek bilgi alışverişi yapmak için kullanılan her türlü araç gereç olarak açıklamıştır. Bu araç gereçlerden bazıları, kişisel bilgisayarlar, tarayıcılar, dijital kameralar, telefonlar, faks makineleri, modemler, CD ve DVD oynatıcılar ve kaydediciler, dijitalleştirilmiş video, radyo ve TV programları, veritabanı programları ve multimedya programları biçimindeki donanım araçları, yazılımlar ve telekomünikasyon olarak sayılmıştır (UNESCO, 2003).

Son zamanlarda bilgi ve iletişim teknolojilerinin bu kadar hızla yaygınlaşması, tüm dünyada hem bilgisayar hem de internet kullanıcı sayısını oldukça artırmıştır. İnternet; dünyadaki tüm bilgisayarları birbirine bağlayarak iletişim kurmasını sağlayan, kullanıcıların içerik paylaşmasına ve paylaşılan içeriği de erişimine izin veren en geniş ağdır (Mert, Bülbül ve Sağıroğlu, 2012).

We Are Social ve Hootsuite tarafından, 2021 yılının Ocak ayında yayımlanan rapora göre;

- Dünyada internet kullananların sayısı 4,66 milyar kişidir, yani dünya nüfusunun %56,5'i internet kullanmaktadır.
- Son bir yıldaki internet kullanıcı sayısındaki değişim ise 317 milyon kişidir yani %7,3 artmıştır (We Are Social and Hootsuite, 2021).

Türkiye İstatistik Kurumunun verileri incelendiğinde Türkiye'de de son dönemde internet ve bilgisayar kullananların sayısının hızlı bir şekilde arttığı görülmüştür. Evden internete erişim sağlama oranı 2019 yılında %88,3 iken, 2020 yılında %90,7 olmuş, internet kullanım oranı 2019 yılında %75,3 iken, 2020 yılında %79,0 olmuştur. Evlerde

bilgisayar kullanımı ise 2017 yılında %56,6 iken, 2018 yılındaki son verilere göre %59,6 olmuştur (TÜİK, 2020).

Teknolojiye erişimin daha kolay ve ucuz hale gelmesiyle birlikte, internet daha yaygın kullanılmaya başlanmış, bu durum ise çeşitli güvenlik risklerini doğurmuştur (Mert vd., 2012). İnternetin ilk kurulma amacı 1960 yılından beri bilgi paylaşımı olduğu için insanların bu sistemi kötüye kullanabilecekleri akla gelmemiş ve güvenlik geri planda bırakılmıştır (Yılmaz vd., 2015). Bilgi ve iletişim teknolojileri de son yıllarda tüm dünya çapında baş döndürücü bir hızla gelişmiş, bir taraftan hayatı kolaylaştıran yeni hizmetler ve uygulamaları geliştirmiş diğer taraftan uluslararası sözleşmelerle garanti altına alınan haberleşme ve mahremiyetin korunması gibi konulara tehdit oluşturmuştur (www.btk.gov.tr).

İçinde bulunduğumuz dönemde hem bilgi ve iletişim teknolojilerinin hem de internet teknolojisinin kolay erişilebilir hale gelmesiyle tüm toplumlarda kullanımı artmıştır. Ancak güvenlik konusunda önlem almak akla gelmemiş veya ikinci plana atıldığı için çeşitli tehditler oluşmuştur.

21. yüzyıla girerken bilgi ve iletişim teknolojilerindeki gelişmeler, ticari kaygıların yanı sıra güvenlik sorununu da gündeme getirmiştir. “Sanayi” (Yazılım, Siber Güvenlik, IoT, Akıllı Arabalar vb) ve “Sınır” (Ticaret, Gümrük, Denetim, Düzenleme, Vergi, Lisans, Güvenlik vb.) kavramında büyük değişikliklere yol açmıştır (On Birinci Kalkınma Planı, 2018).

Son 15 yılda İnternet ve Web dünyayı çok hızlı bir biçimde değiştirmiştir. İnternetin, her türlü bilgiye anında kolay ve hızlı erişim, eğitim, araştırma, eğlence, kültür, sanat, mobil çalışma, çevrimiçi sosyal topluluklar gibi insanların yararına olan avantajları olduğu gibi; spamlar, bilgisayar virüsleri, bilgisayar korsanlığı, çevrimiçi dolandırıcılık, kimlik hırsızlığı, gizlilik ihlali, sanal zorbalık gibi kurum ve kişileri rahatsız eden dezavantajları da olmuştur (W. Kim, Jeong, C. Kim ve So, 2011).

Modern toplumların küresel bağlamda birbirini etkileyerek bilgi ve iletişim teknolojilerine artan bir bağımlılığı ve ihtiyacı olduğu düşünüldüğünde, ülkeler bunun ulusal, bölgesel ve uluslararası düzeylerde yönetilmesi gereken karşılıklı sorumluluklar, bağımlılıklar ve riskler yarattığının giderek daha fazla farkına varmışlardır. Bu nedenle, siber güvenliği artırmak ve kritik bilgi altyapılarını korumak, her ülkenin başta güvenlik olmak üzere sosyal ve ekonomik refahı için de çok önemli olmuştur (ITU, 2008b).

Öztürk’e (2014) göre, modern dünyada, bilgisayar sistemleri ve internet; insanlar, kurumlar ve hükümetler için kritik önem taşıyarak, tüm paydaşlar için büyük avantajları

beraberinde getirmiştir. Hayatımızın hemen her alanını daha rahat ve daha kolay hale getiren bilgi ve iletişim teknolojileri dünyayı birbirine daha bağlı hale getirirken, diğer taraftan dijital güvenlik endişeleri özellikle son on yılda ülkeler için çok hızlı bir biçimde artmıştır. Başlıca sebepleri arasında, hükümetlerin ulaşım, finans, enerji, iletişim gibi kritik altyapılarının bilgisayar kontrollü sistemler veya web tabanlı hizmetler (e-sağlık gibi e-devlet gibi hizmetler) ile kamu kullanımına açması sayılabilir. Bu sistemleri kurmak, geliştirmek, yönetmek ve bakımını yapmak için milyarlarca dolar harcanmakta ve vatandaşlar hakkında çok kritik ve özel bilgileri işlenip ve saklanmaktadır. Dahası askeri, siyasi/diplomatik ve bilimsel araştırmalarla ilgili konular ve bunlarla ilgili çok gizli bilgiler internet üzerinden hükümetler arasında paylaşılabilmektedir. Tüm bu kritik bilgiler, hacker grupları, terörist grupları, istihbarat servisleri ve diğer devletler tarafından tehdit altında olup saldırıya uğramaktadır. Bu nedenle içinde bulunduğumuz dönemde savaş, yalnızca donanmalarla değil, kötü amaçlı kodlar, yazılımlar vb. kullanarak siber saldırı, savaş vb. anlamına da gelir (Öztürk, 2014).

Bilgi ve iletişim teknolojileriyle beraber internet teknolojisinin kullanımındaki bu artış, toplumlara getirdiği faydaların yanı sıra çeşitli tehlikeleri de doğurmuştur. Dijitalleşen dünyada neredeyse tüm sistemlerin teknoloji ve internete bağlı olması, hükumetlerin kritik alt yapıları için tehdit oluşturmaktadır. Siber tehditler ve siber saldırılar ve siber savaşlar bu tehditlerin başında gelmektedir. Bu sebeple siber güvenlik günümüzde devletler ve tüm bireyler için çok kritik bir önem taşımaktadır.

Siber Güvenlik

Günümüz dünyasında dijital ürünlerin hızla yaygınlaşması, bilişim sistemlerini, kritik altyapıları ve kişileri siber saldırıların hedefi haline getirmektedir (On Birinci Kalkınma Planı, 2018). Bilişim teknolojilerinin hızlı gelişimi eskiden beri bilinen suçların rahatça işlenmesine yol açarken, birbirinden farklı suçların da meydana gelmesine de neden olmuştur. Çünkü, internetin getirdiği faydalarla birlikte "siber suç" işlemek önceden olduğu kadar teknolojik beceri gereksinimini ortadan kaldırmıştır. Bununla beraber, bilişim teknolojilerinin hayatımızın hemen her alnında yer alması, kişilerin "suç mağduru olma riskini" artırırken, "siber alanı" da "ulusal güvenliğin" hayati bir unsuru haline getirmiştir. Bu yüzden son zamanlarda siber güvenlik en fazla tartışılan konulardan birisi haline gelmiştir (Hekim ve Başıbüyük, 2013).

Siber güvenlik, bireylerin yaşantısında gün geçtikçe daha fazla yer alan teknoloji ve internetin gelişimiyle hem insanları hem de hükümetleri ilgilendiren en önemli konulardan biri haline geldiği söylenebilir. Çünkü, teknoloji ve internet kullanımının artması, bu ortamları kullanarak kişilere, kurumlara ve hükümetlere zarar verme tehlikesini de artırmıştır. Siber güvenliğin sağlanabilmesi, siber âlemin güvenli olabilmesi ile mümkündür. Siber alanın emniyetli olabilmesi için ise bilginin; "gizliliği (confidentiality), bütünlüğü (intergrity) ve erişilebilirliği (availability)" unsurlarının korunması gerekmektedir (Goodrich ve Tamassio, 2010).

Tüm dünya ülkelerini etkileyen bir konu olarak, siber güvenliğin birbirine benzeyen ve farklılaşan unsurlarıyla literatürde birçok tanımı yer almaktadır. Siber güvenliği tüm açılarıyla anlayabilmek için, bazı OECD ülkelerindeki siber güvenlik tanımlarına bakmakta fayda olacaktır.

Avustralya Başsavcılığı Departmanı, 2009 yılında Siber Güvenlik Stratejisi belgesinde siber güvenliği; elektronik ortamlarda yine elektronik veya benzeri yollarla işlenen, saklanan, kaydedilen ve iletilen bilgilerin gizliliği, kullanılabilirliği ve bütünlüğü ile ilgili tüm önlemler, olarak tanımlamıştır. Kanada Kamu Güvenliği Departmanı ise 2010 yılında, Kanada'nın Siber Güvenlik Stratejisi belgesinde aynı kavramı; elektronik bilgileri ve bu bilgilerin işlenmesi, iletilmesi ve depolanması için kullanılan elektronik ve fiziksel altyapıya yetkisiz erişim, kullanım, manipülasyon, kesinti veya imhaya yönelik saldırıları tespit etmek, korumak ve kurtarmak, olarak açıklamıştır (Klimburg, 2012).

Alman Federal İçişleri Bakanlığı 2011 yılında Almanya için Siber Güvenlik Stratejisi belgesinde, küresel çaptaki siber uzay risklerinin kabul edilebilir ölçüde azaltıldığı bilgi teknolojileri güvenli olması durumu ve bunun için alınan önlemlerin tamamı, olarak siber güvenliği tanımlamıştır (Klimburg, 2012). Fransız Ulusal Savunma ve Güvenlik Genel Sekreterliği 2011 yılında Bilgi Sistemleri Savunması ve Güvenliği-Fransa'nın Stratejisi belgesinde ise, bir bilgi sisteminin, depolanan, saklanan, işlenen veya iletilen veriler ve bu sistemlerin erişilebilir olan ilgili hizmetlerin kullanılabilirliğini, bütünlüğünü ve gizliliğini tehlikeye atabilecek siber uzaydan gelen olaylara karşı korunaklı olması olarak tanımlamış, siber güvenliğin, bilgi sistemlerinin güvenlik yöntem ve tekniklerinden yararlanarak ve siber suçlarla mücadele etme ve siber savunma oluşturmaya dayandığını belirtmiştir (Klimburg, 2012).

Beyaz Sarayın Ulusal Güvenlik Başkanlık Yönergesinde siber güvenlik, bilgisayarların, elektronik iletişim sistemlerinin, elektronik iletişim araçlarının, kablolu iletişim sistemlerinin ve bunlar aracılığıyla gönderilen ve yerleşik bilgiler de dahil olmak

üzere tüm elektronik iletişimin zarar görmesinin önlenmesi, korunması ve onarılması olarak tanımlanmıştır (The White House, 2008).

ABD'de Siber Güvenlik ve Altyapı Güvenliği Ajansı (CISA) kurumu ise siber güvenlik tanımını; ağları, cihazları, ve verileri yetkisiz erişim veya suç niteliği taşıyan kullanımdan koruma sanatı ve bilginin gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlayarak güvende tutma uygulaması, olarak yapmıştır (https://us-cert.cisa.gov).

Siber güvenliğin en belirleyici özelliği, siber uzayın temel yapıtaşı olan bilgi ve iletişim teknolojilerinin kullanımı sonucunda ortaya çıkan güvenlik açıkları nedeniyle korunması gereken tüm varlıkların korunması gerektiği gerçeği olmuştur (Solms ve Niekerk, 2013). Tüm tanımlara bakıldığında ortak olarak siber güvenlik, siber uzayda bilginin, bilgi ve iletişim teknolojileri ve internet yolu ile aktarılması, saklanması, iletilmesi, depolanması, işlenmesi aşamalarında, gizlilik, bütünlük ve kullanılabilirliğinin güvende tutulması ile ilgili olduğu söylenilebilir.

Siber Güvenlik ile Bağlantılı Kavramlar

Siber güvenlik tanımlarından da anlaşıldığı üzere, siber güvenlik kavramının tam olarak anlaşılması ancak siber ile ilgili diğer bileşenlerin de ne ifade ettiğini bilmek suretiyle mümkün olacaktır. Bu nedenle siber güvenlik ile bağlantılı kavramların tanımının yapılması gerekli görülmüştür.

Siber: Merriam sözlüğü "cyber" kelimesini; "Bilgisayar, bilgisayar sistemleri, bilgisayar ağları (internet vb.) veya bunlarla ilgili olan her şey" olarak tanımlamıştır (Merriam-Webster, 1992).

Siber ortam: Uluslararası Telekomünikasyon Birliği siber ortamı, "Ağlara doğrudan veya dolaylı olarak erişim sağlayabilen kullanıcıları, ağları, cihazları, tüm yazılımları, süreçleri, kaydetme, depolama veya aktarımdaki verileri, bilgileri, uygulamaları, hizmetleri ve sistemleri içerir" şeklinde tanımlamıştır (ITU, 2008a).

Siber alan: "Birbirine bağlı halde bulunan bilgi teknolojisi altyapıları ağı anlamına gelir ve internet, telekomünikasyon ağları, bilgisayar sistemleri ve kritik endüstrilerdeki gömülü işlemciler ve denetleyicileri kapsar" şeklinde tanımlanmıştır (The White House, 2008).

Siber uzay: "Sadece donanım, yazılım ve bilgi sistemlerini değil, aynı zamanda bu ağların içinde yer alan kişileri, kurumları ve sosyal etkileşimi de içeren internetten daha fazlası" olarak tanımlanmıştır (Klimburg, 2012).

Siber saldırı: Wamala (2011) siber saldırıları, "Fiziksel olarak veya bilgi varlığı etrafındaki herhangi bir tehdit tarafından güvenlik kontrollerinin ihlal edilmesi" olarak tanımlarken, Kanada Siber Güvenlik Merkezi Sözlüğü benzer şekilde, "Bir bilgisayar sistemine, ağa veya cihaza yetkisiz olarak müdahale etmek, manipüle etmek, yok etmek, zarar vermek veya yetkisiz erişim sağlamak için elektronik cihazların kullanılması" olarak tanımlamıştır (Canadian Centre for Cyber Security, 2021).

Siber Suç: Kanada Siber Güvenlik Merkezi Sözlüğü siber olayı, "Amacına ulaşıp ulaşmamasını gözetmeksizin, herhangi bir bilgisayar ağı veya sistem kaynağına erişim sağlamak, bunları değiştirmek, hasar vermek, bozmak, yok etmek, silmek veya kullanılamaz hale getirmek için yapılan her türlü yetkisiz girişim", olarak tanımlarken, Merriam Webster siber suçu, "Özellikle yasa dışı olarak verilere ve bilgilere erişmek, iletmek veya değiştirmek için bir bilgisayar aracılığıyla gerçekleştirilen suç faaliyetleri (dolandırıcılık, hırsızlık veya çocuk pornografisi dağıtımı gibi)", olarak tanımlamıştır (Merriam-Webster, 1991; Canadian Centre for Cyber Security, 2021).

Siber güvenlik kavramının daha iyi anlaşılabilmesi için; siber, siber ortam, siber alan, siber uzay, siber saldırı ve siber suç tanımları yapılmıştır. Bu tanımlara bakıldığında siber ortam, siber alan ve siber uzayın birbiri ile yakın anlamlar ifade ettiği, benzer durumun siber saldırı ve siber suç için de geçerli olduğu söylenilebilmektedir.

Siber Tehditler

Son zamanlarda siber saldırılar kişiler, kurumlar ve hükümetler için çok daha ciddi problemler haline gelmektedir. Saldırganlar, bilgi sistemlerine sızmak ve saldırmak için çok çeşitli şekillerde siber tehdit türlerini kullanmaktadırlar (Öztürk, 2014). Siber tehditler; bilgi ve iletişim teknolojilerinin imkanlarından yararlanılarak ortaya çıkmış yeni suçları doğuran siber saldırıların beraberinde; bilgi ve iletişim teknolojilerinin imkanlarının araç niteliğinde görev aldığı, var olan suçların siber alana aktarılmış versiyonlarını da kapsamaktadır (Ünver vd., 2009). Siber saldırılar kişi, kurum ve hükümetlerin telafisi mümkün olmayan ekonomik kayıplara yol açmasının yanı sıra, saygınlık ve imajları açısından ciddi problemler oluşturması sebebiyle siber güvenlik kritik bir önem taşımaktadır (Semerci ve Keser, 2019).

Siber tehditlerin kapsadığı alanın genişliği, siber suçların çok farklı şekil ve içeriklerde ortaya çıkabileceği gibi eskiden beri var olan suçların siber alan ile farklı

forma girmiş olmasından ve teknolojideki gelişiminin bu denli hızlı artmasının ön görülememesinden kaynaklanmıştır (Hekim ve Başıbüyük, 2013). Farklı araştırmacıların siber tehditler, siber saldırı yöntemleri ve buna benzer başlıklar altında sınıflandırmaları incelenmiş, benzer ve farklı yönleri ile ele alınarak açıklanmıştır.

Öztürk (2014) siber tehditleri;

- Kötü Amaçlı Kod/Kötü Amaçlı Yazılım (Malicious Code/Malware)
- İstenmeyen Program (Unwanted Program)
- İstenmeyen Elektronik Posta (Spam)
- Oltalama/Yemleme (Phishing)
- Koklama (Sniffing)
- Yanıltma (Spoofing)
- Hizmet Engelleme (DoS and DDoS)
- İçeriden Saldırılar (Insider Attacks)

olarak sınıflamıştır.

Kötü Amaçlı Kod'u ise; virüs, solucan, truva atı, Botlar/Botnet'lerin ortak adı olarak tanımlamıştır. Bu tür kötü amaçlı kodlar/yazılımlar önce ağdaki bir bilgisayara bulaşır ve ardından bu virüslü bilgisayar aracılığıyla ağdaki diğer bilgisayarlara yayılır. Bilgisayar sistemlerine ve ağlarına zarar vermek, çalışamayacak duruma getirmek, işleyişini olumsuz etkilemek için tasarlanmıştır (Öztürk, 2014).

İstenmeyen Program, kötü amaçlı yazılımlara ek olarak bilgisayarlara, tarayıcı paraziti, reklam yazılımı, casus yazılım ve bunlar gibi istenmeyecek yazılımlar, programlar tarafından da tehdit oluşturur. Bu programlar, kullanıcının hiçbir izin vermemesine rağmen gizlice bilgisayara kurularak, genellikle reklam yapma, kullanıcının internet trafiğini toplama ve analiz etme ve bilgi çalma gibi işlemler gerçekleştirir (Schryen, 2007).

İstenmeyen elektronik posta yani daha yaygın kullanılan adıyla spam mesajları; en fazla çok e-posta aracılığıyla gönderilmekle birlikte, SMS, MMS, anlık mesaj, arama motorları, bloglar, VoIP gibi diğer elektronik iletişim kanalları/hizmetleri de bu tür mesajlarla karşı karşıya kalabilmektedir. OECD ise daha genel bir tanım kullanarak, internetle ilişkili olan elektronik mesajlar, önemsiz postalar, önemsiz haber gönderileri ve genellikle ticari faaliyetler ile ilgili toplu gönderiler olarak tanımlamıştır (Schryen, 2007; OECD Glossary of Statistical Terms, 2002).

Oltalama, yemleme veya kimlik avı olarak çevrilen phishing, kullanıcıların banka hesapları, ipotek hesapları, kredi kartı hesapları vb. finansal hesaplara erişmek için kullanılan sosyal güvenlik numaraları, oturum açma adları ve şifreleri gibi gizli bilgilerini elde etmek için yapılan yanıltıcı girişimlerdir (Öztürk, 2014). Koklama ise kullanıcıların bilgisayar ağlarında gönderilen alınan verileri alabilmek için, bilgisayar ağlarında yapılan gizli dinleme girişimleridir (Öztürk. 2014). Yanıltma, kullanıcıların sahte kimlikler kullanılarak bilgilerine erişme girişimleridir (Öztürk, 2014).

Hizmet engelleme DoS ve DDoS olarak iki şekilde gerçekleşmektedir. DoS saldırısı, internette bir ağ veya sunucu tarafından sağlanan hizmeti bozmayı amaçlar. Bir DoS saldırısının trafiği eğer birden fazla kaynaktan gelirse buna da dağıtılmış hizmet reddi, yani (DDoS) saldırısı denmektedir. DDoS saldırısının etkililiğini artırmak ve savunmayı daha zor hale getirmek için, birden fazla saldırı kaynağı kullanılmaktadır (Peng, Leckie ve Ramamohanarao, 2007). İçeriden Saldırılar, kullanıcıların kendi çalıştıkları kurumlarda, içeriden kimselerin daha az çaba sarf ederek sisteme bir saldırı düzenlemesi, verileri silmesi, bozması veya çalması olarak açıklanmaktadır (Öztürk, 2014).

Ünver ve diğerleri (2009) ise Siber Tehditleri 5 temel gruba ayırarak bazı saldırılara;

- Hizmetin Engellenmesi (DoS ya da DDoS) saldırıları,
- Kötücül Yazılımlar, Yemleme (phishing),
- İstem dışı elektronik posta (spam),
- Şebeke trafiğinin dinlenmesi (sniffing, monitoring)

başlıkları içinde yer vermiştir.

DoS ve DDos saldırıları, kullanıcıların haberi olmaksızın sistemin güvenlik açıklarından yararlanılarak ele geçirilen sistemin uzaktan saldırgan tarafından yönetilmesi olarak tanımlanmaktadır (Ünver vd., 2009). Bilgisayar virüsleri (solucanlar, Truva atları, mantık bombaları), klavye izleme (key logger), zombiler veya botlar (zombies, or bots), istem dışı reklam yazılımı (adware), casus yazılımı (sypware) gibi saldırıların hepsi kötü amaçlı yazılımlar sınıfına girmektedir (ITU, 2007).

Virüsler; kullanıcının haberi olmadan bir sisteme yüklenir ve kendini kopyalama özelliği olan kötü amaçlı kodlardan oluşmaktadır (bazı durumlarda çoğaltma kesin değil, bir mutasyon olabilir). Virüslü kullanıcının temas ettiği diğer kullanıcılara da bulaşarak sisteme zarar vermektedir. Çok çeşitli virüsleri ayıt etmek imzalarını, davranışlarını, nasıl çoğaldıklarını ve yayıldıklarını, neden oldukları arıza türlerini bilmekle mümkün

olabilmektedir (ITU, 2007). Klavye izleme, kullanıcının bilgisayar kullanırken yaptığı tuş vuruşlarını izleyerek kaydedebildiği gibi, yazılım olarak görünmeyip tuş vuruşlarını kaydeden donanım keylogger'ları da mevcuttur (ITU, 2007).

Zombiler veya robotların kısaltması olarak kullanılan botlar; bilgisayarlardan oluşan gizli bir ordu oluşturmak amacıyla sisteme uzaktan bağlanarak kontrol eden yazılımlardan oluşan programlardır. İstem dışı reklam yazılımlar ise, ticari işlemleri özelleştirmek için kullanılan programlardır (ITU, 2007).

Casus yazılımı, kullanıcıların bilgisayarlarındaki bilgileri gizlice kaydetmektedir. İnternete bağlanan normal herhangi normal bir bilgisayarda kullanıcıdan habersiz ortalama 28 casus yazılım programı, kurum bilgisayarlarının çok büyük çoğunluğunun ise en az bir casus programı kurulu olmaktadır (ITU, 2007).

Yemleme; bu saldırı tipi saldırganlar tarafından güvenilir internet sitelerinin çok benzerlerini oluşturarak, kullanıcılarına sitelerin bağlantılarını içeren e-postalar göndererek kullanıcıları bu sahte sitelere yönlendirerek bilgilerine ulaşmak yoluyla yapılır. Daha çok bankacılık veya elektronik ticaret hizmeti sunan internet siteleri taklit edilmektedir (Ünver vd., 2009).

İstem dışı elektronik posta, toplu olarak gönderilen ticari veya tanıtım amaçlı istenmeyen e-postalardır. Burada saldırganlar, web kullanıcılarını bir ürün veya hizmet sipariş etmeleri için ikna etme yolu izleyebilirler. Hizmet sağlayıcıları ve kamu yetkilileri spam mesajları engellemek için birçok yol denemekte, bazı spam saldırganları cezalar almakta ancak buna karşın spam hala önemli bir tehdit oluşturmaya devam etmektedir (ITU, 2007).

Şebeke trafiğinin dinlenmesi, saldırgan iletişim protokollerini kullanarak ağ üzerinden iletilen şifrelenmemiş verileri yakalayarak veya dinleyerek gerçekleştirilmektedir (ITU, 2007). Şebeke trafiğinin dinlenmesinin iki alt boyuta; aktif dinleme, izleme (monitoring) ve pasif dinleme (sniffing) olarak ayrılmıştır (Ünver vd., 2009).

Semerci ve Keser (2019) çalışmalarında, siber güvenliği tehlikeye atan siber saldırı türlerini;

- Zararlı Programlar (Malware),
- Hizmet Engelleme ve Hizmet Dışı Bırakmaya Yönelik Saldırılar,
- Kriptografik Saldırılar,
- Enjeksiyon Saldırıları,

- Gizli Dinleme (Eavesdropping),
- Paket Koklama (Packet Sniffing),
- Tuş ve Ekran Kaydediciler (Keylogger ve Screenlogger),
- Sosyal Mühendislik Saldırıları,
- Oltalama/Ses Aldatmacası (Pnishing/Vishing),
- Veri Bütünlüğünü Hedef Alan Saldırılar

olarak sınıflandırmışlardır.

Zararlı Programlar; "Truva atı, virüs, klavye dinleme, casus yazılımlar, önemsiz e-posta gibi kötücül yazılımlar, sistemdeki açıklar kullanılarak verileri elde etme, değiştirme, yok etme" gibi amaçlarla kullanılırlar. Bu saldırı türleri, kolay kullanıldığı ve hızlı sonuç verdikleri için sıkça tercih edilmekte, kişiler, kurumlar ve hükümet için en tehlikeli saldırı türleri arasında sayılmaktadırlar (Yılmaz ve Sağıroğlu, 2013). Günümüz dünyasında kullanıcılar; "virüs, solucan, Truva atı, fidye yazılımı, adware gibi pek çok zararlı yazılımın (malware)" saldırıları ile karşı karşıya kalmaktadırlar. "Virüsler, solucan, adware" ve bunlar gibi yazılımlar; "reklam, siber suçlar, bazen sadece ego tatmini gibi çeşitli çıkarlar için bilgisayar, tablet, akıllı cep telefonu" vb. sistemlere hasar vermek üzere tasarlanmışlardır. Bu tür zararlı yazılımlar son dönemlerde o kadar ilerlemiştir ki, ülkeler arasında siber terör olarak hükümetler arasında siber savaşlar olarak karşımıza çıkmaktadır (Fox, 2016).

Hizmet Engelleme ve Hizmet Dışı Bırakmaya Yönelik Saldırılardan, DoS (Danial Of Service), "hizmeti aksatma veya hizmetin işlevini tamamen yok etme" anlamına gelmekte, kullanıcıların internete erişmeleri ya tamamen engellenmekte ya da çok yavaşlamaktadır. DDos (Distrubuted Denial of Service) saldırısı ise, saldırganın kullanıcılara ulaşmadan önce makine veya bilgisayarlardan oluşan bir sistem oluşturarak harekete geçmekte ve DoS saldırısına benzer şekilde internet "hizmetini aksatmakta veya hiç hizmet veremez hale" getirmektedir. Bu saldırı türünde saldırganın gerçek kimliğini gizlemesi ve tespit edilmesinin zorluğu ortaya çıkmaktadır (Yıldız, 2014). DoS ve DDoS türlerinden bazıları;

- Ölüm Pingi, Flood Saldırıları,
- SYN Flood Saldırıları,
- UDP Flood Saldırıları,
- Media Data Flood Saldırıları,
- Smurf Saldırıları, http saldırıları,

- DNS Zehirleme, Hafıza Taşmaları,
- ICMP (Internet Control Message Protocol),
- Finger Komutu,
- Excessive VERB

olarak sıralanmıştır. (Semerci ve Keser, 2019)

Kriptografik saldırılar, şifreli bilgilerin şifrelerini kriptoanaliz yöntemleri ile çözüp elde edilmesine yönelik saldırı türleridir. (Canbek ve Sağıroğlu, 2007). Kriptanaliz, uygun anahtarlar kullanılarak bilinmeden şifrelenmiş iletişimlerin çözülmesi sanatı olarak tanımlanmaktadır (Yıldız, 2014). Bu saldırı türlerinden bazılarını Semerci ve Keser (2019) aşağıdaki gibi sıralamıştır:

- Kaba Kuvvet (Brute Force) Saldırıları
- Sözlük (Dictionary) Saldırıları
- Ortadaki Adam (Man in The Middle) Saldırıları
- Sadece Şifreli Metin (Ciphertext-Only) Saldırıları
- Bilinen Düz Metin (Know Plaintext) Saldırıları
- Seçilmiş Düz Metin veya Şifreli Metin (Chosen Plaintext, Ciphertext) Saldırıları
- Uyarlanır Seçili Düz Metin (Adaptive Chosen Plaintext) Saldırıları
- İlişkili Anahtar (Related Key) Saldırıları

Enjeksiyon saldırıları; bu saldırı türünde saldırgan bir yorumlayıcıya düşmanca veriler göndermesiyle ortaya çıkmaktadır. Enjeksiyon kusurlarıyla, genellikle eski yazılım türlerinde karşılaşılmaktadır. Genellikle SQL, LDAP, XPath veya NoSQL sorgularında, işletim sistemi komutlarında, XML ayrıştırıcılarında, SMTP üstbilgilerinde, ifade dillerinde ve ORM sorgularında bulunmakta, verilerin bozulmasına, silinmesine veya yetkisiz taraflara ifşa edilmesine, hesap verebilirliğin kaybolmasına veya erişimin reddedilmesine neden olabilmekte hatta bazen ana bilgisayarın tamamen ele geçirilmesiyle sonuçlanmaktadır (OWASP, 2017).

Gizli dinleme; “bir ağ veya kanal üzerinden iletilen verinin, kötü niyetli üçüncü kişiler tarafından araya girilerek alınması” olarak tanımlanmakta olan bu saldırı türü, göndericiden alıcıya aktarılan veriye bir noktada ulaşılıp, farklılaştırarak göndericiye iletilmesine bile sebep olabilir. İngilizce olarak “eavesdropping (saçak damlası)” şeklinde isimlendirilen saldırı türü çok çeşitli araçlarda kullanılabilmektedir. Başka bir cihaz veya ağ ile bağlantısı bulunmayan bilgisayar da dahil olmak üzere, “mikroçip”, “ekran” veya

“yazıcı” vb. elektronik kısımlarından çıkan “elektrik” veya “elektromanyetik” yayılım izlenerek habersizce dinlenebilir (Canbek ve Sağıroğlu, 2007).

Paket koklama (packet sniffing); Sniffing sözcüğü koklamak olarak geçmekte ve temel olarak verinin yolunu kesmek suretiyle ağdaki paketler yakalayarak içeriği okunabilmektedir. Başka bir deyişle ağ üzerinden birbirine bağlı bilgisayarların verilerini dinleyerek, şifreleri (email, web, ftp, telnet, SQL), e-postaları, gönderilen dosyaları (e-mail, ftp) yakalamaktır (Yıldız, 2014).

Tuş ve ekran kaydediciler, bilgisayar kullanıcılarının klavye aracılığıyla yazdıkları metinleri kopyalayarak, tuşlarının vuruşlarını tespit edebilen ve e-posta kullanılarak saldırganın erişmesine imkan veren saldırı türüdür. Bu programlar klavye ile yazılan her şeyi kaydedebilme yeteneğine sahiptir. Ekran kaydediciler ise, kullanıcıların ekran görüntülerini kopyalayarak saldırganın e-posta ile erişmesini sağlayan saldırı türüdür. Ekrandan anlık görüntüler alarak o esnada yapılanlar takip edilebildiği gibi şifrelerde kolaylıkla görülebilir (Türkiye Bankalar Birliği, 2015). Bu saldırılara uğrayan bilgisayarda yapılan, kullanıcıya bilgilerin girildiği internet sitelerinde kullanılan parola, şifre, kredi kartı bilgileri, sosyal medya hesap bilgileri, kullanıcı parolaları gibi kişiye özel bilgi, belge ve resimler bilgisayar korsanlarının eline geçmektedir (Semerci ve Keser, 2019).

Sosyal mühendislik saldırıları; saldırgan öncelikle hedeflediği kişilerin güvenini kazanarak akıllıca oluşturulmuş bir senaryo kullanmaktadır. Bir kurumdaki çalışanların bilgilerini alıp kullanarak o kuruma sızar. Sosyal mühendislik saldırılarının iki türü vardır. Temeli insana dayanan türde saldırganlar, kurbanlarının şifre, parola ve kişisel bilgilerini elde etmek, kendi amaçları doğrultusunda istediklerini yaptırmak amacıyla taklit, etkileme, korkutma ve ikna gibi yöntemler kullanmakta; temeli bilgisayar ve teknolojiye dayanan türde, bilgisayar kullanımı sırasında ortaya çıkarılan pop-up ekranlar, sahte e-postalar, güvenilir kurum ya da işletmelerin sitelerine benzer sahte siteler üzerinden kullanıcı şifre ve bilgilerinin girilmesi gibi uygulamalar olarak açıklanmaktadır (Semerci ve Keser, 2019 ; Türkiye Bankalar Birliği, 2015).

Oltalama/Ses Aldatmacası (Phishing/Vishing); Oltalama olarak Türkçeleşen saldırı türü İngilizce “password (şifre)” ve “fishing (balık avlamak)” kelimelerin karışımı ile ortaya çıkmıştır. Kullanıcıların gizli bilgilerini (şifre, parola, müşteri numarası, kullanıcı adı, kredi kartı numarası vb.) dijital alanlarda yakalanmasını hedefleyen saldırı türüdür. Vishing ise ses kullanılarak kandırma şeklinde gerçekleşir. Bu nedenle İngilizce “phishing” kelimesindeki “p” harfinin yerini “voice” kelimesindeki “v” harfi alarak ses

aldatmacası şeklinde Türkçeleşmiştir. Yut dışı internet servis sağlayıcılarından (proxy) yararlanılarak kurbana istenilen numara gösterilmektedir. Telefon numaralarını kişi tekrar aradığında saldırganın öncesinde derlediği bir kurumun "sesli yanıt sistemine" veya "çağrı merkezine" benzeyen bir konuşma ile saldırganlar kişilere ait özel ve gizli bilgilere ulaşabilmektedir (Türkiye Bankalar Birliği, 2015).

Veri bütünlüğünü hedef alan saldırılar; siber güvenliğin en önemli yapıtaşlarından olan veri bütünlüğünü hedef alarak, siber ortamdaki açıkların kullanıldığı saldırı türüdür (Semerci ve Keser, 2019). Bu saldırı türlerinden biri olan veri dağıtma (data diddling) yöntemi kullanılarak bir bilgisayar sistemine yetkisiz olarak girilip veriler değiştirildikten sonra çıkarken tekrar eski haline getirilmesi olarak gerçekleşmektedir. Yine bu saldırı türlerinden bir diğeri olan dilimleme saldırısı, salam dilimleme saldırısı veya salam sahtekarlığı olarak farklı isimlerle anılmakta, siber suçluların, saldırılarının anlaşılmaması için her seferinde az miktarda yavaş yavaş para veya veri çaldıkları bir yöntemi tarif etmektedir (Burch, Ganda, Kalola ve Borad, 2017).

Türkiye'de Siber Güvenlik

Türkiye, siber saldırıların bir taraftan kaynağı, diğer taraftan hedefi olarak dünyanın ilk 10 ülkesi arasında yer alırken, DDoS saldırılarında Türkiye, %5,84'lük oranı ile dünyada 7.sırada bulunmakta, 2017 yılında siber saldırıların tahmini küresel maliyeti yıllık yaklaşık 400 milyar ABD$ olurken, 2019 yılında ise bu maliyetin 2,1 trilyon ABD$'na çıkması öngörülmektedir (On Birinci Kalkınma Planı, 2018).

Bilgi ve iletişim teknolojilerinin faydalarından en iyi şekilde yararlanabilmek ancak ulusal siber güvenlik ile ilgili yürütülen çalışmaların devamlılık içinde ve etkili bir şekilde gerçekleştirilmesiyle mümkün olacaktır. Her geçen gün farklılaşan siber tehditler karşısında kişilerin, kurumların, sektörlerin yani ulusal siber ortamın güvenliği, ülkemizin ekonomik büyümesinde de çok kritik bir önem taşımaktadır. Küresel salgın ve sonrasında da devam eden süreç, ekonomik ve toplumsal hayatta çok net hissedilir değişimlerin ortaya çıktığı ve teknolojik dönüşümün hızlandığı, siber güvenlikle ilgili gereksinimlerin (altyapı, yeni teknolojiler, insani kaynaklar, farkındalık) de arttığı bir dönem olmuştur (Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, 2020).

Yabancı ülkelerden alınan siber güvenlik ürün ve çözümlerinin bizzat kendileri siber güvenlik risk ve tehdidi (arkakapı vb. güvenlik açıkları) oluşturduğu için siber güvenliğin sağlanmasında yerli ve milli ürün ve çözümlerin geliştirilip kullanılması

büyük önem taşımaktadır (On Birinci Kalkınma Planı, 2018). Siber uzayın ortaya çıkışı hem bireyler için hem de hükümetler için güvenlik konusunda çeşitli tehditler oluşturmuştur. Siber uzayda saldırılar gerçekleştiren kişiler hükümetlerin güvenlik alt yapılarına birçok zarar vererek ciddi boyutta hasarlara yol açabilmektedirler (Bıçakcı, Ergun ve Çelikpala, 2015).

Siber saldırılar sadece kişi ve kurumları değil, ülkelerin ulusal güvenliğini de tehdit etmekte, siber saldırılar ve siber casusluğun ötesine geçerek siber savaş boyutuna ulaşırken; siber güvenlik alanı tüm dünyada kritik bir öneme sahip olmakta, sadece ülkemizde değil, farklı birçok ülkede de büyük bir eleman ihtiyacı oluşmaktadır. 2019 yılına kadar siber güvenlik alanında 1,5 milyon iş gücüne ihtiyaç duyulacağı öngörülmektedir. Ülkemizde ise yaklaşık olarak 15-20.000 siber güvenlik uzmanına gereksinim olacağı tahmin edilmektedir (On Birinci Kalkınma Planı, 2018).

Siber tehditlerin sayısı her geçen gün artarken türleri de değişiklik göstermekte, verdikleri zarar git gide artmaktadır. Bu nedenle, siber tehditlerle mücadele ederken kaynakların da doğru planlanması kritik önem taşımaktadır. Detaylı analiz edilerek oluşturulmuş riskler ve ihtiyaçlar, teknolojik trendler doğrultusunda meydana gelebilecek gelişmelere dayalı kısa ve uzun vadeli planlamalar, güvenli siber uzayın temelini oluşturacaktır (Ulusal Siber Güvenlik Stratejisi ve Eylem planı, 2020).

Yasal Düzenlemeler

Ulusal güvenlik konusunda bu kadar önemli bir hal almadan evvel, siber saldırılar daha çok asayiş ve hukuk ile ilgili bir konu idi. Ordular tarafından, kara, hava, deniz ve uzaydan sonra siber de farklı bir saldırı alanı olarak düşünülmeye başlamadan önce, hükumetler öncelikle siber alanın yasalara aykırı suç işlemeyi önlemek hususu üzerine odaklanmışlardır. Türkiye'de ilk yansıması 6 Haziran 1991'de 3756 Sayılı Türk Ceza Kanunun Bazı Maddelerinin Değiştirilmesine Dair Kanun ile ortaya çıkmıştır. Bu değişikliğin 20. maddesi ile "Bilişim Alanında Suçlar" başlığı altında Onbirinci Bab eklenmiş ve "bir bilgisayardan programların, verilerin veya diğer unsurların hukuka aykırı olarak ele geçirilmesi veya bunların başkasına zarar vermek üzere kullanılması, nakledilmesi veya çoğaltılması" yasada meydana gelen bu değişiklik ile ceza unsuru olarak kabul edilmiştir (Bıcakcı vd., 2015 ; TCK, 1991).

26 Eylül 2004 tarihinde kabul edilen 5237 sayılı Türk Ceza Kanunu'nda ise daha geniş yer verilerek, Üçüncü Kısmın Onuncu Bölümü Bilişim Alanında Suçlar'a

ayrılmıştır. Madde 243 “Bilişim Sistemine Girme”, Madde 244 “Sistemi engelleme, bozma, verileri yok etme veya değiştirme”, Madde 245 “Banka veya kredi kartlarının kötüye kullanılması” olarak maddeler detaylandırılmıştır (TCK, 2004).

18 Temmuz 2006’da 3713 sayılı Terörle Mücadele Kanunu’nun bazı maddelerinde değişiklik yapılmış ve terör suçu niteliği taşıyan suçlar açıklanmıştır. Madde 4 “Aşağıdaki suçlar 1 inci maddede belirtilen amaçlar doğrultusunda suç işlemek üzere kurulmuş bir terör örgütünün faaliyeti çerçevesinde işlendiği takdirde, terör suçu sayılır” denilerek Türk Ceza Kanunu’nun bazı maddeleri sıralamıştır. Bu maddelerin arasında Bilişim Suçları ile ilgili 243, 244, 245 maddeleri de yer almaktadır (Terörle Mücadele Kanunu, 2006).

5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" 23 Mayıs 2007 tarihinde 26530 sayılı Resmî Gazete' de yayımlanarak yürürlüğe girmiştir. Madde 1’de kanunun amaç ve kapsamı; “Bu Kanunun amaç ve kapsamı; içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları ile internet ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usûlleri düzenlemektir” şeklinde yer almaktadır (İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, 2007).

Siber güvenlik alanında atılmış en önemli adımlardan biri olan Türkiye’nin de taraf olduğu Avrupa Siber Suçlar Sözleşmesi olmuştur. Bilişim ile ilgili suçlar ulusal sınırların içinden taşıp tüm dünyayı etkilemektedir. Bu nedenle bu suçlarla baş edebilmenin yolu yine tüm dünyanın ortak ve iş birliği içinde atacağı adımlarla mümkün olacaktır (Aliusta ve Benzer, 2018). Avrupa Siber Suçlar Sözleşmesi, 23 Kasım 2001 tarihinde Budapeşte’de devletlerin imzasına açılmış, 1 Temmuz 2004 tarihinde yürürlüğe girmiş olup bu alandaki ilk uluslararası sözleşme özelliği taşımaktadır. Sözleşme şu ana kadar toplam 68 ülke; Avrupa Konseyi üyesi olan devletlerin yanı sıra, 21’i Avrupa Konseyi üyesi olmayan (ABD, Kanada, Japonya, Karadağ, Güney, Afrika Cumhuriyeti, …) ülkeler tarafından da imzalanmış, 62 devlet ile ilgili de hukuki süreci başlamıştır. Avrupa Konseyi kurucu üyesi olan Türkiye ise 10 Kasım 2010 tarihinde sözleşmeyi imzalamış ve 29 Eylül 2014 tarihinde de yürürlüğe girmiştir. Sözleşmenin resmi olarak Türkçe’ ye çevirisi ise “Sanal Ortamda İşlenen Suçlar Sözleşmesi” olarak yapılmıştır (Aliusta ve Benzer, 2018; Convention on Cybercrime, 2001).

Sözleşmede belirtilen temel amaçlar;

- Öncelikli olarak, uluslararası iş birliği teşvik edilerek, toplumu siber suçlara karşı korumaya yönelik ortak bir suç politikası izlenmesi ve uygun mevzuat geliştirilmesi,
- Bilgisayar ağlarının dijitalleşmesi ve küreleşmesinin yol açtığı değişikliklerin farkına vararak; bilgisayar ağlarının ve elektronik bilgilerin de cezai yaptırım uygulanması gereken suçların işlenmesi için kullanılabileceği ve bu tür suçlarla ilgili kanıtların bu ağlar tarafından saklanabileceği ve aktarılabileceği riskinin bilicinde devlet ve özel sektör arasında iş birliği çalışmalarının yapılması,
- Bilgisayar sistemlerinin, ağlarının ve bilgisayar verilerinin gizliliğine, bütünlüğüne ve kullanılabilirliğine yönelik saldırıların ve ayrıca bu tür sistemlerin, ağların ve verilerin kötüye kullanılmasına yönelik eylemlerin suç sayılarak, caydırmak ve etkin bir şekilde mücadele edebilmek için hem ulusal hem de uluslararası düzeyde tespiti, soruşturulması ve kovuşturulmasını kolaylaştırarak ve hızlı ve güvenilir uluslararası iş birliği için düzenlemeler sağlanması,

olarak sıralanabilir (Convention on Cybercrime, 2001).

Bilgi Güvenliği Derneği tarafından bir çalışma yapılarak, Haziran 2012'de Siber Güvenlik Strateji Çalıştayı'nda tavsiye belgesi yayınlanmış ve siber güvenlikle ilgili yapılması gerekenlere yer verilirken atılması gereken somut adımlar;

- Ulusal Siber Güvenlik Strateji Belgesinin yayınlanması
- Ulusal Siber Güvenlik Kurulu oluşturulması
- Siber güvenlik alanında farkındalığın arttırılmasına yönelik çalışmalar yapılması
- Siber güvenlik kültürünün yaygınlaştırılması
- Kişisel ve kurumsal verilerin korunması için daha sıkı tedbir alınması.
- Uluslararası iş birliğinin artırılması
- Ulusal siber güvenlik Ar-Ge politikasının oluşturulması ve milli teknolojilerin gelişmesinin desteklenmesi
- Üniversitelerin konu ile ilgili bilimsel araştırmalarının derinleşmesi ile ilgili çalışmalar yapılması
- Yeni insan kaynakları yetiştirilmesi ve hali hazırdakilerin geliştirilmesine yönelik çalışmalar yapılması

- Kurumsal siber güvenlik yeteneklerin artırılmasına yönelik ve kurumlara siber güvenlik sızma testleri yapacak bağımsız merkezlerin kurulması
- Yasal mevzuatın düzenlenmesi

şeklinde listelenmiştir (Ulusal Siber Güvenlik Stratejisi, 2012).

20 Haziran 2013 tarihinde Türkiye' de ilk kez "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı", 28683 sayılı Resmî Gazete' de yayımlanarak yürürlüğe girmiştir. 2 yıllık bu Eylem planı ile; siber güvenlik mevzuatının geliştirilmesi, kritik altyapıların güvenliğinin sağlanması, toplumda siber güvenlik farkındalığının oluşturulması, siber tehditlerin tespiti ve önlenmesi gibi alanlarda çalışmalar yürütülmüştür (Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, 2013).

Sonrasında yayımlanan Eylem Planı "2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı" ile de siber güvenlik risklerinin yönetilebilir ve daha az zararlı düzeyde tutulabilmesi için siber savunmanın güçlendirilmesi, kritik altyapıların korunması, siber suçlarla mücadele edilmesi, farkındalık ve insan kaynağı geliştirilmesi, siber güvenlik ekosisteminin geliştirilmesi ve siber güvenliğin milli güvenliğe entegrasyonu gibi alanlarda çalışmalar yürütülmüştür (Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, 2016).

Son dönemde ise ülkemizde siber güvenliğin sağlanması ile ilgili çalışmalar hızlanmış, riskleri en aza indirgeyerek, bu sürecin yönetilebilir ve kabul edilebilir düzeylerde tutulmasını hedeflenmektedir. Bu kapsamda, 5809 sayılı Elektronik Haberleşme Kanunu'nun 5'inci maddesinin birinci fıkrasının (h) bendi ile

> Ulusal siber güvenliğin sağlanması amacıyla politika, strateji ve hedefleri belirlemek, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilere yönelik siber güvenliğin sağlanmasına ilişkin usul ve esasları belirlemek, eylem planlarını hazırlamak, ilgili faaliyetlerin koordinasyonunu sağlamak, kritik altyapılar ile ait oldukları kurumları ve konumları belirlemek, gerekli müdahale merkezlerini kurmak, kurdurmak ve denetlemek, her türlü siber müdahale aracının ve millî çözümlerin üretilmesi ve geliştirilmesi amacı ile çalışmalar yapmak, yaptırmak ve bunları teşvik etmek ve siber güvenlik konusunda bilinçlendirme, eğitim ve farkındalığı artırma çalışmaları yürütmek, siber güvenlik alanında faaliyet gösteren gerçek ve tüzel kişilerin uyması gereken usul ve esasları hazırlamak

yetkisi, görev ve sorumlulukları Ulaştırma ve Altyapı Bakanlığı'na verilmiştir (Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, 2020).

10 Temmuz 2018 tarihli ve 30474 sayılı Resmî Gazete'de yayımlanan 1 no'lu Cumhurbaşkanlığı Kararnamesi ile kurulan Dijital Dönüşüm Ofisine (DDO) *"Bilgi güvenliğini ve siber güvenliği artırıcı projeler geliştirmek"* görevi verilmiştir. Bu çerçevede, 2019/12 sayılı Cumhurbaşkanlığı Genelgesi ile Bilgi ve İletişim Güvenliği Tedbirleri

yayımlanmıştır. 15 Ağustos 2016 tarihinde 5809 sayılı Elektronik Haberleşme Kanunu'na eklenen hükümler[1] ile BTK'ya siber saldırıların engellenmesi ve caydırıcılığın sağlanması görevleri ile bu görevler kapsamında yükümlülüklerini yerine getirmeyen ilgili taraflara yaptırım uygulama yetkisi verilmiştir (Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, 2020).

Güvenli bir siber uzay ortamının sağlanması ve sürdürülebilmesinin yolu teknoloji, insan ve süreç bileşenlerinin güvenliğine bağlıdır. Buna bağlı olarak hayatımızda yer alan teknolojilerin yanı sıra, yer alması öngörülen yeni teknolojiler de; yapay zekâ, nesnelerin interneti, blok zincir, 5G gibi, yakın gelecekteki siber güvenlik planlamalarında öncelikli olarak yer alacaktır (Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, 2020).

Kurumlar ve Kuruluşlar

Türkiye'de siber güvenlik ile ilgili çeşitli kurumlar ve kuruluşlar bulunmaktadır. Bunlar aşağıda kısaca açıklanmaktadır.

Bilgi Teknolojileri ve İletişim Kurumu (BTK)

27 Ocak 2000 yılında Telsiz Kanunu'nda yapılan değişiklikle Telekomünikasyon Kurumu kurulmuştur. 10 Kasım 2008 yılında ise, Elektronik Haberleşme Kanunu ile kurumun adı Bilgi Teknolojileri ve İletişim Kurumu olarak değiştirilmiştir. Bilgi Teknolojileri ve İletişim Kurumu (BTK), telekomünikasyon sektörünü düzenleyip denetleyen bu anlamda Türkiye'nin ilk kurumudur (BTK, 2020).

Telekomünikasyon alanında; "yetkilendirme, denetleme, ihtilaf çözümü, tüketici haklarının korunması, sektör rekabetinin düzenlenmesi, teknik yönergeler yayınlamak ve spektrum yönetimi ve izlenmesinden" sorumludur. Aynı zamanda bilgi teknolojileri konusunda otoritedir ve Telekomünikasyon İletişim Başkanlığı (TİB) aracılığıyla bu konudaki görevleri gerçekleştirmektedir (Bıçakcı, vd., 2015).

Telekomünikasyon İletişim Başkanlığı (TİB)

TİB, 2005 yılında bünyesinde çalışanlara ek olarak "Milli İstihbarat Teşkilatı Müsteşarlığı", "Emniyet Genel Müdürlüğü" ve "Jandarma Genel Komutanlığı'nın" ilgili

birimlerinden birer temsilci barındırmak üzere, yürütülen çalışmalarla ilgili doğrudan BTK Başkanı'na rapor vermek üzere kurulmuştur (Bıçakcı, vd., 2015).

TİB çoğunlukla internet hizmetleri de dahil olmak üzere telekomünikasyon ürünleri aracılığıyla gerçekleşen iletişimin ve sinyal bilgisinin denetimi ve kaydedilmesinden sorumlu olmuştur. Bunun yanı sıra internet hizmetlerinin "emniyet" tarafıyla "içerik sağlayıcı", "yer sağlayıcı", "erişim sağlayıcı" ve "toplu kullanım sağlayıcılarının" kontrol edilmesiyle de ilgilenmiştir. Bu sebeple TİB internette uygulanan erişim engelleri ve kullanıcı gizliliği/ağ takibi gibi konuların muhatabı konumundaki kurum olmuştur. Aynı zamanda internet üzerinde yapılan işlemlerin izlenmesi, takip edilmesi, perdelenmesi ve filtrelenmesi üzere geliştirilmesi gereken yazılım ve donanımlara ilişkin asgari kriterleri belirlemekle görevli olmuştur (Bıçakcı vd., 2015; İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, 2007). 2015 yılında yapılan değişikliklerle TİB içeriğe ve internet sayfalarına hızlı bir biçimde erişebilme yetkisi elde etmiş ve kararlarına uyulması konusunda hukuki caydırıcılara sahip olmuştur (Bıçakcı vd., 2015). Ağustos 2016'da 671 sayılı Kanun Hükmünde Kararname ile Olağanüstü hal kapsamında bazı kurum ve kuruluşlara ilişkin düzenleme yapılmış, Telekomünikasyon İletişim Başkanlığı kapatılmıştır. Yetkileri ise Bilgi Teknolojileri ve İletişim Kurumuna devredilmiştir (KHK, 2016).

Siber Suçlarla Mücadele Daire Başkanlığı

Bilişim teknolojileri kullanılarak işlenen suçların soruşturulması ve dijital delillerin incelenmesi için destek veren görevli Daire Başkanlıkları il birimlerinin dağınık yapısının tek bir çatı altında toplanması ve siber suçlarla etkin bir şekilde mücadele edilebilmesi amacıyla 2011 yılında 2025 sayılı Bakanlar Kurulu Kararı ile Emniyet Genel Müdürlüğü bünyesinde Bilişim Suçlarıyla Mücadele Daire Başkanlığı kurulmuş, Şubat 2013'te ise ismi Siber Suçlarla Mücadele Daire Başkanlığı olarak değiştirilmiştir. Siber Suçlarla Mücadele Daire Başkanlığı vizyonunu aşağıdaki gibi sıralamıştır (EGM, 2021).;

- Siber suçlarla mücadele etmek,
- Siber suçlar konusunda toplumda farkındalık oluşturmak,
- Siber suçlarla mücadelede uluslararası işbirliklerini artırmak,

- Ülkemize yönelik siber suç tehditlerini değerlendirmek, gerekli analizler yapmak ve bu tehditlerle mücadele etmek,
- Siber suçlarla mücadelede alanında uzman soruşturmacı ve adli bilişim personelleri yetiştirmek,
- Teknolojik gelişmeleri takip etmek ve bu teknolojiyi kullanmak suretiyle siber suçlarla mücadele kapasitemizi artırmak.

Siber Güvenlik Kurulu

Haziran 2012'de gerçekleşen Siber Güvenlik Strateji Çalıştayı'nda atılması gereken somut adımlar listesinde yer alan Ulusal Siber Güvenlik Kurulu Oluşturulması, 20 Ekim 2012 Bakanlar Kurulu'nun 2012/3842 sayılı kararı ile gerçekleşmiş, Siber Güvenlik Kurulu oluşturulmuştur. Bakanlar Kurulu'nun aldığı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar Madde 4'te Siber Güvenlik Kurumu'nun; "siber güvenlikle ilgili olarak alınacak önlemleri belirlemek, hazırlanan plan, program, rapor, usul, esas ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak amacıyla" kurulduğunu açıklamıştır (Bakanlar Kurulu Kararı, 2012). Ulaştırma, Denizcilik ve Haberleşme Bakanı başkanlığını üstlenmiş, "Dışişleri", "İçişleri", "Milli Savunma", "Ulaştırma, Denizcilik ve Haberleşme Bakanı müsteşarları", "Kamu Düzeni ve Güvenliği Müsteşarı", "Milli İstihbarat Teşkilatı Müsteşarı", "Genelkurmay Başkanlığı Muhabere Elektronik ve Bilgi Sistemleri Başkanı", "BTK Başkanı", "TÜBİTAK Başkanı", "Mali Suçları Araştırma Kurulu Başkanı", "Telekomünikasyon İletişim Başkanı ve UDH" tarafından, bakanlık ve kamu kurumlarında çalışan üst düzey yöneticilerden, kurul oluşturulmuştur (Bakanlar Kurulu Kararı, 2012). T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı koordinatör kurum olarak tanımlanmıştır (On Birinci Kalkınma Planı, 2018).

Ulusal Siber Olaylara Müdahale Merkezi (USOM)

Siber Güvenlik Kurulu bir sonraki yıl Türkiye'nin birinci Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nı yayınlamıştır. Aynı yıl plan 25 Mart 2013'te 4890 sayılı Bakanlar Kurulu Kararı ile yürürlüğe girmiştir. Eylem planında kritik altyapılara yer verilerek şu şekilde açıklanmıştır:

İşlediği bilginin, gizlilik, bütünlük ve erişilebilirlik özellikleri zarar gördüğünde;

- Can kaybı olmasına,
- Büyük ölçüde ekonomik zararın ortaya çıkmasına,
- Ulusal güvenlik açıklarına veya toplum düzeninin bozulmasına,

neden olabilecek bilişim sistemlerini içine alan altyapıları ifade etmektedir (Uluslararası Siber Güvenlik Stratejisi ve Eylem Planı, 2013).

20213-2014 Eylem Planında, ulusal tehdit ve tehlikelere karşı günün her saatinde müdahale edebilecek Ulusal Siber Olaylara Müdahale Merkezi (USOM) kurularak, USOM'un koordinasyonunda çalışacak sektörel Siber Olaylara Müdahale Ekipleri (SOME) oluşturulacağı yer almıştır. USOM ve SOME'ler görevlerini yerine getirirken ihtiyaç halinde gerekli verileri elde edebilmek amacıyla adli makam ve kolluk birimleri ile koordineli hareket edecekleri belirtilmiştir. USOM'nin uluslararası kuruluşlarla da yakın iş birliği yapması gerektiğine değinilmiştir. 2013-2014 Eylem Planı sayesinde; siber ortamlarda meydana gelen tehlikeler belirlemesi, yaşanabilecek zararların en aza indirgenmesi ve yok edilmesi için önlemlerin geliştirilmesi ve paylaşılması için ulusal düzeyde etkin bir şekilde çalışarak kurum ve kuruluşların siber güvenliklerini sağlaması görevleriyle Siber Olaylara Müdahale Organizasyonu oluşturulmuştur (Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, 2013)

2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı doğrultusunda yapılan çalışmalar çerçevesinde son dönemde;

- Ulusal siber güvenlik kapasite inşası programı kapsamında SOME'lerin insan kaynağının iyileştirip geliştirilmesi ve siber olaylara hazırlık seviyesinin artırılması, ulusal ihtiyaca yönelik insan kaynağının yetiştirilmesine yönelik olarak eğitim, kamp ve yarışma gibi faaliyetler,
- Teknolojik önlemler programı kapsamında, yapay zekâ ve makine öğrenimi gibi teknolojilerden yararlanan AVCI, AZAD ve KASIRGA gibi hızlı tespit ve erken müdahale sistemlerinin geliştirilmesi,
- Tehdit istihbaratı edinimi, üretimi ve paylaşımı programı kapsamında hem ulusal hem uluslararası paydaşlarla çift taraflı yürütülen bilgi paylaşımı ve koordinasyon çalışmaları
- Kritik altyapıların korunması programı kapsamında ise kritik altyapıların hizmet sürekliliğinin takibine yönelik izleme faaliyetleri, zafiyet tarama çalışmaları ve bilgi güvenliği ile ilgili düzenleme ve denetleme çalışmaları yürütülmüştür.

Yürütülen bütün bu yenilikler ve çalışmaların neticesinde, Uluslararası Telekomünikasyon Birliği Global Siber Güvenlik Endeksi'nin 2019'da yayımladığı sonuçları ile 2018 yılında ülkemiz bir önceki yıla göre 23 sıra yükselmiş, dünyada 20'nci sırada, Avrupa'da 11'inci sırada yer almıştır (Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, 2020).

Öğretmenler ve Siber Güvenlik

Siber güvenliğin birbirini etkileyen, içinde insan faktörünün de yer aldığı birçok paydaştan oluşan bütüncül yapıda bir sistem olduğu anlaşılmaktadır. İnsan faktörü yer aldığı birçok sistem gibi bu alanda de en zayıf dişli olarak görülmektedir. Siber güvenlik düzeyini üst noktalara taşımak için güvenlik sistemlerine yapılan yatırımlar ve alınan önlemler kadar insanların bilinçlenmesi ve farkındalık düzeylerinin artırılması da önemli görülmektedir (Yayla, 2018; Şahinaslan, Kantürk, Şahinaslan ve Borandağ, 2009).

Tüm dünyada internet ve bilgi iletişim teknolojilerinin kullanımı artarken kullanan yaşı da gittikçe küçülmektedir (Teker, 2019). Çocukların teknoloji ile tanışma yaşları düşünüldüğünde çeşitli risk ve tehditlerin farkında olmaları için yapılacak çalışmaların ilkokuldan döneminden itibaren başlatılması gerektiği düşünülmektedir (Güldüren ve Keser, 2017). Buradan yola çıkarak toplumda siber güvenlik farkındalığının sistemli bir biçimde kazandırılması için başlangıç noktasının okul çağındaki 6-18 yaş grubu çocuklardan oluşmasının gerekli olduğu söylenebilir. Erken yaşlardan itibaren farkındalık ve bilincin oluşmasını sağlamak toplumu oluşturan tüm bireylerin siber güvenlik alanında daha duyarlı olması anlamına gelmektedir. Çocukların bu bilinç ve farkındalığı kazanması için onlara konu ile ilgili eğitimleri verecek ve eğitim sistemi içerisinde davranışlarıyla rol model olacak öğretmenlerin siber güvenlik farkındalığının yüksek olması önem taşımaktadır. Öğrenciler, özellikle ödevlerini yerine getirirken, oyun oynarken, sosyalleşirken yani günlük hayatlarının birçok alanında bilgi iletişim teknolojilerini ve interneti sıklıkla kullanarak siber tehditlerle her an karşılaşabilecek ortamlarda bulunmaları büyük risk teşkil etmektedir. Bu tehditler ile öğrenciler arasında kilit görevi gören öğretmenlerin siber güvenlik risklerine karşı farkında olması öğrencilerini bu doğrultuda bilinçlendirebilmesi açısından büyük önem taşımaktadır. Bu sebeple öncelikle öğretmenlerin siber güvenlik farkındalık düzeyleri belirlenerek hangi eğitimlere ihtiyaç duydukları tespit edilmeli ve öğrencileri yetiştirecek öğretmenlerin farkındalık düzeyleri artırılmalıdır (Yayla, 2018).

Buradan hareketle MEB'in geçmişten günümüze bilişim teknolojileri ile ilgili öğretmenlere verdiği eğitimler araştırılmıştır. 2001-2011 yılları arasındaki Hizmet İçi Eğitim Planları incelendiğinde bilgi ve iletişim teknolojileri alanında öğretmenlere yönelik seminer ve kursların sayısı çok fazla olmasa da çeşitli eğitimlerin verildiği görülmektedir. Bu eğitimler incelendiğinde genellikle Bilişim Teknolojileri ve Formatör öğretmenlere yönelik olduğu anlaşılmaktadır (MEBb, 2021). Verilen eğitimler başlıca;

- Eğitimde bilgi iletişim teknolojileri kullanımına yönelik,
- Bilgisayar ağ sistemlerine yönelik,
- Programlama dillerine yönelik,
- Web tasarımına yönelik,
- Office programlarına yönelik,
- Grafik tasarımına yönelik,
- İşletim sistemlerine yönelik

olarak sınıflandırılabilir.

Ancak, 2012-2021 yılları arasındaki Öğretmenlerin Hizmet İçi Eğitim Planları incelendiğinde bilgi ve iletişim teknolojileri alanında verilen eğitimlerin Fatih Projesi'nin de pilot olarak uygulanmaya başlanmasıyla birlikte sayı, çeşitlilik ve farklı branşlardaki öğretmenlere ulaşma anlamında hız kazandığını söylemek mümkündür (MEBb, 2021). Önceki yıllardan devam eden eğitimlerin yanı sıra yeni eklenen eğitimler başlıca;

- Fatih projesi kapsamında BT'nin ve internetin bilinçli ve güvenli kullanımına yönelik,
- E-içeriklerin eğitime dahil edilmesine yönelik,
- Android Programlamaya yönelik,
- 3D Yazıcı ile Tasarım ve Üretime yönelik,
- Temel Robotik alanına yönelik,
- STEM'e yönelik,
- Temel Kodlamaya yönelik,
- Arduino uygulamalarına yönelik,
- Algoritmik ve bilgi işlemsel düşünmeye yönelik,
- Dijital girişimciliğe yönelik,
- Siber güvenlik, büyük veri, yapay zeka ve nesnelerin internetine yönelik

olarak sınıflandırılabilir.

Dünyada bilgi iletişim teknolojileri ve internet ile ilgili yaşanan gelişmeler eğitimde değişimi ve gelişimi zorunlu hale getirmektedir. Özellikle son yıllarda birçok ülke eğitim sisteminde bilgi ve iletişim teknolojilerinin güvenli kullanımı doğrultusunda öğretmenlerin bilgi ve beceri düzeylerini artırarak bir standart oluşturma konusunda çalışmakta yeni politikalar ve uygulamaları öğrenme-öğretme sürecine dahil etmektedirler (Özden, 2005).

2.2. İlgili Araştırmalar

Siber güvenlik, günümüz dünyasının hemen her aşamasında, toplumdaki bütün bireyleri ilgilendiren bir kavramdır. Özellikle insan unsurunun siber güvenliğin önemli bir parçası olduğunu söylemek mümkündür. Tüm toplumlar için hayati önem taşıyan siber güvenlik sorunlarının, bireylere yönelik eğitim, bilinçlendirme ve farkındalık çalışmalarıyla ilişkili olduğu anlaşılmaktadır. Bu kapsamda literatür taranarak siber güvenlik ve siber güvenlik farkındalığına yönelik yapılan çalışmalar incelenmiştir. Bu bölümde incelenen bazı çalışmalar özetlenmiştir.

Pusey ve Sadera (2011) öğretmen adayları öğretmen eğitimi programlarında eğitim içeriklerine bilgisayar ve interneti ve teknolojiyi entegre etme yöntemlerini öğrenildiğini, ancak öğretmen adaylarının bu cihazlarla çalışırken güvenlik konularında yetkin olduklarının varsayıldığını belirtmişlerdir. Buradan yola çıkarak yaptıkları çalışmada, öğretmen adaylarının C3 olarak da bilinen; siber etik, siber güvenlik (safety) ve siber güvenlik (security) konularında ne kadar bilgi sahibi oldukları, anlayışları ve bunları öğretme yeteneklerine ilişkin inançları araştırılmıştır. Araştırmacılar, 318 öğretmen adayına ulaşarak hazırladıkları 75 C3 konusundan oluşan anket ile adayların, modelleme veya öğretme yeteneklerini değerlendirmek istemişlerdir. Öğretmen adaylarının gelecekteki öğretimlerinde C3 içeriği hakkındaki bilgileri ve öğretmeye hazır olma durumları hakkında veri toplamak için tasarlanmış ankete dayalı bu çalışmanın sonuçları; katılımcıların C3 konularını modellemeye veya öğretmeye hazır olmadığını göstermiştir. Araştırmada, öğretmen adaylarını C3'ü gelecekteki öğretimlerine entegre etmeye daha iyi hazırlamak için müfredatlarında bu konuları ele almak için stratejiler geliştirmede öğretmen hazırlık programlarına yardımcı olacaktır önerisi yapılmıştır.

Ünver'in (2012) Ulusal Siber Güvenliğin Sağlanmasında Farkındalık Çalışmaları isimli araştırmasında, bireylerin bilgi güvenliği farkındalığı üzerinde yoğunlaşarak, farkındalık kapsamında yapılabilecek çalışmaları yedi başlık altında; Eğitim, Tatbikatlar,

Bilgilendirme Siteleri, Etkinlikler, Yayınlar ve Diğer olarak ele almıştır. Çalışmada öneri olarak, tüm vatandaşlara eğitimler verilerek "Siber Vatandaş" bilinci oluşturulması gerektiği, "Siber Güvenlik Ayı" belirlenmesi gerektiği, ulusal seviyede tatbikatlar yapılması gerektiği, bilgi güvenliği farkındalığı ölçümü yapılması gerektiği ve tüm önerilerin "Ulusal Farkındalık Programı" çerçevesinde bütüncül bir yaklaşımla uygulanması gerektiği geliştirmiştir.

Akın, Çınar, Karaman ve Bilekyiğit'in (2013) "Siber Durum Farkındalığını Artırmada Etkili Bir Yöntem: Bayrağı Yakala (Capture the Flag)" isimli çalışmalarında, amacın "savunmaya yönelik farkındalık oluşturmak" olduğu katılımcılara belirtilmiştir. Yarışmanın hazırlanması ve uygulanması "prosedürel konular" ve "teknik konular" iki aşamada toplanmıştır. Prosedürel konular ile ilgili aşamada, "yarışmanın nasıl yapılması gerektiği, süresi, kullanılacak platform ve donanım" ve buna benzer durumlara yönelinmiş; teknik konular ile ilgili bölümde yarışmada geçen "sorular ve çözümler" detaylı bir biçimde ele alınmıştır. Çalışmada "siber durum farkındalığını artırmaya yönelik bayrağı yakala (BY) yarışması" kurum için farkındalık çalışması olarak personellere uygulanmıştır. Uygulanan yarışmanın etkililiği ise anket düzenlenerek belirlenmiştir. Araştırmanın değerlendirme bölümünde; kullanıcılara "yarışmadan önce ve sonra siber güvenlik alanında kendilerine güvenlerinin nasıl olduğu" sorulmuş, katılımcılar" ortalama olarak %50 oranında güvenlerinin arttığını" ifade etmişlerdir. Katılımcılara, buna benzer bir yarışma yapılsa "tekrar katılmak ister misiniz ya da yarışmanın hazırlanması aşamalarında yer almak ister misiniz" diye sorulmuş, hepsinin cevabı "Evet" olmuştur. Yarışmanın siber güvenlik farkındalığını nasıl etkilediği ile ilgili soruya ise "çok iyi" cevabı alındığı bilgilerine yer verilmiştir. Araştırmanın sonuçları, siber güvenlik konusu ile ilgili görevli olan ve herhangi bir sisteme zarar verme ihtimali olmayan kişilere yönelik yapılacak olan "bayrağı yakalama yarışmaları" sayesinde bu konudaki bilgi ve farkındalık düzeyinin artırılabileceğini göstermiştir. Aynı zamanda siber güvenlik ile ilgili bir görevi olsa dahi çalışanların, öğrendikleri kavramsal bilgilerden daha çok tecrübe ettikleri durumlarda farkındalık düzeylerinin arttığı sonucuna ulaşılmıştır.

Göztepe, Kılıç ve Kayaalp (2014) "Derinliğine Siber Güvenlik: Türkiye Siber Güvenlik Ajansı Organizasyonu Tasarımı" araştırmasında, mobil cihaz kullanımının yaygınlaşması ve "nesnelerin interneti" uygulanmaya başlanmasıyla, insanoğlunun gerçek dünyanın yanında aynı zamanda bir "siber-dünyada" yaşamaya başladığı, siber uzayın ansızın genişlemesiyle birçok siber saldırıya karşı korunmasız kaldığı

belirtilmiştir. Siber saldırganların ve siber saldırıların gün geçtikçe fazlalaşmasına rağmen saldırganların bu konudaki bilgilerinin azaldığı bu ters orantının, kurum, kuruluş ve hükumetleri, siber tehditlere karşı daha kapsamlı güvenlik önlemleri almaya zorladığı ifade edilmiştir. Gelişmiş ülkelerin "kara", "deniz", "hava" ve "uzaydan" sonra siber uzayı "beşinci operasyonel etki alanı" olarak görmeye başladığı vurgulanmıştır. Türkiye için "siber güvenlik ajansı tasarımının", siber güvenlik bazında ülke güvenliğinin sağlanması adına "derinlemesine siber savunmanın" çok önemli bir durum olduğu ifade edilmiştir. Çalışmada, güçlü bir siber savunma elde etmek için en önemli adım olan, bir strateji ve uygun bir siber savunma yapısı ortaya koymak üzere Türkiye "siber güvenlik ajansı kurumu için sekiz katmanlı derinliğine savunma mimarisi" önerilmiş, bu mimarinin, kurum ve kuruluşlar için çok faydalı ve anlık bilgi paylaşımı sağlayacağı belirtilmiştir. Ayrıca, bileşenleri ile birlikte siber güvenlik ajansı organizasyon tasarımı da sunulmuştur. Çalışmada sunulan çerçeve, siber savunma stratejisini bir savunma mimarisi olarak değil, üç ana merkez; siber savunma koordinasyon merkezi, siber teknolojiler araştırma merkezi ve siber operasyon merkezi tarafından çok boyutlu bir organizasyon olarak görmüştür. **S**iber savaşla mücadele eden bir alan olmadan bir devletin kendi güvenliğini sağlayamayacağı ifade edilmiştir.

Yılmaz (2015) siber güvenliğin oluşmasında "yazılım ve kalite süreçlerini" incelediği tez çalışmasında, "siber güvenlik kavramları, güvenli yazılım geliştirme modelleri ile yazılım kalite kriterleri" araştırılmıştır. Çalışmada, "Türkiye'de kamu kurum ve kuruluşları ile özel sektör firmalarında siber güvenlikte yazılım kalite kriterlerinin önemine yönelik farkındalık düzeyi" ortaya konulmaya çalışılmıştır. Türkiye'de yazılımların kalitesi ile ilgili ilerleyen durumları, siber güvenlik için belirlenen kriterlere göre ortaya koymak üzere hazırlanan anket kullanılmış ve farkındalık durumunu ölçmek hedeflenmiştir. Siber güvenlikle ilgili Türkiye'deki durumu ortaya koymaya çalışan anket sonuçları; bilgi güvenliği ve güvenli bilgisayar programları üretme ile ilgili eğitimlerin gerekli görüldüğü, uygulamaların "güvenli yazılım geliştirme yaşam modelleri" ile üretilmeye uğraşıldığı, "risk analizi ve risk azaltma yöntemleri ile tehdit modellemenin" ehemmiyetinin bilincinde olunduğunu göstermiştir. Ancak, bu bilincin göstergesi niteliğindeki sertifikaların kurumlar tarafından kullanılma yüzdesinin oldukça az olduğu fark edilmiştir. Bunun sonucunda "kalite bilincinin yeterince oluşmadığı", sonucuna ulaşılarak, kurumlarda dünya çapında kurumsal bir oluşumun gerçekleşmesi ile ilgili yetersizliklerin var olduğu görülmüştür. Çalışmada, siber güvenlik bilinci yüksek çıkmasına karşın beklenen seviyeye yükselmediği ve siber güvenlik ile ilgili boyutların

içselleştirilmediği ifade edilmiştir. Buradan hareketle yazılımların çok sık saldırıya maruz kalan "siber unsur" olduğu farkındalığının geliştirilmesine gerek olduğu görülmüştür.

Erol'un (2016), yetenek tabanlı model geliştirerek siber güvenlik farkındalığını belirlemek üzere gerçekleştirdiği yüksek lisans tez çalışmasında, siber güvenlik farkındalığı konusunda insan faktörünün önemi belirtilerek, bu farkındalığı yetersiz ve ya hiç gelişmemiş olan olmayan ya da yetersiz olan kişilerin kullandığı sistemler veya cihazlara kolay bir şekilde üstelik az bir mali giderle erişilebildiği ifade edilmiştir. Etkili bir bilgi güvenliğinden söz edebilmek için farkındalık konusu "bir çözüm" olarak değil, "bir problem" olarak ele alınmış, bu konudaki sorunların bilgi güvenliği ile ilgili farkındalığın ne kadar yeterli olduğunun belirlenmesi ve de çıkan sonuçlara göre farkındalık düzeyinin artırılması ile ortadan kalkabileceği "bilgi güvenliği farkındalık yeterlilik seviyesinin" ölçülmesi ve elde edilen sonuçlarla birlikte "farkındalık seviyesinin arttırılması" ile giderilebileceği belirtilmiştir. Araştırmada, ilk defa farkındalığın düzeyinin yeterli olup olmadığını belirlemek üzere "yetenek tabanlı dinamik bir model" ortaya konulmuştur. Geliştirilen modelin başarım ölçütleri tespit edilerek doğrulanma yapılabilmesi için "www.guvenlikicinbirdakika.org" sitesi kurulmuş örnek bir çalışma gerçekleştirilmiştir. Sosyal sorumluluk projesi ile "Gazi Üniversitesi Bilgi Güvenliği Mühendisliği Ana Bilim Dalı öğrencileri" siber güvenlik farkındalığına yönelik kullanıcıların bilgilendirilmesi için "röportajlar, videolar, güncel saldırılara yönelik bilgilendirmeler, bilgi güvenliği konferansları etkinliklerin duyurulması" vb. içerikler yer alacak biçimde hazırlanan bu örnek çalışma kullanıma açılarak durum değerlendirmeleri gerçekleştirilmiş ve farkındalığın artırılabilmesi için siber saldırılara karşı fikir önerileri sunulmuştur. Ancak, bireylerin davranışları ile farkındalık seviyeleri arasında daima tutarlılık göstermediği, farkındalığı gelişmiş olsa bile bireylerin bu farkındalıklarını davranışa dönüştürmedikleri durumda bilgi güvenliğinin bozulduğu ortaya çıkmıştır. Farkındalık olsa da bunların davranışa dönüşmesi ile ilgili kritik olan parametreler ortaya konulmuş ve bu parametrelerin birbiri ile ilgisi araştırılmıştır. Araştırmada, farkındalığın tespit edilebilmesi ve düzenlenebilmesi için bilgi güvenliğinin oluşması ve devam ettirebilmesini sağlayacak sistemli ve düzenli bir yaklaşım şeklinde ortaya konulan bu modelin siber güvenlik farkındalığının arttırılması yönünde olumlu etkileri olacağı sonucuna ulaşılmıştır.

Bulu, Kavuk ve Keser (2017) bilgi ve iletişim teknolojileri öğretmen adaylarının çevrimiçi tehditlere yönelik hazır bulunuşluk düzeylerini belirlemeyi amaçladıkları, Hizmet Öncesi BİT Öğretmenlerinin Okul İnternet Güvenliğine Yönelik Önerileri adlı

çalışmalarında öğrencilerin interneti sorumluluklarını bilerek kullanması gerektiğini bunda da öğretmenler ve okul bilgi teknolojileri uzmanlarının rolleri olduğunu belirtmişlerdir. Çalışmada bilgi ve iletişim teknolojileri öğretmen adaylarına benzersiz bir gerçekçi problem verilmiş ve çözüm stratejileri sorulmuştur. Bilgi ve iletişim teknolojileri öğretmen adaylarının çözüm stratejileri ve önerdikleri etkinlikler içerik analizi yöntemi kullanılarak analiz edilmiştir. Analizden; eğitim, teknik çözümler, rehberlik, veliler, sorun tanımları, engeller, etkinlikler ve iş birliği olmak üzere sekiz kategori ortaya çıkartmışlardır. Araştırmanın sonuçlarında, öğretmen adaylarının çoğunun hazır bulunuşluk düzeylerinin istendiği seviyede olmadığı, internet güvenliği için eğitim ve öğretimin önemini bilmelerine rağmen, internet güvenliğinin eğitim müfredatına entegre edilmesinin önemini vurgulayamadıkları ve de öğrencilerinin internet güvenliği konusunda sorumluluklarını almaya istekli görünmedikleri bilgilerine ulaşılmıştır.

Subramaniam (2017) yaptığı bu çalışmada, Malezya yarımadasının kuzey bölgesinde yer alan bir üniversitedeki öğrencilerin siber güvenlik farkındalık düzeylerini araştırmıştır. Araştırmanın yapılmasına zemin hazırlayan etmenleri; öğrencilerin yoğun biçimde bilgisayar kullanmasıyla birlikte tehlikelerle yüz yüze olmaları ve eğitimlerini tamamladıktan sonra meslek hayatlarına başlayacakları için siber güvenlik bilincinin şu anda kazandırılması gerektiği, olarak açıklamıştır. Literatürdeki diğer anketlerden uyarlanan Siber Güvenlik Farkındalık Düzeyi anketi toplam 318 öğrenciye uygulanmıştır. Tüm derslerden katılımcı olarak almak amacıyla tabakalı örnekleme kullanılmıştır. Araştırma bulguları, öğrencilerin farkındalıklarının ortalama düzeyde olduğunu, kız ve erkek öğrenciler arasında siber güvenlik farkındalık düzeyinde bir fark olmadığını göstermiştir. Çalışma ayrıca, bilgisayar kullanımının öğrencilerin siber güvenlik farkındalık düzeylerine katkı sağlamadığını ortaya koymuştur. Ayrıca, farklı derslerden gelen öğrenciler arasında farklı seviyelerde siber güvenlik farkındalığı bulunduğunu ve daha iyi bilgi işlem becerilerine sahip öğrencilerin daha iyi siber güvenlik farkındalık seviyelerine sahip olduğu ortaya çıkmıştır. Araştırmada, üniversite öncesi kurumlarda siber güvenlik sorunlarını ele alan pratik çözüm önerileri sunulmuştur. Tüm birinci sınıf öğrencilerine üniversite öncesi ders kayıtlarının ilk haftasında siber güvenlik farkındalık programı yapılabilir, Üniversite öncesi kurumlarda ara sıra siber farkındalık programı yaptırılarak tüm derslerden öğrenciler faydalanabilir, farkındalık programı siber güvenlik yasalarını, risk ve önleme yöntemlerini içermelidir, eğitmen ve yöneticiler de genç neslin dijital çağ savaşını donatmalarına ve bunlarla mücadele etmelerine yardımcı olmak için

eğitim almalıdır önerileri yapılmıştır. Siber suçlarla ilgili daha fazla araştırma ve deney yapılması şiddetle tavsiye edilmiştir.

Semerci (2019a) eğitim fakültelerinde öğrenim gören öğrenciler ile farklı fakültelerde öğrenim gören öğrencilerin siber güvenlik farkındalıklarını karşılaştırmıştır. Siber uzaydaki kullanıcıların, siber güvenlik farkındalıklarının yetersiz durumda olması fazlaca zarar gördüklerini, bu yüzden tüm bireyler için kritik bir önemi olduğunu, ancak öğretmenlerin bu konudaki üstlenmeleri gereken sorumluluklarının çok daha fazla olduğunu belirtmiştir. Çalışmada "öğretmen adayı eğitim fakültesi öğrencilerinin siber güvenlik farkındalık düzeylerinin diğer fakülte öğrencilerinin farkındalık düzeyleriyle" karşılaştırılmış ve birçok farklı değişken açısından incelenmiştir. Çalışma, tarama modelinde gerçekleştirilmiş olup, çalışma grubunu ise üç tane devlet üniversitesinden toplam 448 öğrenci olarak belirlenmiştir. Verilerin toplanmasında *"Kişisel Siber Güvenliği Sağlama Ölçeği"* ve anket form kullanılmıştır. Çalışmanın bulgular kısmı incelendiğinde, öğrencilerin kişisel siber güvenlik farkındalık düzeylerinin orta ve üzeri olduğu, eğitim fakültesinde öğrenim gören öğrencilerin siber güvenlik farkındalık düzeyleri ile farklı fakültelerdeki öğrenim gören öğrencilerin farkındalık düzeyleri ve cinsiyetleri arasında anlamlı bir farklılık bulunmamıştır. Katılımcıların siber güvenlik farkındalıkları "sınıf düzeyi" ve "günlük internet kullanım süreleri" bazında incelendiğinde farklı etki düzeylerinde anlamlı farklılık bulunduğu sonucuna ulaşılmıştır.

Semerci'nin (2019b) üniversitede öğrenim gören öğrencilerinin, kişisel siber güvenliği sağlama davranışları ile "cinsiyet", "sınıf düzeyi", "günlük akıllı telefon kullanım süreleri", "bilgisayar ve internet kullanma becerileri" arasındaki ilişkiye baktığı, "Üniversite Öğrencilerinin Kişisel Siber Güvenlik Davranışlarının Farklı Değişkenler Açısından İncelenmesi" isimli çalışmasında, ilişkisel tarama modeli kullanılmıştır. Araştırmanın örneklemi ise üniversitede öğrenim gören 196 kişiden oluşmuştur. *"Kişisel Siber Güvenliği Sağlama Ölçeği"* ve cinsiyet, sınıf düzeyi gibi verilerin toplanmasında geliştirilen anket formu kullanılmıştır. Çalışmaya, %63.3' oranında kadın, %36.7 oranında erkek öğrenci katılmış, yaş ortalamaları 22 olarak çıkmıştır. Katılımcıların bir günde ortalama internet kullanma süreleri neredeyse 5 saat, büyük bir kısmının da internete bağlanmak için cep telefonlarını kullandıkları belirlenmiştir. Araştırma sonuçları incelendiğinde, katılımcıların kişisel siber güvenliği sağlamaya yönelik davranışlarının orta düzeyde olduğu görülmüştür. Öğrencilerin kişisel siber güvenlik sağlama davranış düzeyi ile "cinsiyet" ve "bir günde kullandıkları internet süreleri" arasında anlamlı farklılık olduğu gözlenirken, "sınıf düzeyi", "bilgisayar kullanma" ve

“internet kullanma becerileri” arasında ise anlamlı bir farklılık gözlenmediği bulgusuna ulaşılmıştır. Bulgular ve sonuçlar doğrultusunda öğrencilerin kişisel siber güvenlik farkındalık düzeylerinin arttırılmasına için öneriler geliştirilmiştir.

Selimoğlu ve Altunel’in (2019) “Siber Güvenlik Risklerinden Korunmada Köprü ve Katalizör Olarak İç Denetim” isimli çalışmalarında, iş ortamlarında hem kamu hem de özel sektörde büyük oranda dijital alt yapı kullanıldığı için bilginin depolanması, raporlanması gibi işlemlerin elektronik ortamda gerçekleştiği belirtilmiştir. Bu dijital alt yapı faydalı olduğu kadar büyük tehdit ve riskleri de beraberinde getirdiği, hem “özel sektörde” hem de “kamu sektöründe” siber saldırılara yönelik önlemlerin alınması ve risklerinin azaltılmasının önemli olduğu belirtilmiştir. Bu kapsamda “üçlü savunma hattının” siber riskleri kapsayacak şekilde geliştirilmesi ve kurum içinde siber risklere ve tehditlere yönelik çalışmalar gerçekleştirilmesi siber güvenlik tehlikelerinin ve yol açacağı risklerin en aza indirgenmesinde etkili olacağı görüşünden yola çıkılmıştır. Bunun için ilk olarak kurumda farkındalık düzeyinin artırılabilmesi için bir taraftan kurumda, diğer taraftan kurum dışında ilgili kişilere “siber güvenlik riski” konusunda eğitimler, programlar düzenlenmesi gerektiği belirtilmiştir. Farkındalığın oluşmasının ardından risklerin yönetilmesinde kullanılan, “üçlü savunma hattı modeli” oluşturulmalı, bu doğrultuda kurumların, “birinci savunma hattında” siber güvenlikle ilgili görevleri olan kişilerin ve kontrol faaliyetlerin ele alınması gerektiği bilgisi verilmiştir. “İkinci savunma hattı”, risklerin değerlendirilmesi, risklerin kurum standardına uygun olup olmadığının takip edilmesi, risklerin değerlendirmeleri ile ilgili yapılan değişikliklerin izlenmesi, risklerin en aza indirgenmesi konusunda “birinci savunma hattıyla” birlikte hareket edilmesi gerektiği ifade edilmiştir. “Üçüncü savunma hattının” yani “iç denetim”, “yönetişim”, “risk yönetimi” ve “kontroller” konusunda özerk ve tarafsız güvence sağladığı bilgisi verilmiştir.

Alanyazın taraması sonucu ulaşılan çalışmalar incelendiğinde, siber güvenliğin özellikle son dönemlerde araştırılması ve bütün unsurlarıyla ortaya konulması gereken bir konu olduğu anlaşılmaktadır. Ayrıca siber güvenlik farkındalığının da toplumun birçok kesiminde tespit edilmesi gereken en önemli hususlardan biri olduğu görülmektedir. Yapılan çalışmalarda siber güvenlik konusunun ele alınma biçimi daha çok kurumlar ve kuruluşlar, üniversite öğrencileri ve öğretmen adayları üzerinde ilerlemekte olduğu ortaya çıkmaktadır. Alanyazın, siber güvenlik farkındalık düzeylerini birçok farklı model kullanılarak çeşitli değişkenler açısından inceleyen çalışmalara rastlanmaktadır. Çalışmaların sonuçlarına bakıldığında, siber güvenlik farkındalığının

erken yaşta oluşması ve bu konuda yetkin olunabilmesi için öğretim programlarının ve bu programları uygulayan öğretmenlerin önemi vurgulanmış olsa da, farkındalığın oluşmasında çok kritik bir rol oynayan eğitim sistemi ve eğitiminde en önemli bileşenlerinden biri olan öğretmenler üzerinde detaylı bir değerlendirme yapan araştırmaya rastlanmamaktadır. Ayrıca, çalışmaların genelinde, araştırma gruplarından veri toplama aşamalarında anket kullanıldığı, görüşmeler yapıldığı, örnek olayların analiz edildiği görülürken bir ölçek kullanılarak farkındalığın incelendiği araştırma sayısı oldukça az olduğu görülmektedir.

BÖLÜM 3

YÖNTEM

Bu bölümde araştırmanın modeli, araştırmanın evreni ve örneklemi, veri toplama araçları, verilerin toplanması ve verilerin çözümlenmesine ilişkin bilgiler yer almaktadır.

Araştırmanın Modeli

Ortaokul öğretmenlerinin siber güvenlik farkındalık düzeylerinin farklı değişkenlere göre değerlendirilmesini amaçlayan bu çalışma, nicel ve nitel yöntemin bir arada kullanılmasını ifade eden karma yöntem modelinde tasarlanmıştır. Karma yöntem "verilerin eşzamanlı veya ardışık olarak toplanıp analiz edilmesi ve birleştirilmesinden" oluşur (Creswell, Plano-Clark, Gutmann ve Hanson, 2003). Karma yöntemin güçlü yönü, istatistiksel değerlendirmelerin yapılabildiği nicel veriler ile bireylerin yaşanmışlıklarıyla ortaya çıkan farklı nitel verileri bir arada kullanmasıdır. Böylelikle tek başına kullanılmasında meydana gelebilecek eksikler tamamlanarak araştırma problemini daha etkin bir biçimde ortaya koyar (Creswell ve Plano Clark, 2018). Karma yöntem, bilhassa toplumsal vakaların tüm yönleriyle incelenmesi ve ortaya koyulmasındaki zorluğu farklı yöntemleri bir arada kullanarak en aza indirgemekte, doğru bir şekilde anlaşılmasına katkı sağlamaktadır (Creswell ve diğerleri, 2003).

Bu kapsam doğrultusunda yürütülen çalışmada, nicel ve nitel verilerin eşzamanlı olarak toplanarak eş değer öncelikle ayrı ayrı çözümlenmesi ve birlikte tartışılarak yorumlanmasını ifade eden karma yöntem araştırma tasarımlarından eşzamanlı tasarım benimsenmiştir (Creswell ve Plano Clark, 2018). Eşzamanlı tasarımın literatürde; paralel karma yöntem tasarımı (Tashakkori, Johnson ve Teddlie, 2021), eş zamanlı nicel + nitel karma yöntem tasarımı (Plano Clark ve Ivankova, 2016) veya çeşitlemeli karma yöntem tasarımı (triangulation mixed method design) (Creswell, 2005) olarak kullanılabildiği görülmektedir. Farklı isimlerle adlandırılsa da tasarımın ifade ettiği anlam, nitel ve nicel verilerin faydalarını eşzamanlı bir araya getirerek analizlerde karşılaştırma yapabilmektir (Çetinkaya, 2013).

Araştırmada ortaokul öğretmenlerinin siber güvenlik düzeylerinin cinsiyet, yaş gibi demografik özellikler, bilgi ve iletişim teknolojileri eğitimi alıp almama durumu gibi özellikler için nicel yöntem kullanılmış, öğretmenlerin siber güvenlik farkındalık düzeylerini artırmaya yönelik önerilerini almak için ise nitel yöntem kullanılmıştır. Nitel veriler Kişisel Bilgiler formunun son sorusunda öğretmenler bilgilendirilerek açık uçlu olarak toplanmıştır. Açık uçlu araştırma sorusu "Siber güvenlik farkındalık düzeyinin artırılmasına yönelik önerileriniz nelerdir? Yazınız." şeklinde düzenlenerek yöneltilmiştir. Konu hakkındaki görüşlerinin belirlenmesi amacıyla yöneltilen soru, öğretmenlerin serbestçe ve detaylı bir biçimde düşüncelerini ifade etmelerine olanak sağlamak amacıyla yazılı olarak yanıtlanmak üzere sınıf ortamında ve araştırmacı tarafından verilmiştir (Çetinkaya ve Sütçü, 2018).

Evren-Örneklem

Araştırmanın çalışma evrenini 2019-2020 eğitim-öğretim yılında (COVID-19 salgını nedeniyle mümkün olmadığı takdirde 2020-2021 öğretim yılında), Ankara il merkezinde bulunan ilçelere (Altındağ, Çankaya, Etimesgut, Gölbaşı, Keçiören, Mamak, Pursaklar, Sincan, Yenimahalle) bağlı kamu ortaokullarında görev yapan ortaokul öğretmenlerinin oluşturması hedeflenmiştir. Araştırmanın evreninde yer alacak okulların belirlenebilmesinde T.C. Milli Eğitim Bakanlığı resmi web sitesinden yararlanılmıştır. Web sitesinde yer alan resmi istatistiklere göre Ankara'daki 9 merkez ilçenin 322 resmi ortaokulunda görev yapan 15883 öğretmen, 49 resmi ortaokulunda görev yapan 1590 imam hatip öğretmeni bulunduğu bilgisine ulaşılmıştır. Ulaşılan bu bilgiler doğrultusunda toplam 371 kamu ortaokullarında görev yapan 17473 öğretmen bulunmaktadır (MEBa, 2021). Ankara'da bulunan tüm ortaokul öğretmenlerine erişmek güç olacağı için araştırma örneklemi, oranlı tabakalı örnekleme yöntemi kullanılarak belirlenmiştir. Tabakalı örnekleme, evreni oluşturan alt grupların saptanarak, evren büyüklüğündeki oranlarıyla örneklemde yansıtmasını amaçlayan bir yöntemdir (Büyüköztürk vd., 2018).

Araştırmada öğretmenlerin görev yaptıkları okul türü (genel ortaokul ve imam hatip ortaokulu) ile okulların bağlı olduğu ilçelerdeki öğretmen sayıları temel alınarak ilçelere göre dağılımları belirlenmiş ve evrende oluşturdukları yüzdelik dilime bakılarak örneklem seçimi yapılmıştır. Buna göre Ankara ilindeki ortaokullarda görev yapan 17473 öğretmeni; %91 ile genel ortaokul öğretmenlerinin (15883 kişi) ve %9 ile imam hatip

öğretmenlerinin (1590 kişi) oluşturduğu sonucuna ulaşılmıştır. Bu doğrultuda örneklem sayısı %9 imam hatip, %91 ise genel ortaokul öğretmenleri olarak belirlenmiştir.

Cochran'ın tabakalı örneklemede, örneklem büyüklüğü hesaplama formülünden yararlanılarak, araştırmanın örneklem büyüklüğü hesaplanmıştır (1962; Akt. Balcı, 2010) yararlanılmıştır.

$$n = \frac{t^2(PQ)/d^2}{1 + (1/N)t^2(PQ)/d^2}$$

Formüle bakıldığında;

n : Örneklem büyüklüğü

N : Evren büyüklüğü

d : Tolerans düzeyi (.05 ya da .01),

t : Güven düzeyinin tablo değeri (1.96 ya da 2.58),

PQ : (.50)(.50)=.25 maksimum örneklem büyüklüğü için örneklem yüzdesini göstermektedir.

Örneklem büyüklüğü, N=17473, tolerans düzeyi d=.05; güven düzeyi t=1.96; maksimum örneklem büyüklüğü için örneklem yüzdesi, PQ=.25 alınarak hesaplanmıştır. Yapılan hesaplamalar doğrultusunda araştırmanın örneklem büyüklüğü 385 olarak bulunmuştur.

Yazıcıoğlu ve Erdoğan (2007), çeşitli örnekleme hatalarına yönelik farklı evren büyüklüklerinden alınması gereken örneklem büyüklükleriyle ilgili bir çalışma gerçekleştirmişlerdir. Çeşitli hesaplamalarla ortaya çıkan sonucu tablolaştırmışlardır. Bu hesaplamalar ile ilgili tablo incelendiğinde evreni temsil etmek için %5 toleransla en az 377 elemandan oluşan örneklemin yeterli olduğu görülmüştür (Tablo 1).

Tablo 1

Farklı Evren Büyüklüklerine Göre Örneklem Büyüklüğü Dağılımı

Evren Büyüklüğü	**Kesinlik (Göz Yumulabilir Hata)**				
	±%**1**	±%**2**	±%**3**	±%**4**	±%**5**
1.000	*	*	*	375	287
2.000	*	*	696	462	322
3.000	*	1334	782	500	341
4.000	*	1500	842	522	350
5.000	*	1622	879	536	357
10.000	4899	1936	964	566	370

(Devam ediyor)

Tablo 1 (Devam)

Farklı Evren Büyüklüklerine Göre Örneklem Büyüklüğü Dağılımı

Evren Büyüklüğü	**Kesinlik (Göz Yumulabilir Hata)**				
	±%1	**±%2**	**±%3**	**±%4**	**±%5**
20.000	6489	2144	1013	583	377
50.000	8057	2291	1045	593	381
100.000	8763	2345	1056	597	383
500.000-∞	9423	2390	1065	600	384

Kaynak: Yazıcıoğlu ve Erdoğan (2007)

Tablo 1'e bakıldığında, %5 toleransla en az 377 elemandan oluşan örneklemin, evreni temsil etmek için yeterli olduğu görülmektedir. Bu duruma bakılarak Cochran'ın (1962; Akt. Balcı, 2010) formülünde hesaplanan örneklem sayısı ile yakın olduğu görülmektedir. Bu doğrultuda yapılan araştırmanın örneklem büyüklüğü en az 377 öğretmen olarak belirlenmiştir. Belirlenen bu örneklem büyüklüğü Ankara iline bağlı ilçelerde görev yapan öğretmenlerin oranlarına göre dağıtılarak seçilmiştir. Her ilçeden alınacak örneklem sayısı Tablo 2'de belirtilmiştir.

Tablo 2

Ankara İlçeleri Genel ve İmam Hatip Ortaokul Öğretmen Dağılımı Frekans ve Yüzde Oranları

İlçeler	Genel Ortaokul				İmam Hatip Ortaokulu			
	Evren		Örneklem		Evren		Örneklem	
	f	%	*f*	%	*f*	%	*f*	%
Altındağ	1291	85.61	38	85.61	217	14.39	6	14.39
Çankaya	2293	95.50	59	95.50	108	4.40	2	4.40
Etimesgut	1828	96.61	54	96.61	64	3.39	2	3.39
Gölbaşı	545	96.81	19	96.81	18	3.19	1	3.19
Keçiören	2906	90.81	66	90.81	294	9.19	6	9.19
Mamak	2157	93.21	53	93.21	157	6.79	4	6.79
Pursaklar	479	70.96	17	70.96	196	29.04	6	29.04
Sincan	2035	89.73	50	89.73	233	10.27	5	10.27
Yenimahalle	2349	88.57	59	88.57	303	11.43	8	11.43
Toplam	15883	100	415	100	1590	100	40	100

Ulaşılması gereken örneklem sayısını %91'i (350 öğretmen) genel ortaokulda, %9'u (35 öğretmen) imam hatip ortaokulunda görev yapan öğretmenler oluşturmaktadır. Tablo 2'de verilen oranlar ışığında her ilçeden alınacak imam hatip ve genel ortaokuldaki öğretmen sayısı belirlenerek okullar, rastgele bir şekilde seçilme suretiyle ulaşılması

gerekenden daha fazla öğretmen örnekleme dâhil edilmiştir. 415'i genel ortaokul ve 40'ı imam hatip ortaokulu olmak üzere seçilen bu okullarda görev yapan toplam 455 öğretmene ulaşılmıştır. Araştırmaya katılan %9'u imam hatip ortaokulunda, %91'i ise genel ortaokulda görev yapan öğretmenlerin %73'ü kadın, %27'si ise erkektir. Demografik bilgilere ilişkin analiz sonuçları bulgular bölümünde detaylandırılarak sunulmuştur.

Tablo 3

Kişisel Siber Güvenliği Sağlama Ölçeği Betimsel İstatistikleri

Değişkenler	**N**	**X̄**	**Ss**	**Çarpıklık (Skewness)**	**Basıklık (Kurtosis)**
Kişisel Gizliliği Koruma	455	39.54	5.84	-.831	1.382
Güvenilmeyenden Kaçınma	455	16.83	4.53	-1.708	1.911
Önlem Alma	455	18.71	4.06	-.480	-.174
Ödeme Bilgilerini Koruma	455	8.69	1.94	-1.584	1.967
İz Bırakmama	455	15.59	2.90	-.690	.709
Ölçek toplamı	455	99.36	11.54	-.395	-.048

Tablo 3'de detaylandırılan çalışmada kullanılan ölçme araçlarının normal dağılım gösterip göstermediğine yönelik yapılan analiz işlemleri sonucunda aritmetik ortalama, mod ve medyan değerlerinin birbirine yakın ve basıklık-çarpıklık (Kurtosis- Skewness) katsayılarının (±2.0) aralığında yer aldığı görülmüştür. Elde edilen bu değerlerin yanı sıra Q-Q grafiği de incelenmiş ve grafikte yer alan noktaların 45 derecelik doğru üzerinde ya da bu doğruya yakın olarak değerlendirilen sınırlar içinde bulunduğu gözlenmiştir. Bir veri setinde Basıklık-Çarpıklık (Kurtosis- Skewness) değerlerinin ±2.0 aralığında olmasının normal dağılım için kabul edilebilir bir ölçüt (Georgeve Mallery, 2003) olmasının yanı sıra Q-Qgrafiği verileri değerlendirildiğinde de çalışmada kullanılan ölçme araçlarının normal dağılım gösterdiği sonucuna ulaşılmıştır. Ayrıca cinsiyetlerine göre öğretmenlerin kişisel siber güvenliği sağlama ölçeği toplam puanları ve alt ölçek puanları arasında homojenliğin [Levene Testi F(Kişisel Gizliliği Koruma=3.549; Güvenilmeyenden Kaçınma= .234; Önlem Alma= 1.091; Ödeme Bilgilerini Koruma= .529; İz Bırakmama: .022 Ölçek toplam=.000), P>.05] söz konusu olduğu belirlenmiştir.

Elde edilen bu sonuçlar doğrultusunda çalışmanın amacı doğrultusunda uygulanacak analiz tekniklerinin uygulanması için gerekli şartları sağlandığı belirlenmiştir. Bu doğrultuda karşılaştırması yapılacak gruplar arasında gözlenen farkların istatistiksel olarak manidar olması durumda ise beliren farkın hangi grup ya da

gruplardan kaynaklandığını tespit edebilmek adına post-hoc testi yapılmıştır (Köklü ve ark., 2006; Roscoe, 1975). Bunun içinde post-hoc istatistiklerinden, "en esnek ve karşılaştırılacak grup sayılarının çok olması durumunda hata payını kontrol altında tutabilen" ve "gruplardaki gözlem sayılarının eşit olması" durumunu göz önünde bulundurmayan bir post hoc türü olan Scheffe metodu kullanılmıştır (Kayri, 2009; Scheffe, 1959). Varyansların homojen olmadığı durumlarda ise gruplardaki gözlem sayılarının eşit olması durumunu göz önünde bulundurmayan post-hoc istatistiklerinden Tamhane's T2 metodu kullanılmıştır. Grupların puan ortalamaları arasındaki farkın manidarlığı .05 düzeyinde yorumlanmış ve veriler analiz edilirken SPSS programından faydalanılmıştır. Elde edilen verilerin çözümlenmesinin ardından bulgular, alanyazın çerçevesinde yorumlanmıştır.

Verilerin Toplanması

Araştırmada veri toplama aracı olarak Erol, Şahin, Yılmaz ve Haseski (2015) tarafından geliştirilen "Kişisel Siber Güvenliği Sağlama Ölçeği" ile araştırmacı tarafından hazırlanan kişisel bilgi formu kullanılmıştır. Ölçme aracı, alınan etik kurul onayı ve Ankara İl Milli Eğitim Müdürlüğü'nden MEB'e bağlı ortaokullarda uygulamasının yapılması izni ile ortaokul düzeyinde görevlerine devam eden 455 öğretmene uygulanmıştır. Katılımcılara, okulların açık olduğu veya resmi toplantılar, imzalar için okulda bulundukları dönemler gözetilerek (COVİD-19 salgını nedeniyle bazı dönemlerde okullar kapalı olduğu için) ölçme aracı uygulanmıştır.

Kişisel Siber Güvenliği Sağlama Ölçeği: İnternet kullanıcılarının siber güvenlik ile ilgili davranışlarını belirlemeye yönelik Erol, Şahin, Yılmaz ve Haseski (2015) tarafından geliştirilen 25 maddeden oluşan ölçek 5' li likert tipi olarak hazırlanmıştır. Her bir madde, "1-Hiçbir zaman", "2-Nadiren", "3-Arasıra", "4-Sıksık" ve "5-Her zaman" arası değerler aldığı 5 faktörlü yapıya sahip olan ölçeğin toplam varyansın %48.026' sını açıkladığı belirlenmiştir. Gerçekleştirilen doğrulayıcı faktör analizi (DFA) sonucunda 5 faktörlü yapı doğrulanmış ve ölçeğin tamamı için Cronbach Alfa güvenirlik katsayısı .763; her alt boyut için sırasıyla; Kişisel Gizliliği Koruma: .763, Güvenilmeyenden Kaçınma: .771, Önlem Alma: .704, Ödeme Bilgilerini Koruma: .829 ve İz Bırakmama: .557 olarak belirlenmiş. Araştırmacılarca yapılan analizler sonucunda bireylerin kişisel siber güvenlik düzeylerini belirlemek amacıyla geliştirilen ölçeğin, geçerli ve güvenilir bir ölçme aracı olduğu sonucuna ulaşılmıştır. Gerçekleştirilen çalışmadan elde edilen

verilerin analizi sonucunda ise ölçme aracının, Cronbach Alfa güvenirlik katsayısının .785; her alt boyut için sırasıyla; Kişisel Gizliliği Koruma: .691, Güvenilmeyenden Kaçınma: .842, Önlem Alma: .774, Ödeme Bilgilerini Koruma: .816 ve İz Bırakmama: .595 olarak belirlenmiştir. Yapılan Kaiser-Meyer-Olkin (KMO) testi sonucu (KMO=.774) çalışmanın örneklem büyüklüğünün orta düzey (Çokluk, Şekercioğlu ve Büyüköztürk., 2012; Field, 2000;), Bartlett testi ise (<.05) verilerin çok değişkenli normal dağılımdan geldiğini göstermektedir (Büyüköztürk, 2011).

Kişisel Bilgi Formu: Çalışmada bağımsız değişkenlere ait veriler kişisel bilgi formu kullanılarak toplanmıştır. Kişisel bilgi formunda çalışmaya katılan öğretmenlerin cinsiyet, yaş, gibi kişisel bilgilerinin yanı sıra bilgi güvenliğiyle ilişkilendirilecek olan bilgi ve iletişim teknolojilerine ya da siber güvenliğe yönelik alınan eğitimlere ait bilgileri içermektedir.

Verilerin Çözümlenmesi ve Yorumlanması

Araştırmada kullanılan kişisel bilgileri içeren anketten ve Kişisel Siber Güvenliği Sağlama ölçeğinden elde edilen veriler ile ilgili hem betimsel istatistiklere hem de karşılaştırması yapılacak gruplar arasında gözlenen farkların istatistiksel olarak manidar olup olmadıklarına bakılmıştır. Bu doğrultuda iki ilişkisiz örneklem arasındaki farkın manidar olup olmadığı "bağımsız örneklem t testi" analizi ile grup sayısının ikiden daha fazla olduğu durumda ise "tek yönlü varyans analizi (ANOVA)" ile çözümleme yapılması planlanmıştır. Bunun için öncelikle Bilgi güvenliği ölçeği ve alt faktörlerinin normal dağılıp dağılmadığı ve homojenlik ön şartlarına bakılmıştır.

BÖLÜM 4

BULGULAR VE YORUMLAR

Çalışmanın bu bölümünde öğretmenlerin siber güvenlik farkındalık düzeylerine ilişkin elde edilen bulgular ve yorumlar başlıklar altında sunulmaktadır.

4.1. Öğretmenlerin Kişisel Siber Güvenliği Sağlama Düzeyleri

Öğretmenlerin siber güvenlik farkındalık düzeylerine yönelik ortalama ve standart sapma değerleri Tablo 4'te verilmiştir.

Tablo 4

Öğretmenlerin Kişisel Siber Güvenliği Sağlama Düzeyleri

Ölçek alt Faktörleri	**Min.**	**Max.**	**N**	**X̄**	**Ss**
Kişisel Gizliliği Koruma	10	50	455	39.54	5.84
Güvenilmeyenden Kaçınma	4	20	455	16.83	4.53
Önlem Alma	5	25	455	18.71	4.06
Ödeme Bilgilerini Koruma	2	10	455	8.69	1.94
İz Bırakmama	4	20	455	15.59	2.90
Ölçek toplamı	59	125	455	99.36	11.54

Öğretmenlerin kişisel siber güvenliği sağlama durumlarına ilişkin yapılan analizler sonucunda, kişisel siber güvenliği sağlama düzeylerini belirlemeye yönelik ölçekten ortalamanın üstünde ($\bar{X}$ = 99.36) puan aldıkları belirlenmiştir. Yine ölçeğin kişisel gizliliği koruma ($\bar{X}$ =39.54), güvenilmeyenden kaçınma ($\bar{X}$ =16.83), önlem alma ($\bar{X}$ =18.71), ödeme bilgilerini koruma ($\bar{X}$ =8.69) ve iz bırakmama ($\bar{X}$ =15.59) alt faktörlerinden de alınan puanların ortalamanın üstünde olduğu görülmektedir.

Öğretmenleri demografik özellikleri ile kişisel siber güvenliği sağlama durumlarına ilişkin elde edilen araştırma bulguları aşağıda verilmektedir.

4.2. Öğretmenlerin Demografik Özelliklerine Göre Siber Güvenliği Sağlama Durumları

Öğretmenlerin demografik özelliklerinin, siber güvenliği sağlama düzeylerine ilişkin elde edilen araştırma bulguları aşağıda başlıklar altında sunulmuştur.

4.2.1. Öğretmenlerin Cinsiyetlerine Göre Siber Güvenliği Sağlama Durumları

Öğretmenlerin siber güvenliği sağlama düzeylerinin cinsiyetlerine göre anlamlı bir farklılık gösterip göstermediğini belirlemek amacıyla gerçekleştirilen ilişkisiz örneklemler için t-testi analizi sonuçları Tablo 5'te verilmiştir.

Tablo 5

Öğretmenlerin Cinsiyetleri ile Siber Güvenliği Sağlama Düzeylerine İlişkin T-Testi Sonuçları

Ölçek alt Faktörleri	Cinsiyet	N	X̄	S	t	df	p
Kişisel Gizliliği Koruma	Kadın	331	39.89	5.59	2.102	453	.036*
	Erkek	124	38.61	6.38			
Güvenilmeyenden Kaçınma	Kadın	331	16.99	4.54	1.257	453	.209
	Erkek	124	16.40	4.49			
Önlem Alma	Kadın	331	18.72	4.02	.041	453	.968
	Erkek	124	18.70	4.20			
Ödeme Bilgilerini Koruma	Kadın	331	8.80	1.92	2.091	453	.037*
	Erkek	124	8.38	1.96			
İz Bırakmama	Kadın	331	15.58	2.92	-.071	453	.943
	Erkek	124	15.61	2.87			
Ölçek Toplamı	Kadın	331	99.99	11.47	1.903	453	.058
	Erkek	124	97.69	11.60			

*p<.05

Tablo 5 incelendiğinde, öğretmenlerin siber güvenliği sağlama düzeylerinin cinsiyetlerine göre anlamlı bir farklılık göstermediği belirlenmiştir, [t(453)=1.903, P>.05]. Ölçeğin tüm faktörlerinin toplamından elde edilen puanlara göre kadın öğretmenlerin (X̄=99.99) siber güvenliği sağlama düzeylerinin erkek öğretmenlerden (X̄=97.69) daha yüksek düzeyde olduğu belirlenmiştir. Bu durum kadın öğretmenlerin siber güvenliği sağlama düzeylerinin erkek öğretmenlere göre daha yüksek düzeyde olduğunu gösterse de cinsiyet ile siber güvenliğin sağlanma düzeyi arasında anlamlı bir ilişkinin olmadığı bulgusuna ulaşılmıştır. Diğer taraftan gerçekleştirilen analizler sonucunda, ölçeğin kişisel gizliliği koruma [t(453)=2.102, P<.05] ve ödeme bilgilerini

koruma [t(453)=2.091, P<.05] alt faktörlerinin cinsiyete göre anlamlı bir farklılık gösterdiği belirlenmiştir. Ancak, ölçeğin güvenilmeyenden kaçınma [t(453)=1.257, P>.05], önlem alma [t(453)=.041, P>.05], ve iz bırakmama [t(453)=-.071, P>.05] alt faktörleri ile öğretmenlerin cinsiyetleri arasında anlamlı bir farklılık gözlenmemiştir.

Siber güvenliği sağlama düzeyine yönelik cinsiyetlere göre anlamlı bir fark oluşmaması araştırmaya katılan kadın ve erkek öğretmenlerin dijital ortamlarda siber güvenliği sağlama konusunda benzer özellikler gösterdiği şeklinde yorumlanabilir. Yiğit ve Seferoğlu'nun (2019) üniversite öğrencilerinin siber güvenlik davranışlarını inceledikleri araştırmalarında benzer şekilde, siber güvenlik davranış puanlarının cinsiyete göre farklılaşmadığı tespit edilmiştir. Yine benzer şekilde ölçeğin alt faktörlerinden kişisel gizliliği koruma konusunda kadın öğrencilerin lehine anlamlı fark bulunmuştur. Siber güvenliği sağlama düzeyine ilişkin bulgulara bakıldığında kadın ve erkek öğretmenler arasında anlamlı bir fark gözlenmemesinin nedeni öğretmenlerin karşılaştıkları risk faktörlerinin benzer olabileceği ve bu risklere karşı verilen tepkilerin de benzerlik gösterdiği şeklinde yorumlanabilir.

Karacı, Akyüz ve Bilgici'nin (2017) "Bilgisayar Mühendisliği" bölümde öğrenim gören öğrenciler ile "Bilgisayar ve Öğretim Teknolojileri Öğretmenliği" bölümünde öğrenim gören öğrencilerin siber güvenlik davranışlarını inceledikleri araştırmalarında, cinsiyet değişkenine göre "siber güvenlik davranış puanları" arasında, tüm faktörlere bakılmış ancak istatistiksel olarak anlamlı bir farklılık gözlenmemiştir. Ancak, Akgün ve Topal'ın (2015) araştırma grubunu eğitim fakültelerinde öğrenim gören son sınıf öğrencileri oluşturmuş, katılımcıların interneti eğitim amacıyla kullanımlarındaki "öz yeterlilik algılarını" çeşitli değişkenlerle belirlemeye çalışmışlardır. Araştırmalarında, cinsiyete göre anlamlı bir farklılık bularak "bazı bilişim güvenliği konularında" kız öğrencilerin erkek öğrencilere göre farkındalık sahibi oldukları bilgisine ulaşılmıştır.

4.2.2. Öğretmenlerin Yaşlarına Göre Siber Güvenliği Sağlama Durumları

Öğretmenlerin yaşlarına göre siber güvenlik farkındalıklarına yönelik ortalama ve standart sapma değerleri Tablo 6'te verilmiştir.

Tablo 6

Öğretmenlerin Yaşlarına Göre Siber Güvenliği Sağlama Düzeyleri Ortalama ve Standart Sapma Değerleri

Ölçek alt Faktörleri	Yaş Aralıkları	N	X̄	Ss
Kişisel Gizliliği Koruma	30 ve altı	56	38,00	5,94
	31-35	106	39,69	5,48
	36-40	121	39,78	6,43
	41-45	77	40,14	4,94
	46-50	45	39,38	5,94
	50 ve üstü	50	39,60	6,09
	Toplam	455	39,54	5,84
Güvenilmeyenden Kaçınma	30 ve altı	56	17,59	3,97
	31-35	106	17,39	4,18
	36-40	121	17,12	4,37
	41-45	77	16,39	4,44
	46-50	45	16,84	4,22
	50 ve üstü	50	14,76	5,96
	Toplam	455	16,83	4,53
Önlem Alma	30 ve altı	56	19,02	3,58
	31-35	106	18,63	4,03
	36-40	121	19,12	4,31
	41-45	77	18,40	4,01
	46-50	45	18,58	4,01
	50 ve üstü	50	18,18	4,23
	Toplam	455	18,71	4,06
Ödeme Bilgilerini Koruma	30 ve altı	56	8,96	1,44
	31-35	106	8,79	1,82
	36-40	121	8,88	1,90
	41-45	77	8,61	1,73
	46-50	45	7,82	2,72
	50 ve üstü	50	8,58	2,07
	Toplam	455	8,69	1,94
İz Bırakmama	30 ve altı	56	15,54	2,70
	31-35	106	15,26	2,75
	36-40	121	15,88	2,98
	41-45	77	15,25	2,60
	46-50	45	15,84	3,28
	50 ve üstü	50	15,94	3,29
	Toplam	455	15,59	2,90

(Devam ediyor)

Tablo 6 (Devam)

Öğretmenlerin Yaşlarına Göre Siber Güvenliği Sağlama Düzeyleri Ortalama ve Standart Sapma Değerleri

Ölçek alt Faktörleri	Yaş Aralıkları	N	X̄	Ss
Ölçek Toplamı	30 ve altı	56	99,11	9,88
	31-35	106	99,76	11,32
	36-40	121	100,78	12,87
	41-45	77	98,79	10,87
	46-50	45	98,47	11,69
	50 ve üstü	50	97,06	11,21
	Toplam	455	99,36	11,54

Öğretmenlerin yaş gruplarına göre kişisel siber güvenliği sağlama durumları incelendiğinde özellikle 36-40 yaş aralığındaki kişisel siber güvenliği sağlama düzeylerine ilişkin puanlarının ölçeğin tamamı ve alt faktörlerinin çoğunda diğer yaş gruplarına göre daha yüksek olduğu görülmektedir. Burada özellikle 36-40 yaş gurubu öğretmenlerin sonrasında yer alan daha yüksek yaş gruplarında kademeli olarak kişisel siber güvenliği sağlama düzeylerine ilişkin ortalama puanların düşüşe geçtiği ve 50 üstü yaş gurubunun düşük puana sahip olması dikkat çekmektedir. Yine benzer durumun 36-40 yaş grubundan daha küçük yaş gruplarından gözlendiği ve yaş gurubu küçüldükçe kişisel siber güvenliği sağlama düzeylerine ilişkin ortalama puanların düşüşe geçtiği görülmektedir. Bu noktada öğretmenlerin siber güvenlik farkındalıklarının yaşlarına göre anlamlı bir farklılık gösterip göstermediğini belirlemek amacıyla gerçekleştirilen ANOVA analizi sonuçları Tablo 7'da verilmiştir.

Tablo 7

Öğretmenlerin Yaşları ile Siber Güvenliği Sağlama Düzeylerine İlişkin ANOVA Sonuçları

Ölçek alt Faktörleri	Varyansın Kaynağı	Kareler Toplamı	sd	Kareler Ort.	F	p	Fark
Kişisel Gizliliği Koruma	Gruplararası	171.290	5	34.258	1.006	.414	
	Grupiçi	15287.708	449	34.048			
	Toplam	15458.998	454				
Güvenilmeyenden Kaçınma	Gruplararası	304.791	5	60.958	3.041	.010*	50> ile <30, 31-35, 36-40
	Grupiçi	9001.178	449	20.047			
	Toplam	9305.969	454				

(Devam ediyor)

Tablo 7 (devam)

Öğretmenlerin Yaşları ile Siber Güvenliği Sağlama Düzeylerine İlişkin ANOVA Sonuçları

Önlem Alma	Gruplararası	47.967	5	9.593	.579	.716	
	Grupiçi	7444.891	449	16.581			
	Toplam	7492.857	454				
Ödeme Bilgilerini Koruma	Gruplararası	44.871	5	8.974	2.432	.034*	46-50 ile <30 ve 36-40
	Grupiçi	1656.812	449	3.690			
	Toplam	1701.684	454				
İz Bırakmama	Gruplararası	39.429	5	7.886	.937	.457	
	Grupiçi	3780.716	449	8.420			
	Toplam	3820.145	454				
Ölçek toplamı	Gruplararası	589.033	5	117.807	.884	.492	
	Grupiçi	59864.131	449	133.328			
	Toplam	60453.165	454				

*p<.05

Analiz sonucunda öğretmenlerin kişisel siber güvenliği sağlama düzeylerinin yaşlarına göre anlamlı bir farklılık göstermediği belirlenmiştir, [F(5-449)=.884, p<.05]. Başka bir deyişle öğretmenlerin kişisel siber güvenliği sağlama düzeylerine ilişkin ortalama puanları yaşlarına bağlı olarak anlamlı bir şekilde değişmemektedir. Kişisel siber güvenliği sağlama durumlarına ilişkin ölçeğin alt faktörlerinin, öğretmenlerin yaş aralıkları ve kişisel siber güvenliği sağlama düzeylerine göre farklılık gösterip göstermediği incelendiğinde ise; Kişisel Gizliliği Koruma [F(5-449)=1.006, p>.05], Önlem Alma [F(5-449)=.576, p>.05] ve İz Bırakmama [F(5-449)=.937, p>.05] alt faktörlerinde anlamlı bir farklılığın olmadığı belirlenmiştir. Ölçeğin Güvenilmeyenden Kaçınma [F(5-449)=3.041, p<.05] ve Ödeme Bilgilerini Koruma [F(5-449)=8.974, p<.05] alt faktörlerinde ise kişisel siber güvenliği sağlama düzeylerine göre anlamlı bir farklılığın ortaya çıktığı görülmüştür.

Ölçeğin tamamında görülmese de güvenilmeyenden kaçınma ve ödeme bilgilerini koruma alt faktörlerinde görülen anlamlı farklılığın kaynağının belirlenmesi için gerçekleştirilen Scheffe testi gerçekleştirilmiştir. Yapılan analizler sonucunda güvenilmeyenden kaçınma alt faktöründe belirlenen 50 yaş üstü bireylerin olduğu ve bu yaş grubunun 40 yaş altı (<30, 31-35, 36-40) tüm guruplarla farklılık gösterdiği belirlenmiştir. Ödeme bilgilerini koruma alt faktöründe ise farklılığı 46-50 ile <30 ve 36-40 guruplarından kaynaklandığı sonucuna ulaşılmıştır. Elde edilen veriler özellikle güvenilmeyenden kaçınma ve ödeme bilgilerini koruma ile ilgili konularda yaş ilerledikçe

siber güvenlik ile ilgili daha az bilgi sahibi olunması ve siber uzayda deneyimsel açıdan dezavantajlı olunması anlamlı farklılığın kaynağını oluşturduğunu göstermektedir. Ayrıca, bu yaş grubu için gelişen teknolojinin hayatlarının birçok alanına sonradan dahil olması ve erken yaşlardan itibaren konu ile ilgili eğitimleri mezun oldukları fakültelerde ve mesleki yaşantılarında alamamaları farklılığın oluşmasına sebep olduğu anlaşılmaktadır.

Ünal ve Ergen (2018) İstanbul'da yaşayan 18 yaş ve üzeri bireylerin siber alanda gerçekleştirdikleri uygulamalar sırasında siber güvenlikle ilgili davranışlarını ölçtükleri çalışmada, 26-35 yaş aralığındaki bireylerin lehine anlamlı farklılık bulunmuştur. Benzer şekilde Aksoğan, Bayer, Gülada ve Çelik'in (2018) İletişim Fakültesinde farklı bölüm ve sınıflarda öğrenim gören öğrencilerin siber suçlar ve siber güvenlik hakkındaki farkındalıklarını incelemek amacıyla yaptıkları araştırmada, 26 ve üstü yaştaki öğrencilerin diğer yaş gruplarındaki öğrencilere göre anlamlı farklılık gösterdiği bulgusuna ulaşılmıştır.

4.2.3. Öğretmenlerin Kıdem/Görev Yılına Göre Siber Güvenliği Sağlama Durumları

Öğretmenlerin kıdemlerine göre siber güvenliği sağlama düzeylerinin ortalama ve standart sapma değerleri Tablo 8'de verilmiştir.

Tablo 8

Öğretmenlerin Kıdemlerine Göre Siber Güvenliği Sağlama Düzeyleri Ortalama ve Standart Sapma Değerleri

Ölçek alt Faktörleri	Kıdem/Yıl	N	X̄	Ss
Kişisel Gizliliği Koruma	10 ve altı	140	38.74	5.88
	11-20	215	39.93	5.58
	21-30	88	39.88	6.18
	31-40	12	39.50	7.00
	Toplam	455	39.54	5.84
Güvenilmeyenden Kaçınma	10 ve altı	140	17.17	4.23
	11-20	215	16.87	4.40
	21-30	88	16.52	4.93
	31-40	12	14.33	6.47

(Devam ediyor)

Tablo 8 (Devam)

Öğretmenlerin Kıdemlerine Göre Siber Güvenliği Sağlama Düzeyleri Ortalama ve Standart Sapma Değerleri

Ölçek alt Faktörleri	Kıdem/Yıl	N	X̄	Ss
	Toplam	455	16.83	4.53
Önlem Alma	10 ve altı	140	18.71	3.63
	11-20	215	18.84	4.34
	21-30	88	18.57	4.05
	31-40	12	17.67	4.12
	Toplam	455	18.71	4.06
Ödeme Bilgilerini Koruma	10 ve altı	140	8,71	1,81
	11-20	215	8,74	1,94
	21-30	88	8,51	2,07
	31-40	12	8,75	2,53
	Toplam	455	8,69	1,94
İz Bırakmama	10 ve altı	140	15,29	2,80
	11-20	215	15,63	2,82
	21-30	88	15,74	3,20
	31-40	12	17,17	3,04
	Toplam	455	15,59	2,90
Ölçek Toplamı	10 ve altı	140	98,62	10,77
	11-20	215	100,01	12,10
	21-30	88	99,22	11,31
	31-40	12	97,42	12,21
	Toplam	455	99,36	11,54

Öğretmenlerin kıdemlerine göre kişisel siber güvenliği sağlama durumları incelendiğinde, kişisel siber güvenliği sağlama düzeylerine ilişkin puanlarının ölçeğin tamamı ve alt faktörlerinin çoğunda birbirine yakın olduğu görülmektedir. Ölçeğin Kişisel Gizliliği Koruma alt faktörüne bakıldığında, en yüksek ortalama puanı ($\bar{x}$= 39.93) 11-20 yıl arasında görev yapan öğretmenler alırken, en düşük ortalama puanı ($\bar{x}$= 38.74) 10 yıl ve daha az görev yapan öğretmenlerin aldığı görülmektedir. Güvenilmeyenden Kaçınma alt faktöründe ise en yüksek ortalama puanın ($\bar{x}$= 17.17) 10 yıl ve daha az görev yapan öğretmenlere, en düşük ortalama puanın ($\bar{x}$= 14.33) 31-40 yıl görev yapan öğretmenlere ait olduğu görülmektedir. Önlem Alma alt faktöründen alınan puanlar, en yüksek ortalama ($\bar{x}$= 18.84) 11-20 yıl, en düşük ortalama ($\bar{x}$= 17.67) 31-40 yıl, Ödeme Bilgilerini Koruma alt faktöründe ise en yüksek ortalama ($\bar{x}$= 8.75) 31-40 yıl, en düşük ortalama ($\bar{x}$= 8.51) 21-30 yıl, İz Bırakmama alt faktöründe en yüksek ortalama ($\bar{x}$= 17.17)

31-40 yıl, en düşük ortalama ($\bar{x}$= 15.29) 10 yıl ve daha az görev yapan öğretmenlere ait olduğunu göstermektedir. Bu noktada öğretmenlerin siber güvenlik farkındalıklarının kıdemlerine göre anlamlı bir farklılık gösterip göstermediğini belirlemek amacıyla gerçekleştirilen ANOVA analizi sonuçları Tablo 9'da verilmiştir.

Tablo 9

Öğretmenlerin Kıdemleri ile Siber Güvenliği Sağlama Düzeylerine İlişkin ANOVA Sonuçları

Ölçek alt Faktörleri	Varyansın Kaynağı	Kareler Toplamı	sd	Kareler Ort.	F	p	Fark
Kişisel Gizliliği Koruma	Gruplararası	130.821	3	43.607	1.283	.280	
	Grupiçi	15328.177	451	33.987			
	Toplam	15458.998	454				
Güvenilmeyenden Kaçınma	Gruplararası	99.853	3	33.284	1.631	.182	
	Grupiçi	9206.116	451	20.413			
	Toplam	9305.969	454				
Önlem Alma	Gruplararası	18.304	3	6.101	.368	.776	
	Grupiçi	7474.553	451	16.573			
	Toplam	7492.857	454				
Ödeme Bilgilerini Koruma	Gruplararası	3.522	3	1.174	.312	.817	
	Grupiçi	1698.162	451	3.765			
	Toplam	1701.684	454				
İz Bırakmama	Gruplararası	44.525	3	14.842	1.773	.152	
	Grupiçi	3775.620	451	8.372			
	Toplam	3820.145	454				
Ölçek toplamı	Gruplararası	215.457	3	71.819	.538	.657	
	Grupiçi	60237.708	451	133.565			
	Toplam	60453.165	454				

*p<.05

Analiz sonucunda öğretmenlerin kişisel siber güvenliği sağlama düzeylerinin görev yıllarına göre anlamlı bir farklılık göstermediği belirlenmiştir, [F(3-451)=.538, p<.05]. Başka bir deyişle öğretmenlerin kişisel siber güvenliği sağlama düzeylerine ilişkin ortalama puanları görev yıllarına bağlı olarak anlamlı bir şekilde değişmemektedir. Kişisel siber güvenliği sağlama durumlarına ilişkin ölçeğin alt faktörlerinin, öğretmenlerin görev yılları ve kişisel siber güvenliği sağlama düzeylerine göre farklılık gösterip göstermediği incelendiğinde ise; Kişisel Gizliliği Koruma [F(3-451)=1.283, p>.05], Güvenilmeyenden Kaçınma [F(3-451)=1.631, p>.05] Önlem Alma [F(3-

451)=.368, p>.05], Ödeme Bilgilerini Koruma [F(3-451)=.312, p>.05] ve İz Bırakmama [F(3-451)=1.773, p>.05] alt faktörlerinde anlamlı bir farklılığın olmadığı belirlenmiştir.

Yılmaz ve diğerleri (2016) 29 farklı okulda görev yapan 870 öğretmenin katıldığı, "Milli Eğitim Bakanlığı'na bağlı okullarda" çalışan öğretmenlerin "dijital veri güvenliği farkındalıklarını" irdeledikleri araştırmada, öğretmenlerin "dijital veri güvenliği farkındalıklarının" mesleki deneyimlerine göre fark gösterip göstermediği incelenmiştir. Yapılan analiz sonucunda, "dijital veri güvenliği farkındalığının" öğretmenlik mesleğini yapma süresine göre değişmediği görülmüştür. Benzer şekilde, Teker (2019) tarafından, "Milli Eğitim Bakanlığı'na bağlı ilk ve ortaöğretim okullarında" görev yapan 603 öğretmenin ve lisede öğrenim gören 4223 öğrencinin katılımıyla gerçekleştirilen araştırmada, öğretmenlerin hizmet süresine göre bilgi güvenliği farkındalıkları arasındaki ilişki incelenerek anlamlı bir farklılık bulunmamıştır. Ölçeğin alt faktörlerine bakıldığında; Genel Güvenlik, Saldırı ve Tehditler, Mobil Cihazlar, Mahremiyet ve İletişim faktörlerinde de bilgi güvenliği farkındalığının hizmet sürelerine ilişkin anlamlı bir farklılık olmadığı görülmüştür.

4.2.4. Öğretmenlerin Branşlarına Göre Siber Güvenliği Sağlama Durumları

Öğretmenlerin branşlarına göre siber güvenliği sağlama düzeylerinin ortalama ve standart sapma değerleri Tablo 10'da verilmiştir.

Tablo 10

Öğretmenlerin Branşlarına Göre Siber Güvenliği Sağlama Düzeyleri Ortalama ve Standart Sapma Değerleri

Ölçek alt Faktörleri	Branş	N	X̄	Ss
Kişisel Gizliliği Koruma	Matematik	59	38.37	5.58
	Türkçe	67	40.06	5.44
	Fen	52	38.33	6.04
	Görsel sanatlar	6	37.67	4.80
	Beden eğitimi	17	37.76	6.66
	Sosyal bilgiler	30	39.27	7.12
	Bilişim Teknolojileri	60	42.53	6.21
	Diğer	164	39.34	5.24
	Toplam	455	39.54	5.84

(Devam ediyor)

Tablo 10

Öğretmenlerin Branşlarına Göre Siber Güvenliği Sağlama Düzeyleri Ortalama ve Standart Sapma Değerleri

Ölçek alt Faktörleri	Branş	N	X̄	Ss
Güvenilmeyenden Kaçınma	Matematik	59	17.63	3.05
	Türkçe	67	17.33	4.14
	Fen	52	16.00	5.42
	Görsel sanatlar	6	13.50	6.44
	Beden eğitimi	17	17.88	3.30
	Sosyal bilgiler	30	17.97	2.68
	Bilişim Teknolojileri	60	17.65	3.39
	Diğer	164	16.11	5.27
	Toplam	455	16.83	4.53
Önlem Alma	Matematik	59	18.46	4.07
	Türkçe	67	17.18	3.87
	Fen	52	18.33	3.66
	Görsel sanatlar	6	17.17	3.37
	Beden eğitimi	17	18.12	3.76
	Sosyal bilgiler	30	19.33	4.25
	Bilişim Teknolojileri	60	21.65	3.01
	Diğer	164	18.49	4.14
	Toplam	455	18.71	4.06
Ödeme Bilgilerini Koruma	Matematik	59	8.32	2.06
	Türkçe	67	8.61	2.02
	Fen	52	8.48	2.15
	Görsel sanatlar	6	9.00	1.67
	Beden eğitimi	17	9.29	1.36
	Sosyal bilgiler	30	9.53	1.01
	Bilişim Teknolojileri	60	9.20	1.45
	Diğer	164	8.50	2.06
	Toplam	455	8.69	1.94
İz Bırakmama	Matematik	59	15.53	2.36
	Türkçe	67	15.48	2.84
	Fen	52	14.94	3.36
	Görsel sanatlar	6	15.67	2.94
	Beden eğitimi	17	16.18	2.88
	Sosyal bilgiler	30	16.23	2.42
	Bilişim Teknolojileri	60	16.67	2.38
	Diğer	164	15.29	3.12
	Toplam	455	15.59	2.90
Ölçek Toplamı	Matematik	59	98.31	11.44
	Türkçe	67	98.66	10.51
	Fen	52	96.08	11.12
	Görsel sanatlar	6	93.00	12.35
	Beden eğitimi	17	99.24	11.51
	Sosyal bilgiler	30	102.33	10.67
	Bilişim Teknolojileri	60	107.70	10.33
	Diğer	164	97.73	11.35
	Toplam	455	99.36	11.54

Öğretmenlerin branşlarına göre kişisel siber güvenliği sağlama durumları incelendiğinde Bilişim Teknolojileri branşındaki öğretmenlerin kişisel siber güvenliği sağlama düzeylerine ilişkin puanlarının ölçeğin tamamında diğer branştaki öğretmenlere göre daha yüksek olduğu, görülmektedir. Ölçeğin Kişisel Gizliliği Koruma alt faktörüne bakıldığında, en yüksek ortalama puanı ($\bar{x}$= 42.53) Bilişim Teknolojileri branşındaki öğretmenler alırken, en düşük ortalama puanı ($\bar{x}$= 37.67) Görsel Sanatlar branşındaki öğretmenlerin aldığı görülmektedir. Güvenilmeyenden Kaçınma alt faktöründe ise en yüksek ortalama puanın ($\bar{x}$= 17.97) Sosyal Bilgiler branşı, en düşük ortalama puanın ($\bar{x}$= 13.50) Görsel Sanatlar branşının aldığı görülmektedir. Önlem Alma alt faktöründen alınan puanlar, en yüksek ortalama ($\bar{x}$= 21.65) Bilişim Teknolojileri, en düşük ortalama ($\bar{x}$= 17.17) Görsel Sanatlar olarak, Ödeme Bilgilerini Koruma alt faktöründe ise en yüksek ortalama ($\bar{x}$= 9.53) Sosyal Bilgiler, en düşük ortalama ($\bar{x}$= 8.32) Matematik olarak, İz Bırakmama alt faktöründe en yüksek ortalama puanı ($\bar{x}$= 16,67) Bilişim Teknolojileri branşının, en düşük ortalama puanı ($\bar{x}$= 14,94) Fen Bilimleri branşının aldığı görülmektedir. Bu noktada öğretmenlerin siber güvenlik farkındalıklarının branşlarına göre anlamlı bir farklılık gösterip göstermediğini belirlemek amacıyla gerçekleştirilen ANOVA analizi sonuçları Tablo 11'da verilmiştir.

Tablo 11

Öğretmenlerin Branşları ile Siber Güvenliği Sağlama Düzeylerine İlişkin ANOVA Sonuçları

Ölçek alt Faktörleri	Varyansın Kaynağı	Kareler Toplamı	sd	Kareler Ort.	F	P	Fark
Kişisel Gizliliği Koruma	Gruplararası	795.927	7	113.704	3.466	.001	BT ile Matematik, Fen,
	Grupiçi	14663.070	447	32.803			
	Toplam	15458.998	454				
Güvenilmeyenden Kaçınma	Gruplararası	339.491	7	48.499	2.418	.019	BT ile Fen, Diğer; Görsel sanatlar ile BT Matematik
	Grupiçi	8966.478	447	20.059			
	Toplam	9305.969	454				
Önlem Alma	Gruplararası	727.030	7	103.861	6.862	.000	BT ile Matematik, Türkçe, Fen, Diğer;
	Grupiçi	6765.827	447	15.136			
	Toplam	7492.857	454				

(Devam ediyor)

Tablo 11 (Devam)

Öğretmenlerin Branşları ile Siber Güvenliği Sağlama Düzeylerine İlişkin ANOVA Sonuçları

Ölçek alt Faktörleri	Varyansın Kaynağı	Kareler Toplamı	sd	Kareler Ort.	F	P	Fark
Ödeme Bilgilerini Koruma	Gruplararası	60.315	7	8.616	2.347	.023	BT ile Matematik, Fen, Diğer; Sosyal Bilimler ile Türkçe, Fen, Diğer
	Grupiçi	1641.369	447	3.672			
	Toplam	1701.684	454				
İz Bırakmama	Gruplararası	125.855	7	17.979	2.175	.035	BT ile Matematik, Fen, Türkçe, Diğer
	Grupiçi	3694.290	447	8.265			
	Toplam	3820.145	454				
Ölçek toplamı	Gruplararası	5778.882	7	825.555	6.749	.000	BT ile Matematik, Türkçe, Fen, Diğer
	Grupiçi	54674.283	447	122.314			
	Toplam	60453.165	454				

*p<.05

Analiz sonucunda öğretmenlerin kişisel siber güvenliği sağlama düzeylerinin branşlarına göre anlamlı bir farklılık gösterdiği belirlenmiştir [F(7-447)=6.749, p<.05]. Başka bir deyişle öğretmenlerin kişisel siber güvenliği sağlama düzeylerine ilişkin ortalama puanları branşlarına bağlı olarak anlamlı bir şekilde değişmemektedir. Kişisel siber güvenliği sağlama durumlarına ilişkin ölçeğin alt faktörlerinin, öğretmenlerin branşları ve kişisel siber güvenliği sağlama düzeylerine göre farklılık gösterip göstermediği incelendiğinde ise; Kişisel Gizliliği Koruma [F(7-447)=3.466, p<.05], Güvenilmeyenden Kaçınma [F(7-447)=2.418, p<.05], Önlem Alma [F(7-447)=6.862, p<.05], Ödeme Bilgilerini Koruma [F(7-447)=2.347, p<.05] ve İz Bırakmama [F(7-447)=2.175, p<.05] bütün alt faktörlerde kişisel siber güvenliği sağlama düzeylerine göre anlamlı bir farklılığın ortaya çıktığı görülmüştür.

Ölçeğin tamamında görülen anlamlı farklılığın kaynağının belirlenmesi için gerçekleştirilen Scheffe testi gerçekleştirilmiştir. Yapılan analizler sonucunda Kişisel Gizliliği Koruma alt faktöründe belirlenen Bilişim Teknolojileri branşının Matematik ve Fen Bilimleri branşları ile farklılık gösterdiği belirlenmiştir. Güvenilmeyenden Kaçınma

alt faktöründe Bilişim Teknolojileri ile Fen Bilimleri ve Diğer branşlarının, Görsel Sanatlar ile Bilişim Teknolojileri ve Matematik branşlarının farklılık gösterdiği belirlenmiştir. Önlem Alma alt faktöründe, Bilişim Teknolojileri ile Matematik, Türkçe, Fen Bilimleri ve Diğer branşları ile farklılık gösterdiği belirlenmiştir. Ödeme Bilgilerini koruma alt faktöründe, Bilişim Teknolojileri ile Matematik, Fen Bilimleri ve Diğer branşları, Sosyal Bilimler ile Türkçe Fen Bilimleri ve Diğer branşları ile farklılık gösterdiği belirlenmiştir. İz Bırakmama alt faktöründe Bilişim Teknolojileri ile Matematik, Fen Bilimleri, Türkçe ve Diğer branşları ile farklılık gösterdiği belirlenmiştir. Ölçeğin tamamında ise Bilişim Teknolojileri branşının diğer tüm gruplarla farklılık gösterdiği sonucuna ulaşılmıştır. Elde edilen veriler özellikle Bilişim Teknolojileri öğretmenlerinin mezun oldukları bölümdeki öğretim programında siber güvenlik ile yakından ilişkili derslerin yer alması, mesleki deneyimlerinden elde ettikleri bilgilerin siber güvenlik ile yakın ilişki içinde olması ve bu alandaki yatkınlık anlamlı farklılığın kaynağını oluşturduğu söylenebilir.

Teker (2019) tarafından yapılan çalışmada benzer şekilde, öğretmenlerin bilgi güvenliği farkındalığının branşlara göre anlamlı farklılık gösterdiği sonucuna ulaşılmış, Bilişim Teknolojileri öğretmenlerinin bilgi güvenliği farkındalık puanlarının, ölçeğin tamamında ve alt faktörlerinin tümünde diğer branşlarda görev yapan öğretmenlere göre daha yüksek olduğu bulunmuştur. Özbek'in (2019) eğitim fakültelerinde öğrenim gören öğretmen adaylarının kişisel siber güvenlik sağlama durumlarının incelendiği araştırma bulgularında, "Bilgisayar ve Öğretim Teknolojileri Eğitimi" bölümünde öğrenim gören öğretmen adaylarının Türkçe ve Matematik bölümünde öğrenim görmekte olan öğretmen adaylarından kişisel siber güvenliği sağlama konusunda farkındalık düzeylerinin daha fazla olduğu gözlenmiştir.

4.2.5. Öğretmenlerin Bilgi ve İletişim Teknolojilerine Yönelik Eğitim Alma Durumlarına Göre Siber Güvenliği Sağlama Durumları

Öğretmenlerin siber güvenliği sağlama durumları bilgi ve iletişim teknolojilerine yönelik eğitim (ders ya da kurs) alma durumlarına göre anlamlı bir farklılık gösterip göstermediğini belirlemek amacıyla gerçekleştirilen ilişkisiz örneklemler için t-testi analizi sonuçları Tablo 12'de verilmiştir.

Tablo 12

Öğretmenlerin Bilgi ve İletişim Teknolojilerine Yönelik Ders Alma Durumlarına Göre Siber Güvenliği Sağlama Düzeylerine İlişkin T-Testi Sonuçları

Ölçek alt Faktörleri		N	X̄	S	t	df	P
Kişisel Gizliliği Koruma	Evet	318	39.72	6.05	1.017	453	.310
	Hayır	137	39.12	5.29			
Güvenilmeyenden Kaçınma	Evet	318	16.95	4.41	.831	453	.407
	Hayır	137	16.56	4.79			
Önlem Alma	Evet	318	19.12	4.05	3.302	453	.001*
	Hayır	137	17.77	3.94			
Ödeme Bilgilerini Koruma	Evet	318	8.71	1.98	.382	453	.703
	Hayır	137	8.64	1.84			
İz Bırakmama	Evet	318	15.81	2.94	2.433	453	.015*
	Hayır	137	15.09	2.76			
Ölçek Toplamı	Evet	318	100.31	11.48	2.681	453	.008*
	Hayır	137	97.17	11.43			

*p<.05

Tablo 12 incelendiğinde, öğretmenlerin siber güvenliği sağlama düzeylerinin bilgi ve iletişim teknolojilerine yönelik ders alma durumlarına göre anlamlı bir farklılık gösterdiği belirlenmiştir [t(453)=2.681, P<.05]. Ölçeğin tüm faktörlerinin toplamından elde edilen puanlara göre bilgi ve iletişim teknolojilerine yönelik ders/kurs alan öğretmenlerin (x̄=100.31) siber güvenliği sağlama düzeylerinin, bilgi ve iletişim teknolojilerine yönelik ders/kurs almayan öğretmenlerden (x̄=97.17) daha yüksek düzeyde olduğu belirlenmiştir. Bu durum bilgi ve iletişim teknolojilerine yönelik ders/kurs alan öğretmenlerin siber güvenliği sağlama düzeylerinin, bilgi ve iletişim teknolojilerine yönelik ders/kurs almayan öğretmenlere göre daha yüksek düzeyde olduğunu gösterirken, siber güvenliğin sağlanma düzeyine ile de anlamlı bir ilişkinin olduğu bulgusuna ulaşılmıştır. Gerçekleştirilen analizler sonucunda, ölçeğin Önlem Alma [t(453)=3.302, P<.05] ve İz Bırakmama [t(453)=2.433, P<.05] alt faktörlerinin bilgi ve iletişim teknolojilerine yönelik ders/kurs almalarına göre anlamlı bir farklılık gösterdiği belirlenmiştir. Ancak, ölçeğin Kişisel Gizliliği Koruma [t(453)=1.017, P>.05], Güvenilmeyenden Kaçınma [t(453)=.831, P>.05] ve Ödeme Bilgilerini Koruma [t(453)=-.382, P>.05] alt faktörleri ile öğretmenlerin bilgi ve iletişim teknolojilerine yönelik ders/kurs alma durumları arasında anlamlı bir farklılık gözlenmemiştir.

Siber güvenliği sağlama düzeyi ile bilgi ve iletişim teknolojilerine yönelik ders/kurs alma durumu arasında anlamlı farkın oluşması, araştırmaya katılan öğretmenlerin aldıkları eğitimlerin siber güvenlik farkındalıkları konusunda etkili

olduğunu, farkındalık için eğitim almanın önemini yansıtmaktadır. Benzer şekilde, Yiğit ve Seferoğlu'nun (2019) çalışmasında, "üniversite öğrencilerinin siber güvenlik davranış düzeyleri bilişim güvenliği eğitimi alma durumuna göre incelenmiş" ve ölçeğin tamamından alınan siber güvenlik davranış puanlarının "eğitim alan katılımcıların lehine bir farklılık gösterdiği" bulgusuna ulaşılmıştır. Akgün ve Topal'ın (2015) yaptığı çalışmada ise eğitim fakültesinde öğrenim gören son sınıf öğrencilerinin "bilişim güvenliği" farkındalıklarının, "bilişim güvenliği eğitimi alıp almama durumuna göre" anlamlı bir farklılık göstermediği bulgusuna ulaşılmıştır.

4.2.6. Öğretmenlerin Siber Güvenlik Alanına Yönelik Eğitim Alma Durumlarına Göre Siber Güvenliği Durumları

Öğretmenlerin siber güvenliği sağlama durumlarının siber güvenlik konusunda eğitim alma (ders ya da kurs) durumu göre anlamlı bir farklılık gösterip göstermediğini belirlemek amacıyla gerçekleştirilen ilişkisiz örneklemler için t-testi analizi sonuçları Tablo 13'de verilmiştir.

Tablo 13

Öğretmenlerin Siber Güvenlik Konusunda Eğitim Alma (ders ya da kurs) Durumlarına Göre Siber Güvenliği Sağlama Düzeylerine İlişkin T-Testi Sonuçları

Ölçek alt Faktörleri		N	X̄	S	t	df	p
Kişisel Gizliliği Koruma	Evet	125	39.65	6.88	.241	453	.809
	Hayır	330	39.50	5.40			
Güvenilmeyenden Kaçınma	Evet	125	17.18	4.34	1.024	453	.306
	Hayır	330	16.70	4.59			
Önlem Alma	Evet	125	20.21	3.56	4.950	453	.000*
	Hayır	330	18.15	4.10			
Ödeme Bilgilerini Koruma	Evet	125	8.55	2.05	-.921	453	.357
	Hayır	330	8.74	1.89			
İz Bırakmama	Evet	125	15.96	2.68	1.682	453	.093
	Hayır	330	15.45	2.97			
Ölçek Toplamı	Evet	125	101.55	11.35	2.505	453	.013*
	Hayır	330	98.53	11.52			

*p<.05

Tablo 13 incelendiğinde, öğretmenlerin siber güvenliği sağlama düzeylerinin siber güvenlik alanına yönelik ders alma durumlarına göre anlamlı bir farklılık gösterdiği belirlenmiştir, [t(453)=2.505, P<.05]. Ölçeğin tüm faktörlerinin toplamından elde edilen

puanlara göre siber güvenlik alanına yönelik ders/kurs alan öğretmenlerin ($\bar{X}$=101.55) siber güvenliği sağlama düzeylerinin, siber güvenlik alanına yönelik ders/kurs almayan öğretmenlerden ($\bar{X}$=98.53) daha yüksek düzeyde olduğu belirlenmiştir. Bu durum siber güvenlik alanına yönelik ders/kurs alan öğretmenlerin siber güvenliği sağlama düzeylerinin, siber güvenlik alnına yönelik ders/kurs almayan öğretmenlere göre daha yüksek düzeyde olduğunu gösterirken, siber güvenliğin sağlanma düzeyi ile de anlamlı bir ilişkinin olduğu bulgusuna ulaşılmıştır. Gerçekleştirilen analizler sonucunda, ölçeğin Önlem Alma [t(453)=4.950, P<.05] alt faktörünün siber güvenlik alnına yönelik ders/kurs almalarına göre anlamlı bir farklılık gösterdiği belirlenmiştir. Ancak ölçeğin Kişisel Gizliliği Koruma [t(453)=.241, P>.05], Güvenilmeyenden Kaçınma [t(453)=1.024, P>.05] ve Ödeme Bilgilerini Koruma [t(453)=-.921, P>.05] ve İz Bırakmama [t(453)=1.682, P>.05] alt faktörleri ile öğretmenlerin siber güvenlik alanına yönelik ders/kurs alma durumları arasında anlamlı bir farklılık gözlenmemiştir. Siber güvenliği sağlama düzeyi ile siber güvenlik alanına yönelik ders/kurs alma durumu arasında anlamlı farkın oluşması, araştırmaya katılan öğretmenlerin bu konuda aldıkları eğitimlerin etkili olduğunu, siber güvenlik farkındalığının oluşması için siber güvenlik alnına yönelik eğitimlerin önemli ve bu konu ile doğrudan ilişkili olduğunu göstermektedir.

Benzer şekilde Karacı ve diğerlerinin (2017) çalışmalarında, siber güvenlik davranışlarının katılımcıların "bilgisayar ya da internet güvenliğine yönelik alınan eğitim veya iş deneyimine göre" değişimi incelenmiş, bu konuda eğitim alan katılımcılar, eğitim almayan katılımcılara göre, siber güvenlik davranışları arasında "kişisel gizliliği koruma, önlem alma faktörleri ve ölçeğin tümüne ait puanları" arasında istatistiksel açıdan anlamlı bir fark bulunmuştur.

4.2.7. Öğretmenlerin Sahip Oldukları Teknolojilere Göre Siber Güvenliği Sağlama Durumları

Öğretmenlerin siber güvenliği sağlama durumlarının sahip oldukları teknolojilere göre anlamlı bir farklılık gösterip göstermediğini belirlemek amacıyla gerçekleştirilen ilişkisiz örneklemler için t-testi analizi sonuçları Tablo 14'te verilmiştir.

Tablo 14

Öğretmenlerin Sahip Oldukları Teknolojilere Göre (Bilgisayar/Tablet/Akıllı Telefon) Siber Güvenliği Sağlama Düzeylerine İlişkin T-Testi Sonuçları

Teknoloji	Durum	N	$\bar{X}$	S	t	df	p
Bilgisayar	Evet	443	99.71	11.41	3.950	453	.000*
	Hayır	12	86.58	9.04			
Tablet	Evet	297	100.99	11.60	4.217	453	.000*
	Hayır	158	96.29	10.80			
Akıllı Telefon	Evet	445	99.43	11.47	.821	453	.412
	Hayır	10	12.42	14.69			

*p<.05

Öğretmenlerin siber güvenliği sağlama düzeylerinin öğretmenlerin sahip oldukları teknolojilere göre anlamlı bir farklılık gösterip göstermediği incelenmiş, Tablo 13'e bakıldığında, bilgisayar [t(453)=3.950, P<.05] ve tablete [t(453)=4.217, P<.05] sahip olmanın siber güvenliği sağlama düzeyleri arasında anlamlı bir farklılık gösterdiği belirlenmiştir. Bilgisayara sahip olan öğretmenlerin ortalama puanı ($\bar{X}$=99.71) bilgisayara sahip olmayan öğretmenlerin ortalama puanından ($\bar{X}$=86.58) daha yüksek düzeyde olduğu belirlenmiştir. Tablete sahip olan öğretmenlerin ortalama puanı ($\bar{X}$=100.99) tablete sahip olmayan öğretmenlerin ortalama puanından ($\bar{X}$=96.29) daha yüksek düzeyde olduğu belirlenmiştir. Akıllı telefona sahip olan öğretmenlerin ortalama puanı ($\bar{X}$=99.43) akıllı telefona sahip olmayan öğretmenlerin ortalama puanından ($\bar{X}$=12.42) daha yüksek düzeyde olduğu belirlenmiştir. Bu durum bilgisayar ve tablete sahip olan öğretmenlerin siber güvenliği sağlama düzeylerinin, bilgisayar ve tablete sahip olmayan öğretmenlere göre daha yüksek düzeyde olduğunu gösterirken, siber güvenliğin sağlanma düzeyi ile de anlamlı bir ilişkinin olduğu bulgusuna ulaşılmıştır. Ancak, akıllı telefona [t(453)=.821, P>.05] sahip olmanın siber güvenliği sağlama düzeyleri arasında anlamlı bir farklılık göstermediği belirlenmiştir. Siber güvenliği sağlama düzeyi ile bilgisayar ve tablete sahip olma arasında anlamlı farkın oluşmasında, akıllı telefonun günümüzde hemen herkes tarafından kullanılıyor olması ancak bilgisayar ve tablet kullanımının bilişim alanında daha çok üreten, internet bağlantısı ile diğer cihazlarla etkileşim halinde olan kişilerce kullanılması, bu kişilerin de kayıtlı verilerini korumaları gerektiği için siber güvenlik konusunda kendilerini geliştirmiş olmalarının etkili olduğu söylenebilir.

Yılmaz, Şahin ve Akbulut'un (2016), öğretmenlere yönelik gerçekleştirdikleri, dijital veri güvenliği farkındalıklarını inceledikleri araştırmada, öğretmenlerin bilgisayar,

tablete, bilgisayara veya akıllı telefona göre farklılık gösterip göstermediğini incelemişlerdir. Öğretmenlerin, bu teknolojilere sahip olanlarının olmayanlara göre farkındalık düzeyleri anlamlı derecede daha yüksek olarak bulunmuştur.

4.3. Ortaokul Kademesinde Görev Yapan Öğretmenlerin Siber Güvenlik Farkındalık Düzeylerinin Artırılmasına Yönelik Önerileri

Araştırmaya katılan öğretmenlerin siber güvenlik farkındalık düzeyinin artırılmasına yönelik önerileri Tablo 15'te verilmiştir.

Tablo 15

Öğretmenlerin Siber Güvenlik Farkındalık Düzeyinin Artırılmasına Yönelik Önerileri

	f	%
1. Gerekli güvenlik önlemlerinin alınması ve gerekli uygulamaların kullanılması için insanlar bilinçlendirilebilir.*	23	17.6
2. Kişisel bilgi gizliliğinin güvence altına alınması için konu ile ilgili yasal yaptırımlar artırılabilir.*	22	16.8
3. Kişisel bilgi iletişim teknoloji araçları daha güvenli hale getirilebilir.*	20	15.3
4. Üniversiteler ve halk eğitim kurslarında eğitimler verilebilir.*	19	14.5
5. İnternet hizmetlerinde güvenlik ön planda tutulabilir.*	18	13.7
6. Teknolojik aletlere virüs koruma programları yüklenebilir.*	12	9.2
7. İlkokuldan itibaren müfredata bu konu ile ilgili ders koyulabilir.*	9	6.9
8. Çocukların kullanım alanına yönelik kısıtlamalar yapılabilir.*	8	6.1

Öğretmenlerin, toplumda siber güvenlik farkındalık düzeyini artırmaya yönelik önerileri incelendiğinde, öncelik sıralamaları birbirinden farklı olsa da birçok önerinin ortak noktalarda birleştiği görülmektedir. Çalışma sonucunda siber güvenlik farkındalık düzeyini artırmaya yönelik, gerekli güvenlik önlemlerinin alınması ve gerekli uygulamaların kullanılması için insanların bilinçlendirilmesi (*f*=23, %=17.6) ile ilgili bilinç ve tedbir amaçlı önerileri öğretmenlerin sıklıkla paylaştığı görülmektedir.

Siber güvenlik ile ilgili yaşanan birçok sorunun insanların konu ile ilgili bilgi ve bilinç seviyesinin çok az olmasından kaynaklandığı söylenebilir. Bu konuda Matematik Öğretmeni (k74), "İlkokuldan başlayarak veli ve öğrenciler bilinçlendirilmeli." şeklinde önerisini belirtirken Fen Bilimleri Öğretmeni (k222), "Bilinçli bireyler yetiştirmek." şeklinde siber güvenlik ile ilgili bilinçli olmanın önemine değinmektedir. Sosyal Bilgiler Öğretmeni ise (k342), "Medyada insanlara yönelik daha fazla uyarıların yer alması." şeklinde önerisini belirtirken Türkçe Öğretmeni (k233), "Tüm medyada toplum bilinçlendirilmeli." şeklinde siber güvenlik ile ilgili bilgilendirme ve bilinçlendirme çalışmalarında medyanın önemini vurgulamaktadır. Öğretmenlerin siber güvenlik düzeyini artırmaya yönelik diğer önerileri incelendiğinde;

- Kişisel bilgi gizliliğinin güvence altına alınması için konu ile ilgili yasal yaptırımlar artırılabilir (*f*=22, *%*=16.8)
- Kişisel bilgi iletişim teknoloji araçları daha güvenli hale getirilebilir (*f*=20, *%*=15.3)
- Üniversiteler ve halk eğitim kurslarında eğitimler verilebilir (*f*=19, *%*=14.5)
- İnternet hizmetlerinde güvenlik ön planda tutulabilir (*f*=18, *%*=13.7)
- Teknolojik aletlere virüs koruma programları yüklenebilir (*f*=12, *%*=9.2)
- İlkokuldan itibaren müfredata bu konu ile ilgili ders koyulabilir (*f*=9, *%*=6.9)
- Çocukların kullanım alanına yönelik kısıtlamalar yapılabilir (*f*=8, *%*=6.1)

doğrultusunda çeşitli öneriler sunmaktadırlar. Görüş bildiren öğretmenler siber güvenlik ile ilgili meydana gelen problemlerin bu öneriler dikkate alınarak hareket edildiğinde tüm toplumda azalacağını belirtmektedirler.

BÖLÜM 5

SONUÇLAR VE ÖNERİLER

Bu bölümde araştırmadan elde edilen sonuçlar ile araştırmacılara yönelik öneriler yer almaktadır.

5.1. Sonuçlar

Bu bölümde araştırmanın amacı ve oluşan bulgular doğrultusunda çalışmadan elde edilen sonuçlar başlıklar halinde verilmiştir.

5.1.1. Ortaokul Kademesinde Görev Yapan Öğretmenlerin Siber Güvenlik Farkındalık Düzeylerine İlişkin Sonuçlar

Öğretmenlerin kişisel siber güvenliği sağlama durumlarına ilişkin verdikleri cevaplara bakılarak, kişisel siber güvenliği sağlama düzeylerini belirlemeye yönelik ölçekten ortalamanın üstünde puan aldıkları sonucuna ulaşılmıştır. Yine ölçeğin "Kişisel Gizliliği Koruma, Güvenilmeyenden Kaçınma, Önlem Alma, Ödeme Bilgilerini Koruma ve İz Bırakmama" alt faktörlerinden de alınan puanların ortalamanın üstünde olduğu görülmektedir. Ölçeğin tamamından ve tüm alt faktörlerinden çıkarılan sonuç, öğretmenlerin kişisel siber güvenlik farkındalıklarının yeterli düzeyde olduğudur.

5.1.2. Ortaokul Kademesinde Görev Yapan Öğretmenlerin Demografik Özelliklerine Göre Siber Güvenlik Farkındalık Durumlarına İlişkin Sonuçlar

Yapılan araştırmada ortaokul öğretmenlerinin siber güvenlik farkındalık durumları demografik özelliklerine göre değerlendirilmiştir. Öğretmenlerin siber güvenlik farkındalık durumları; cinsiyet, yaş, görev yılı, branş, bilgi ve iletişim teknolojilerine yönelik ders alma durumları, siber güvenlik alanına yönelik ders alma durumları ve sahip oldukları teknolojilere göre incelenmiştir. Bu değişkenlere göre ortaya çıkan sonuçlar:

- Ölçeğin tüm faktörlerinin toplamından elde edilen puanlara göre kadın öğretmenlerin siber güvenliği sağlama düzeylerinin erkek öğretmenlerden daha yüksek düzeyde olduğu belirlenmiştir. Bu durum kadın öğretmenlerin siber güvenliği sağlama düzeylerinin erkek öğretmenlere göre daha yüksek düzeyde olduğunu gösterse de cinsiyet ile siber güvenliğin sağlanma düzeyi arasında anlamlı bir ilişkinin olmadığı sonucuna ulaşılmıştır.
- Öğretmenlerin kişisel siber güvenliği sağlama düzeylerinin yaşlarına göre anlamlı bir farklılık göstermediği sonucuna ulaşılsa da yaş gruplarına göre kişisel siber güvenliği sağlama durumları özellikle 36-40 yaş aralığındaki öğretmenlerin ölçeğin tamamı ve alt faktörlerinin çoğunda diğer yaş gruplarına göre puanları daha yüksek olarak bulunmuştur. 36-40 yaş gurubu öğretmenlerin sonrasında ve öncesinde yer alan yaş gruplarında kademeli olarak kişisel siber güvenliği sağlama düzeylerinin düşüşe geçtiği ve 50 üstü yaş gurubunun düşük puana sahip olduğu sonucuna ulaşılmıştır. Kişisel siber güvenliği sağlama durumlarına ilişkin ölçeğin alt faktörlerinde ise; Kişisel Gizliliği Koruma, Önlem Alma ve İz Bırakmama alt faktörlerinde anlamlı bir farklılığın olmadığı, ancak ölçeğin Güvenilmeyenden Kaçınma ve Ödeme Bilgilerini Koruma alt faktörlerinde kişisel siber güvenliği sağlama düzeylerine göre anlamlı bir farklılığın ortaya çıktığı saptanmıştır. Güvenilmeyenden kaçınma alt faktöründe ortaya çıkan sonucun 50 yaş üstü öğretmenlerin 40 yaş altı tüm guruplarla farklılık gösterdiği, Ödeme Bilgilerini Koruma alt faktöründe ise farklılığı 46-50 ile <30 ve 36-40 guruplarından kaynaklandığı sonucuna ulaşılmıştır.
- Öğretmenlerin kişisel siber güvenliği sağlama düzeylerinin görev yıllarına göre anlamlı bir farklılık göstermediği belirlenmiştir. Öğretmenlerin kişisel siber güvenliği sağlama düzeylerine ilişkin ortalama puanları görev yıllarına bağlı olarak anlamlı bir şekilde değişmemektedir. Kişisel siber güvenliği sağlama durumlarına ilişkin ölçeğin alt faktörlerinin, öğretmenlerin görev yılları ve kişisel siber güvenliği sağlama düzeylerine göre farklılık gösterip göstermediği incelenerek alt faktörlerin de tamamında anlamlı bir farklılığın olmadığı sonucuna ulaşılmıştır.
- Öğretmenlerin kişisel siber güvenliği sağlama düzeylerinin branşlarına göre anlamlı bir farklılık gösterdiği belirlenmiştir. Öğretmenlerin branşlarına göre kişisel siber güvenliği sağlama durumları incelendiğinde Bilişim Teknolojileri

branşındaki öğretmenlerin kişisel siber güvenliği sağlama düzeylerine ilişkin puanlarının ölçeğin tamamında diğer branştaki öğretmenlere göre daha yüksek olduğu sonucuna ulaşılmıştır. Ölçeğin çoğu alt faktöründe en yüksek ortalama puanı Bilişim Teknolojileri branşındaki öğretmenlere, en düşük ortalama puanın ise Görsel Sanatlar branşındaki öğretmenlere aittir. Ayrıca bütün alt faktörlerde kişisel siber güvenliği sağlama düzeylerine göre anlamlı bir farklılık olduğu sonucu çıkmıştır. Ölçeğin tamamında ise Bilişim Teknolojileri branşının diğer tüm gruplarla farklılık göstermektedir.

- Öğretmenlerin siber güvenliği sağlama düzeyleri bilgi ve iletişim teknolojilerine yönelik eğitim alma durumlarına göre anlamlı bir farklılık göstermektedir. Ölçeğin tüm faktörlerinin toplamından elde edilen puanlara göre bilgi ve iletişim teknolojilerine yönelik ders/kurs alan öğretmenlerin siber güvenliği sağlama düzeylerinin, bilgi ve iletişim teknolojilerine yönelik ders/kurs almayan öğretmenlerden daha yüksek düzeyde olduğu belirlenmiştir.
- Öğretmenlerin siber güvenliği sağlama düzeyleri siber güvenlik alanına yönelik ders alma durumlarına göre anlamlı bir farklılık göstermektedir. Ölçeğin tüm faktörlerinin toplamından elde edilen puanlara göre siber güvenlik alanına yönelik ders/kurs alan öğretmenlerin siber güvenliği sağlama düzeyleri, siber güvenlik alanına yönelik ders/kurs almayan öğretmenlerden daha yüksek düzeydedir.
- Öğretmenlerin siber güvenliği sağlama düzeylerinin öğretmenlerin sahip oldukları teknolojilere göre anlamlı bir farklılık gösterip göstermediği incelenerek, bilgisayar ve tablete sahip olmanın siber güvenliği sağlama düzeyleri arasında anlamlı bir farklılık gösterdiği sonucuna ulaşılmıştır. Bilgisayara, tablete ve akıllı telefona sahip olan öğretmenlerin ortalama puanı, bu teknolojilere sahip olmayan öğretmenlerin ortalama puanından daha yüksek düzeydedir.

5.1.3. Ortaokul Kademesinde Görev Yapan Öğretmenlerin Siber Güvenlik Farkındalık Düzeylerini Artırmaya Yönelik Önerilerine İlişkin Sonuçlar

"Öğretmenlerin, siber güvenlik düzeyinin artırılmasına yönelik önerileriniz nelerdir?" sorusuna çok çeşitli cevaplar verdikleri görülmüştür. Ancak, bu cevapların; gerekli güvenlik önlemlerinin alınması ve gerekli uygulamaların kullanılması için

insanlar bilinçlendirilebilir, kişisel bilgi gizliliğinin güvence altına alınması için konu ile ilgili yasal yaptırımlar artırılabilir, kişisel bilgi iletişim teknoloji araçları daha güvenli hale getirilebilir, üniversiteler ve halk eğitim kurslarında eğitimler verilebilir, İnternet hizmetlerinde güvenlik ön planda tutulabilir, teknolojik aletlere virüs koruma programları yüklenebilir, ilkokuldan itibaren müfredata bu konu ile ilgili ders koyulabilir, çocukların kullanım alanına yönelik kısıtlamalar yapılabilir, önerileri altında birleştiği görülmüştür. Öğretmenlerin, bu öneriler doğrultusunda hareket edildiğinde toplumda yaşanan siber güvenlik sorunlarının azalacağı görüşünde oldukları sonucuna ulaşılmıştır.

5.2.Öneriler

Bu bölümde araştırmanın sonuçlarına dayalı olarak uygulamaya yönelik ve daha sonra yapılacak araştırmalara yönelik geliştirilen önerilere yer verilmektedir.

5.2.1. Uygulamaya Yönelik Öneriler

Araştırma sonucunda elde edilen sonuçlar ışığında uygulamaya yönelik belirlenen sorunların giderilmesi için geliştirilen öneriler aşağıda verilmiştir.

- Araştırma sonucunda bilgi ve iletişim teknolojileri ile siber güvenlik konusunda eğitim alan öğretmenlerin durumlarına bakıldığında, eğitim alan öğretmenlerin farkındalıklarının daha yüksek olduğu sonucuna ulaşılmıştır. Bu sonuçtan hareketle siber güvenlik farkındalığının artırılmasına yönelik başta öğretmenler olmak üzere okuldaki tüm paydaşlara eğitim verilmesi gerektiği söylenebilir.
- Siber Güvenlik alanında verilecek eğitimler, kurumda görevli tüm öğretmenlere aynı anda verilmemesi yaş, branş, daha önce bu konuda eğitim alınma durumları gözetilerek ayrı ayrı gruplandırılarak verilmelidir. Daha önce eğitim alan öğretmenlere yönelik ileri seviye farkındalık eğitimleri gerçekleştirilebilir.
- Araştırma sonucunda 50 yaş üstü öğretmenlerin siber güvenlik farkındalığının düşük olmasından hareketle öğretmenlerin yaşları gözetilerek daha deneyimli öğretmenlere farkındalık eğitimlerinin daha sık verilmesi, gereksinimlerini karşılayacak bir içerikte, uygun yöntem ve değerlendirme yaklaşımları esas alınarak düzenlenmelidir.

- Üniversitelerdeki eğitim fakültelerinin öğretim programlarında siber güvenlik farkındalığının oluşmasına katkı sağlayacak derslere yer verilmelidir.
- Araştırma sonucunda Bilişim Teknolojileri Öğretmenlerinin diğer branşlardaki öğretmenlere göre farkındalık düzeylerinin daha yüksek olduğu sonucuna ulaşılmıştır. Bu sonuçtan hareketle Bilişim Teknolojileri öğretmenlerinin, kurumdaki diğer paydaşlara siber güvenlik farkındalığının artırılmasına yönelik eğitimler verilmeleri ve rehberlik etmeleri sağlanabilir.
- Araştırma sonucunda öğretmenlerin siber güvenlik farkındalığının artırılmasına yönelik önerilerinin çok büyük çoğunluğunun konu ile ilgili yasal yaptırımların artırılması, bilgi iletişim teknoloji araçlarının daha güvenli hale getirilmesi ve üniversiteler ve halk eğitim kurslarında eğitimler verilmesi gerektiği sonucuna ulaşılmıştır. Bu sonuçtan hareketle siber güvenlik kurumlarının yasal yaptırımlar, bilgi iletişim teknolojilerinin daha güvenli hale getirme ve eğitim kurumlarının farkındalığın artırılmasına yönelik eğitimler için çalışmalar gerçekleştirilmelidir.

5.2.2. Araştırmacılara Yönelik Öneriler

Bu araştırma ile ortaokul öğretmenlerinin siber güvenlik farkındalık düzeyleri çeşitli değişkenler aracılığıyla değerlendirilmiştir. Araştırma sonucunda elde edilen sonuçlar ışığında araştırmacılara yapılan öneriler aşağıda verilmiştir.

- Yapılan bu araştırma Ankara ilindeki ortaokul öğretmenleri ile sınırlandırılmıştır. Türkiye'nin farklı bölgelerindeki okullarda siber güvenlik farkındalığına yönelik araştırmalar yapılarak ülke genelindeki duruma bakılabilir.
- Yapılan araştırmada öğretmenlerin kişisel siber güvenliği sağlama düzeylerinin yaşlarına göre anlamlı bir farklılık göstermediği sonucuna ulaşılsa da özellikle 36-40 yaş aralığındaki öğretmenlerin ölçeğin tamamı ve alt faktörlerinin çoğunda puanlarının daha yüksek olduğu ayrıca 50 yaş üstü öğretmenlerin bazı alt faktörlerde puanlarının düşük olduğu ve 40 yaş altı tüm gruplarla anlamlı bir farklılık gösterdiği sonucuna ulaşılmıştır. Bu sonuçlardan hareketle bu farklılıkların sebeplerinin oluşturan unsurların detaylı bir araştırması yapılabilir.
- Öğretmenlerin siber güvenlik farkındalıkları ile günlük internet kullanımları, bilgisayar, tablet gibi teknolojileri kullanmaya başladıkları süre, siber zorba ve mağdur olma durumları gibi değişkenlerle arasındaki ilişki incelenebilir.

- Bu araştırma, ortaokul öğretmenleri üzerinde gerçekleştirilmiştir. Benzer bir araştırma diğer okul kademelerinde görev yapan öğretmenler için yapılabilir.
- Bu araştırmadan elde edilen sonuçlar bir ölçek uygulamasıyla elde edilmiş nicel verilerdir. Araştırmacılar görüşme ve gözlem gibi nitel veri toplama yöntemlerini kullanarak daha derinlemesine ve ayrıntılı bulgulara ulaşabilir.

KAYNAKLAR

Akgün, Ö. E. 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

Akın, O., Çınar, I., Karaman, M., & Bilekyiğit, F. (2013, September). *Siber Durum Farkındalığını Artırmada Etkili Bir Yöntem: Bayrağı Yakala (Capture the Flag*). In 6th International Conference on Information Security and Cryptology, Ankara. Erişim adresi: https://www.iscturkey.org/assets/files/2016/03/2013-paper19.pdf

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. Erişim adresi: https://www.researchgate.net/publication/330278948_Iletisim_Fakultesi_Ogrencilerinin_Siber_Guvenlik_Farkindaligi_Inonu_Universitesi_Ornegi

Aktan, C.C. ve Tunç, M. (1998). Bilgi Toplumu ve Türkiye. *Yeni Türkiye,* 118-134. Erişimadresi:https://www.researchgate.net/publication/318672963_BILGI_TOPLUMU_VE_TURKIYE

Aktan, C. C. ve Vural, İ. (2016). Bilgi Toplumu, Yeni Temel Teknolojiler ve Yeni Ekonomi. *Yeni Türkiye Bilim ve Teknoloji Özel Sayısı, 88*(1), 1-37. Erişim adresi: https://www.researchgate.net/publication/318673064_BILGI_TOPLUMU_YENI_TEMEL_TEKNOLOJILER_VE_YENI_EKONOMI

Alkan, C. (1987). *Eğitim Teknolojisi* (8. Baskı). Ankara: Anı Yayıncılık.

Alkan, C. (1998). *Eğitim Teknolojisi*. Ankara: Anı Yayıncılık.

Aliusta, C. ve Benzer, R. (2018). Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, 4*(2), 35-42. doi: 10.18640/ubgmd.512829

Alp, Ö. (2018). *Akıllı Şehirlerde Siber Güvenlik* (Yayımlanmamış Yüksek Lisans Tezi). İstanbul Bilgi Üniversitesi, İstanbul, Türkiye.

Balcı, A. (2010). *Sosyal Bilimlerde Araştırma Yöntem, Teknik ve İlkeler* (8. baskı). Ankara: Pegem Yayınları.

Barutçugil, İ. (2002). *Bilgi Yönetimi.* İstanbul: Kariyer Yayınları.

Bedük, A. ve Balcılar, H. (2009). Türkiye'nin Bilgi Toplumu Olma Yolunda Bilgi Teknolojilerinden İnternetin Kullanımı: Muş İlindeki İnternet Kafe Kullanıcılarının Amaçları Üzerinde Bir Araştırma. *Sosyal Ekonomik Araştırmalar Dergisi,* 8(16), 82-106. Erişim adresi: https://dergipark.org.tr/tr/pub/susead/issue/28423/302681

Bıçakcı, S., Ergun, D. ve Çelikpala, M. (2015). Türkiye'de Siber Güvenlik. S. Ülgen ve EDAM (Editörler), *Türkiye'de Siber Güvenlik ve Nükleer Enerji.* (ss. 28-73). İstanbul: İmak Ofset Basım Yayın.

Blurton, C. (1999); New directions in education. M. Tawfik, G. Bartagnon & Y. Courrier (Eds.), *World communication and in formation report* (pp. 46-61). France: UNESCO.

Bölükoğlu, H. İ. (2002). Bilgi Çağında Eğitim Fakültelerinde Resim İş Eğitiminin Genel Bir Değerlendirmesi. *Gazi Üniversitesi Gazi Eğitim Fakültesi Dergisi*, *22*(3), 247-259. Erişim adresi: http://www.gefad.gazi.edu.tr/tr/pub/issue/6764/91010

Buch, R., Ganda, D., Kalola, P., & Borad, N. (2017). World of Cyber Security and Cybercrime. *STM Journals*, *4*(2), 18-23. Erişim adresi: https://www.researchgate.net/publication/327110771_World_of_Cyber_Security_and_Cybercrime

Bulu, Ş., Kavuk, M., & Keser, H. (2017). Pre-service ICT teachers' recommendations for school internet safety. M. Simonson & d. Seepersaud (Eds.), *The Association for Educational Communications and Technology*, (pp. 93-97). Abstract retrieved from: https://eric.ed.gov/?id=ED580817

Bulu, Ş. ve Keser, H. (2019). *Eğitim 4.0 ve Eğitimde Dönüşüm.* A. İşman, H. F. Odabaşı ve B. Akkoyunlu (Editörler), Eğitim Teknolojileri Okumaları. (ss. 203-221). Ankara: Pegem Akademi.

Bulut, E. ve Akçacı, T. (2017). Endüstri 4.0 ve İnovasyon Göstergeleri Kapsamında Türkiye Analizi. *ASSAM Uluslararası Hakemli Dergi*, 7, 50-72.

Büyüköztürk, Ş. (2011). *Sosyal Bilimler İçin Veri Analizi El Kitabı* (13. Baskı). Ankara: Pegem Akademi.

Büyüköztürk Ş., Kılıç Ç. E., Akgün Ö. E., Karadeniz Ş. ve Demirel F. (2018). *Bilimsel Araştırma Yöntemleri* (23. Baskı). Ankara: Pegem Akademi.

Canbay, C. Beydoğan, T. A., (2008, June). *Provıdıng Cyber Securıty And Protectıon Of Crıtıcal Informatıon And Infrastructures: A Road Map For Developıng Countrıes*. International Telecommunications Society 17th Biennial Conference, Montreal, Kanada.

Canbek, G. ve Sağıroğlu, Ş. (2007). Bilgisayar Sistemlerine yapılan Saldırılar ve Türleri: Bir İnceleme. *Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, *23*(1-2), 1-12. Erişim adresi: https://dergipark.org.tr/en/download/article-file/252301

Canadian Centre for Cyber Security glossary (2021). Canada: Canadian Centre for Cyber.

Computer Security Resource Center, (2021). Retrieved from: https://csrc.nist.gov/glossary/term/cybersecurity

Convention on Cybercrime, (2001). European Treaty Series (185), Budapest. Retrieved from:https://www.coe.int/en/web/conventions/full-list/ /conventions/treaty/185?module=treaty-detail&treatynum=185

Creswell, J. W., Plano-Clark, V. L., Gutmann, M. L. and Hanson, W. E. (2003). Advanced Mixed Methods Research Designs, In A. Tashakkori & C. Teddlie (Eds.), *Handbook of Mixed Methods in Social and Behavioral Research*. Thousand Oaks, CA:Sage.

Creswell, J. W. (2005). *Educational Research: Planning, Conducting, and Evaluating Quantitative and Qualitative Research* (2nd ed.). New Jersey: Merrill Prentice Hall.

Creswell, J. W. ve Plano Clark, V. L. (2018). *Designing and Conducting Mixed Method Research* (3.Baskı). CA: Sage Publications.

Çelik, A., Çelen, F. K. ve Seferoğlu, S. S. (2014, Şubat). *Ortaokul Öğrencilerinin İnternet Bağımlılık Düzeylerinin Çeşitli Değişkenler Açısından İncelenmesi*. Akademik Bilişim'14 - XVI. Akademik Bilişim Konferansı Bildirileri, Mersin.

Çetinkaya, L. (2013). *Uyarlanabilir Eğitsel İçerikli Web Ortamlarının Tasarım İlkeleri* (Yayımlanmamış Doktora Tezi). Ankara Üniversitesi, Ankara, Türkiye.

Çetinkaya L, Sütçü SS. The effects of Facebook and WhatsApp on success in English vocabulary instruction. *J Comput Assist Learn.* 2018;34:504–514. doi: 10.1111/jcal.12255

Çokluk, Ö., Şekercioğlu, G., & Büyüköztürk, Ş. (2012). *Sosyal Bilimler İçin Çok Değişkenli İstatistik: SPSS ve LISREL Uygulamaları* (2.Baskı). Ankara: Pegem Akademi.

George, D. & Mallery, P. (2003). *SPSS for Windows step by step: a simple guide and reference*. Boston: Allyn & Bacon.

Çeliktaş, M. S., Sonlu, G., Özgel, S., ve Atalay, Y. (2015). Endüstriyel Devrimin Son Sürümünde Mühendisliğin Yol Haritası. *TMMOB Makine Mühendisleri Odası Mühendis ve Makine Dergisi, 56*(662), 24-24. Erişim adresi: https://www.mmo.org.tr/sites/default/files/fa26017c792a3d4_ek.pdf

Demiraslan, V. ve Elaldı, F. (2017). Kurum ve Kuruluşlarda Bilgi Güvenliği Tehdit ve Önlemleri ile Türk Hukukunda Bilişim Suçlarının Yeri ve Önemi. D. K. Dimitrov, D. Nikoloski & R. Yılmaz (Eds.), *V. International Balkan and Near Eastern Social Sciences Congress Series - Kırklareli / Turkey* (pp. 59-70)

Drucker, P. F. (1993). *Kapitalist Ötesi Toplum*, (B. Çorakçı, Çev.). İstanbul: İnkılap Kitabevi.

Ege Bölgesi Sanayi Odası Raporu. (2015). Sanayi 4.0. Erişim adresi: http://www.ebso.org.tr/tr/dosyalar/yayinlar/ekonomik-raporlar

Erkan, H. (1993). *Bilgi Toplumu ve Ekonomik Gelişme*. Ankara: Türkiye İş Bankası Kültür Yayınları.

Erkan, H. (1998). *Bilgi Toplumu ve Ekonomik Gelişme*. Ankara: Türkiye İş Bankası Kültür Yayınları.

Erkan, H. ve Erkan, C. (2007). "Bilgi Toplumu ve Ekonomik Kalkınma", *Üniversite ve Araştırma Kütüphanecileri Derneği Dergisi*, İstanbul

Erol, O., Şahin, L., Yılmaz, E. ve Haseski, H. İ. (2015). Kişisel Siber Güvenliği Sağlama Ölçeği geliştirme çalışması. *International Journal of Human Sciences,* 12(2), 75-91. doi: 10.14687/ijhs.v12i2.3185

Erol, S. E. (2016). *Siber Güvenlik Farkındalığı İçin Yetenek Tabanlı Dinamik Model* (Yayımlanmamış Yüksek Lisans Tezi). Gazi Üniversitesi, Ankara, Türkiye.

Fox, S. J. (2016). Flying challenges for the future: aviation preparedness-in the face of cyber-terrorism. *Journal of Transportation Security, 9*(3-4), 191-218. doi:10.1007/s12198-016-0174-1

Galbraith, J. K. (1967). *The new industrial state.* Boston: Houghton Mifflin Company

Goodman, S. E. (2008). Critical Information Infrastructure Protection, In Centre of Excellence Defence Against Terrorism (Eds.), *Responses to Cyber Terrorism NATO Science for Piece and Security* (pp. 24-33). Amsterdam, IOS Press.

Goodrich, M. & Tamassia, R. (2011). *Introduction To Computer Security*. London: Pearson.

Goztepe, K., Kılıc, R. & Kayaalp, A. (2014). Cyber defense ın depth: designing cyber security agency organization for Turkey. *Journal of Naval Science and Engineering, 10*(1), 1-24. Abstract retrieved from:

Gökmen, Ö. F. ve Akgün, Ö. E. (2016). Öğretmen Adaylarının Bilişim Suçlarına Yönelik Deneyimleri ve Bilişim Güvenliği Ders İçeriğine Yönelik Görüşleri. *Mustafa Kemal Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 33*(13), 178-193.

Güldüren, C. ve Keser, H. (2017). Bilgi Güvenliği Farkındalık Eğitimi. B. Akkoyunlu, A. İşman ve H.,F. Odabaşı (Editörler), *Eğitim Teknolojileri Okumaları* (ss.33-56). Ankara: Pegem Akademi.

Güven, Y.G., Kalelioğlu, F., Kert, S.B., Kaplan, A., Koçak, B., İliş, E.B.,…Özgür, Y.K. (2017). *5. Sınıflar Bilişim Teknolojileri ve Yazılım Dersi Öğretmen Rehberi*. Erişim adresi: http://tegm.meb.gov.tr/meb_iys_dosyalar/2017_10/03105825_Ogretmen-Rehberi_compressed.pdf

Hekim, H. ve Başıbüyük, O. (2013). Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları. *Uluslararası Güvenlik ve Terörizm Dergisi, 4*(2), 135-158. Erişim adresi: https://app.trdizin.gov.tr/makale/TVRVd09UWTVPUT09/siber-suclar-ve-turkiye-nin-siber-guvenlik-politikalari-

ITU, (2007). Cybersecurity guide for developing countries. Retrieved from: https://www.itu.int/pub/D-STR-SECU-2007

Türk Dil Kurumu. (2019). *Türkçe Sözlük*. Türk Dil Kurumu Sözlükleri

ITU (2008a). Definition of cybersecurity, referring to ITU-T X.1205, Overview of cybersecurity.Retrievedfrom:https://www.itu.int/en/ITUT/studygroups/com17/Pages/cybersecurity.aspx

ITU (2008b, Feb). *Draft Meeting Report: ITU regional workshop on frameworks for cybersecurity and critical information infrastructure protection (CIIP) & cybersecurity forensics workshop*. Regional Cybersecurity Forum, Doha, Qatar. Retrieved from: https://www.itu.int/ITU-D/cyb/events/2008/doha/docs/doha-cybersecurity-forum-report-feb-08.pdf

İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun (2007). 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun. Erişim adresi: https://www.resmigazete.gov.tr/eskiler/2007/05/20070523-1.htm

İşman, A. (2001). Teknolojinin Felsefi Temelleri. *Sakarya Üniversitesi Eğitim Fakültesi Dergisi, 0*(1), 1-19. Erişim adresi: https://dergipark.org.tr/tr/download/article-file/115674

Yılmaz, B. (1998). Bilgi toplumu: Eleştirel bir yaklaşım. *Hacettepe Üniversitesi Edebiyat Fakültesi Dergisi, 15*(1). 147-158. doi: 10.18069/fusbed.72486

İşman, A. (2008). *Uzaktan eğitim*. Ankara: Pegem Akademi.

Karacı, A., Akyüz. H. İ. ve Bilgici, G. (2017). Üniversite Öğrencilerinin Siber Güvenlik Davranışlarının İncelenmesi. *Kastamonu Eğitim Dergisi, 25*(6). 2079-2094. Erişim adresi: 10.24106/kefdergi.351517

Karasar, Ş. (2004). Eğitimde Yeni İletişim Teknolojileri-İnternet ve Sanal Yüksek Eğitim. *The Turkish Online Journal of Educational Technology, 3*(4), 117-125. Erişim adresi: http://www.tojet.net/articles/v3i4/3416.pdf

Kaşıkcı, D. N., Çağıltay, K. ve Karakuş, T. (2014). Türkiye ve Avrupa'daki Çocukların İnternet Alışkanlıkları ve Güvenli İnternet Kullanımı. *Eğitim ve Bilim, 171*(39), 230-243.

Kayri, M. (2009). Araştırmalarda Gruplar Arası Farkın Belirlenmesine Yönelik Çoklu Karşılaştırma (Post-Hoc) Teknikleri. *Journal of Social Science, 19*(1), 51-64. Erişim adresi: https://dergipark.org.tr/en/download/article-file/72000#page=57

KHK, (2016). 671 Sayılı Olağanüstü Hal Kapsamında Bazı Kurum ve Kuruluşlara İlişkin Düzenleme Yapılması Hakkında Kanun Hükmünde Kararname. Erişim adresi: https://www.resmigazete.gov.tr/eskiler/2016/08/20160817-18..htm

Kim, W., Jeong, O. R., Kim, C., & So, J. (2011). The dark side of the Internet: Attacks, costs and responses. *Information systems*, *36*(3), 675-705. doi: 10.1016/j.is.2010.11.003

Klimburg, A. (2012). National cyber security framework manual. *NATO CCD COE Publication*, Tallinn. Retrieved from: https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf

Köklü, N., Büyüköztürk Ş. & Bökeoğlu, Ç.Ö. (2006). *Sosyal Bilimler İçin İstatistik.* Ankara: PegemA Yayıncılık.

Macdougall, W. (2014), *Industrie 4.0: Smart Manufacturing for the Future* (Brochure, 20750). Technical report of Germany Trade and Invest. Retrieved from: https://www.gtai.de/gtai-en/invest/service/publications/industrie-4-0-germany-market-report-and-outlook-64602

MEB, (2019). Erişim adresi: https://sgb.meb.gov.tr/www/icerik_goruntule.php?KNO=424

MEBa, (2021). Erişim adresi: https://www.meb.gov.tr/baglantilar/okullar/index.php?ILKODU=6&ILCEKODU 1

MEBb, (2021) Erişim adresi: http://oygm.meb.gov.tr/www/icerik_goruntule.php?KNO=28

Meder, M. (2001). Bilgi Toplumu ve Toplumsal Değişim. *Pamukkale Üniversitesi Eğitim Fakültesi Dergisi*, *9*(9), 72-81. Erişim adresi: https://dergipark.org.tr/tr/pub/pauefd/issue/11134/133165

Merriam-Webster.com dictionary (n.d.). (2021). Springfield, MA: Merriam-Webster.

Mert, M., H.İ. Bülbül ve Ş. Sağıroğlu (2012). Milli Eğitim Bakanlığına Bağlı Okullarda Güvenli İnternet Kullanımı, *TÜBAV Bilim Dergisi, 5*(4), 1-12. Erişim adresi: https://dergipark.org.tr/tr/download/article-file/200974

OECD Glossary of Statistical Tersms (2002). Paris: OECD.

Olakulehin, F. K. (2007). Information and communication technologies in teacher training and professional development in Nigeria. *Turkish Online Journal of Distance Education*, *8*(1), 133-142. Retrieved from: https://eric.ed.gov/?id=ED494808

On Birinci Kalkınma Planı (2018). T.C. Kalkınma Bakanlığı Bilgi ve İletişim Teknolojileri Özel İhtisas Komisyonu Raporu. Erişim adresi: https://www.sbb.gov.tr/wpcontent/uploads/2020/04/Bilgi_ve_IletisimTeknolojileri OzelIhtisasKomisyonuRaporu.pdf

Öztürk, O. (2014). Digital dark side: cyber warfare (Unpublished master's thesis). Boston University Metropolitan College, Boston, USA. Retrieved from: https://www.btk.gov.tr/uploads/thesis/submitted-in-partial-fulfillment-of-the-requirements-for-the-degree-of-master-of-science-in-administrative-studies-2014.pdf

OWASP, (2017). Retrieved from: https://owasp.org/www-project-top-ten/2017/A1_2017-Injection

Öğüt, A. (2003). *Bilgi Çağında Yönetim*. Ankara: Nobel Yayıncılık.

Öztemel, E. (2018). Eğitimde Yeni Yönelimlerin Değerlendirilmesi ve Eğitim 4.0. *Üniversite Araştırmaları Dergisi, 1*(1), 25-30. doi: 10.26701/uad.371662

Özer, Ö. A. ve Turhan, M. (2019). 4. Sanayi Ve Enformasyon Toplumu Çerçevesinde Kamu Politikalarının Gelişimi. *Yönetim ve Ekonomi Dergisi, 26*(2), 361-375. doi: 10.18657/yonveek.514341

Öğün, M. N. ve Kaya, A. (2013). Siber Güvenliğin Milli Güvenlik Açısından Önemi Ve Alınabilecek Tedbirler. *Güvenlik Stratejileri Dergisi, 9*(18), 145-181.

Özbek, Y. (2019). *Öğretmen Adaylarının Siber Güvenlik Farkındalıklarının İncelenmesi* (Yayımlanmamış Yüksek Lisans Tezi). Necmettin Erbakan Üniversitesi, Konya, Ankara.

Özyurt Ö., Özyurt, H. (2015). A Study For Determining Computer Programming Students' Attitudes Towards Programming And Their Programming Self-Efficacy. *Journal of Theory and Practice in Education, 11*(1), 51-67.

Pamuk, N. ve Soysal, M. (2018). Yeni Sanayi Devrimi Endüstri 4.0 Üzerine Bir İnceleme. *Verimlilik Dergisi,* (1), 41-66. Erişim adresi: https://dergipark.org.tr/tr/pub/verimlilik/issue/34982/388198

Peng, T., Leckie, C., & Ramamohanarao, K. (2007). Survey of network-based defense mechanisms countering the DoS and DDoS problems. *ACM Computing Surveys (CSUR), 39*(1), 1-42. doi: 10.1145/1216370.1216373

Plano Clark, V. L., & Ivankova, N. V. (2016). *Mixed Methods Research: A Guide to the Field*. CA: Sage.

Pusey, P. & Sadera, W.A. (2011). Cyberethics, cybersafety and cybersecurity: Preservice teacher knowledge, preparedness and the need for teacher education to make a difference. *Journal of Digital Learning in Teacher Education, 28*(2), 82-88. Retrieved from: https://files.eric.ed.gov/fulltext/EJ960154.pdf

Roscoe, J. T. (1975). *Fundemental research statistics for the behavioral sciences.* New York: Holt, Rinehart and Winston, Inc.

Rübmann, M., Lorenz, M., Gerbert, P., Waldner, M., Justus, J., Engel, P., & Harnisch, M. (2015). Industry 4.0: The future of productivity and growth in manufacturing industries. *Boston Consulting Group*, *9*(1), 54-89.

Schatz, D., Bashroush, R. & Wall, J. (2017). Towards A More Representative Definition Of Cyber Security. *The Journel of Digital Forensics, Security and Law*, *12*(2), 53-74. Retrieved from: https://commons.erau.edu/jdfsl/vol12/iss2/8

Scheffe, H. (1959). *The analysis of variance*. New York: John Wiley press

Schwab, K. (2015). The Fourth Industrial Revolution What it means and How to Respond. Retrieved from: https://www.foreignaffairs.com/articles/2015-12-12/fourth-industrial-revolution

Semerci, A. (2019a). Eğitim Fakültesi Öğrencileri ile Diğer Fakültelerdeki Öğrencilerin Siber Güvenlik Farkındalıklarının Karşılaştırılması. *Akdeniz Eğitim Araştırmaları Dergisi, 13*(29), 138-156. doi: 10.29329/mjer.2019.210.8

Semerci, A. (2019b, Nisan). *Üniversite Öğrencilerinin Kişisel Siber Güvenlik Davranışlarının Farklı Değişkenler Açısından İncelenmesi.* The Twelfth International Congress of Educational Research, Rize. Erişim adresi: https://www.researchgate.net/publication/333038791_UNIVERSITE_OGRENCILERININ_KISISEL_SIBER_GUVENLIK_DAVRANISLARININ_FARKLI_DEGISKENLER_ACISINDAN_INCELENMESI

Semerci, A. ve Keser, H. (2019). Siber Saldırı Motivasyonları ve Siber Güvenlik. A. İşman, H. F. Odabaşı ve B. Akkoyunlu (Editörler), *Eğitim Teknolojileri Okumaları*. (ss. 579-600). Ankara: Pegem Akademi.

Soylu, A. (2018). Endüstri 4.0 ve Girişimcilikte Yeni Yaklaşımlar. *Pamukkale Üniversitesi Sosyal Bililmler Enstitüsü Dergisi*, 32, 43-57.

Solms, V. R., & Niekerk, V. J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97-102. doi: 10.1016/j.cose.2013.04.004

Schryen, G. (2007). *Anti-spam measures: analysis and design*. Berlin: Springer.

Subramaniam, S. R. (2017). Cyber security awareness among Malaysian pre-university students. *Conference: 6th Global Summit of Education*, Kualalumpur, Malaysia. *Global Summit of Education*, Kualalumpur, Malaysia. Abstract retrieved from: https://scholar.google.com.tr/scholar?q=Subramaniam+2017+Cyber+security+awareness+among+Malaysian+preuniversity+students&hl=tr&as_sdt=0&as_vis=1&oi=scholart

Şahinaslan, E., Kantürk, A., Şahinaslan, Ö. ve Borandağ, E. (2009). Kurumlarda Bilgi Güvenliği Farkındalığı, Önemi ve Oluşturma Yöntemleri. M. Akgül, M. U. Çağlayan, E. Derman ve A. Özgit (Editörler), *Akademik Bilişim '09 -XI.Akademik Bilişim Konferansı Bildirileri.* (ss. 597-602). Erişim adresi: https://ab.org.tr/

Tashakkori, A., Johnson, R. B., & Teddlie, C. (2021). *Foundations of mixed methods research: Integrating quantitative and qualitative approaches in the social and behavioral sciences* (2nd ed.). CA: Sage.

Taşbaşı, A. ve Altınbaşak, (2006). *Bilgi ve İletişim Teknolojisi,* İstanbul: Altaş Yayıncılık.

TCK, (1991). 765 Sayılı Türk Ceza Kanununun Bazı Maddelerinin Değiştirilmesine Dair Kanun. Erişim adresi: https://www.resmigazete.gov.tr/arsiv/20901.pdf

TCK, (2004). 5237 Sayılı Türk Ceza Kanunun İlk Hali. Erişim adresi: https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237-20040926.pdf

Teker, E. (2019). *Öğretmenlerin ve Lise Öğrencilerinin Bilgi Güvenliği Farkındalık Düzeylerinin Değerlendirilmesi* (Yayımlanmamış Yüksek Lisans Tezi). Ankara Üniversitesi, Ankara, Türkiye.

Terörle Mücadele Kanunu (2006). 3713 Sayılı Terörle Mücadele Kanununda Değişiklik Yapılmasına Dair Kanun. Erişim adresi: https://www.resmigazete.gov.tr/eskiler/2006/07/20060718-1.htm

The White House (2008). Retrieved from: https://fas.org/irp/offdocs/nspd/nspd-54.pdf

Tonta, Y. (1999). Bilgi Toplumu ve Bilgi Teknolojisi. *Türk Kütüphaneciliği,* 13(4), 363-375.

Tonta, Y. & Küçük, M.E. (2005). The Turkish General Staff Directorate of Military History, Strategic Studies and Inspection Publications. In A. Erdinç, (Eds.), *Main Dynamics of the Transition from Industrial Society to Information Society. Proceedings of the Third International Symposium on Society, Governance, Management and Leadership Approaches in the Light of the Technological Developments and the Information Age* (pp. 3-16).

Tosun, G., Vural, Z. B. A., Yurdakul, N. B., Çelik, T., Köseoğlu, Ö. ve Yakın, M. (2006). *Bilgi İletişim Teknolojileri ve Yansımaları*. Z. B. Akıncı Vural (Editör), Ankara: Nobel Akademik Yayıncılık.

TÜİK (2020). Erişim adresi: https://data.tuik.gov.tr/Kategori/GetKategori?p=bilgi-teknolojileri-ve-bilgi-toplumu-102&dil=1

Türkiye Bankalar Birliği (2015). Dolandırıcılık Eylemleri ve Korunma Yöntemleri. Erişim adresi: https://www.tbb.org.tr/Content/Upload/Dokuman/7328/TBB-Dolandiricilik-Eylemleri-ve-Korunma-Yontemleri.html

Ulusal Siber Güvenlik Stratejisi (2012). T. C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı ve Bilgi Güvenliği Derneği. Erişim adresi: https://www.researchgate.net/publication/303909502_Turkiye_Ulusal_Siber_Guvenlik_Stratejisi_Onerisi_National_Cyber_Security_Strategy_Proposal_of_Turkey

Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2013). T. C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı. Erişim adresi: https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-plani-2013-2014-5a3412cf8f45a.pdf

Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2016). T. C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı. Erişim adresi: https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf

Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020). T. C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı. Erişim adresi: https://hgm.uab.gov.tr//uploads/pages/siber-guvenlik/ulusal-siber-guvenlik-stratejisi-ep-2020-2023.pdf

UNESCO. (2003). *Developing and using indicators of ICT use in education*. UNESCO Asia and Pacific Regional Bureau for Education, Bankok. Retrieved from: https://unesdoc.unesco.org/ark:/48223/pf0000131124?posInSet=14&queryId=828bf873-b7bb-4cba-829a-3bb168306c0f

Ünal, A.N. ve Ergen, A. (2018). Siber Uzayda Yeterince Güvenli Davranıyor Muyuz? İstanbul İlinde Yürütülen Nicel Bir Araştırma. *Manisa Celal Bayar Üniversitesi Sosyal Bilimler Dergisi. 16*(2), 191-216. doi: 10.18026/cbayarsos.439489

Ünal, Y. (2009). Bilgi Toplumunun Tarihçesi. *Tarih Okulu Dergisi*, (V), 123-144 Erişim adresi: https://dergipark.org.tr/tr/pub/usakjhs/issue/13546/164068

Ünver, M. (2012). Ulusal Siber Güvenliğin Sağlanmasında Farkındalık Çalışmaları. Erişim adresi: https://www.academia.edu/24842057/Ulusal_Siber_G%C3%BCvenli%C4%9Fin_Sa%C4%9Flanmas%C4%B1nda_Fark%C4%B1ndal%C4%B1k_%C3%87al%C4%B1%C5%9Fmalar%C4%B1

Ünver, M., Canbay, C. ve Mirzaoğlu, A. G. (2009). Bilgi Teknolojileri ve İletişim Kurumu. Siber Güvenliğin Sağlanması Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler. Erişim adresi: https://www.btk.gov.tr/uploads/undefined/sg.pdf

Yalın, H. İ. (2012). *Öğretim Teknolojileri ve Materyal Geliştirme* (25.Baskı). Ankara: Nobel Akademik Yayıncılık.

Yayla, H. G. (2018). *Fatih Projesi Uygulanan ve Uygulanmayan Okullardaki Öğretmenlerin Bilgi Güvenliği Farkındalığının İncelenmesi*. (Yayımlanmamış Yüksek Lisans Tezi). Ankara Üniversitesi, Ankara, Türkiye.

Yazıcıoğlu, Y. ve Erdoğan, S. (2007). *Spss Uygulamalı Bilimsel Araştırma Yöntemleri.* Ankara: Detay Yayıncılık.

Yenilmez, K. (2008). Open primary education school students' opinions about mathematics television programmes. *Turkish Online Journal of Distance Education, 9*(4), 176-189.

Yeşilorman, M. ve Koç, F. (2014). Bilgi Toplumunun Teknolojik Temelleri Üzerine Eleştirel Bir Bakış. *Fırat Üniversitesi Sosyal Bilimler Dergisi, 24*(1), 177-133. Erişim adresi: https://dergipark.org.tr/en/download/article-file/157362

Yıldız, M. (2014). *Siber Suçlar ve Kurum Güvenliği* (Yayımlanmamış Uzmanlık Tezi). T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, Ankara, Türkiye.

Yılmaz, E. N., Ulus, H. İ. ve Gönen, S. (2015). Bilgi Toplumuna Geçiş ve Siber Güvenlik. *Bilişim Teknolojileri Dergisi*, 8(3), 133-146. doi: 10.17671/btd.87028

Yılmaz, E., Şahin, L. ve Akbulut, Y. (2016). Öğretmenlerin Dijital Veri Güvenliği Farkındalığı. *Sakarya University Journal of Education, 6*(2), 26-45. doi: 10.19126/suje.29650

Yılmaz, S. (2015). *Siber Güvenliğin Sağlanmasında Yazılım Kalite Süreçlerinin Önemi.* (Yayımlanmamış Yüksek Lisans Tezi). Gazi Üniversitesi, Ankara, Türkiye.

Yılmaz, S. ve Sağıroğlu, Ş. (2013, Eylül). *Siber Güvenlik Risk Analizi, Tehdit ve Hazırlık Seviyeleri.* 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, Ankara. Erişim adresi: https://www.iscturkey.org/assets/files/2016/03/2013-paper81.pdf

Yiğit, M. F. ve Seferoğlu, S. (2019). Öğrencilerin Siber Güvenlik Davranışlarının Beş Faktör Kişilik Özellikleri ve Çeşitli Diğer Değişkenlere Göre İncelenmesi. *Mersin Üniversitesi Eğitim Fakültesi Dergisi, 15*(1), 186-215. doi: 10.17860/mersinefd.437610

Yücel, A. (2003). Sürdürülebilir Kalkınmanın Sağlanmasında Çevre Korumanın ve Ekonomik Kalkınmanın Karşıtlığı ve Birlikteliği. *Çukurova Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 11*(11), 100-120. Erişim adresi: https://dergipark.org.tr/tr/pub/cusosbil/issue/4367/59734

Yüksel, M. (2014). *Bilgi Çağında Değişen Eğitim Paradigmaları Çerçevesinde Öğretmen İstihdamı: Türkiye Örneği* (Yayımlanmamış Yüksek Lisans Tezi). Süleyman Demirel Üniversitesi, Isparta, Türkiye.

We Are Social & Hootsuite (2021). Digital 2021 Global Overview Report. Retrieved from: https://wearesocial.com/digital-2021

Wamala, F. (2011). ITU national cybersecurity strategy guide. *International Telecommunications Union*, Geneva. Retrieved from: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-national-cybersecurity-guide.pdf

EKLER

Ek 1. Kişisel Bilgiler Formu

KİŞİSEL SİBER GÜVENLİĞİ SAĞLAMA ÖLÇEĞİ

Sayın Öğretmenler;

Bu araştırma, sizlerin siber güvenlik konusu ile ilgili farkındalıklarınızı tespit etmek amacıyla yapılmaktadır. İki bölümden oluşan ölçekte, birinci bölümde Kişisel Bilgiler Formu, ikinci bölümde Kişisel Siber Güvenliği Sağlama Ölçeği yer almaktadır. Sizlerden, aşağıda siber güvenlik ile ilgili verilen ifadeleri inceleyerek, uyma ya da uymama durumunuzu belirtmeniz beklenmektedir. Ekteki her bölümü soruları atlamadan, dikkatlice okumanız ve belirtilen ifadelerden size en uygun olanını (X) işareti koyarak işaretlemeniz gerekmektedir. Burada yer alan maddelere, doğru ya da yanlış şeklinde bir değerlendirme yapılmayacak olup araştırmadan elde edilen veriler, sadece bilimsel amaçla kullanılacaktır. İsminizi yazmanıza gerek yoktur.

Katkılarınız için teşekkür ederim. Araştırmacı: İmren ALTINER

Danışman: Prof. Dr. Hafize KESER

Tanımlar

Bilgi İletişim Teknolojileri: Bilginin toplanmasını, işlenmesini, depolanmasını, ağlar aracılığıyla bir yerden bir yere iletilmesini sağlayan iletişim ve bilgisayar teknolojilerini de kapsayan bütün teknolojilerdir.

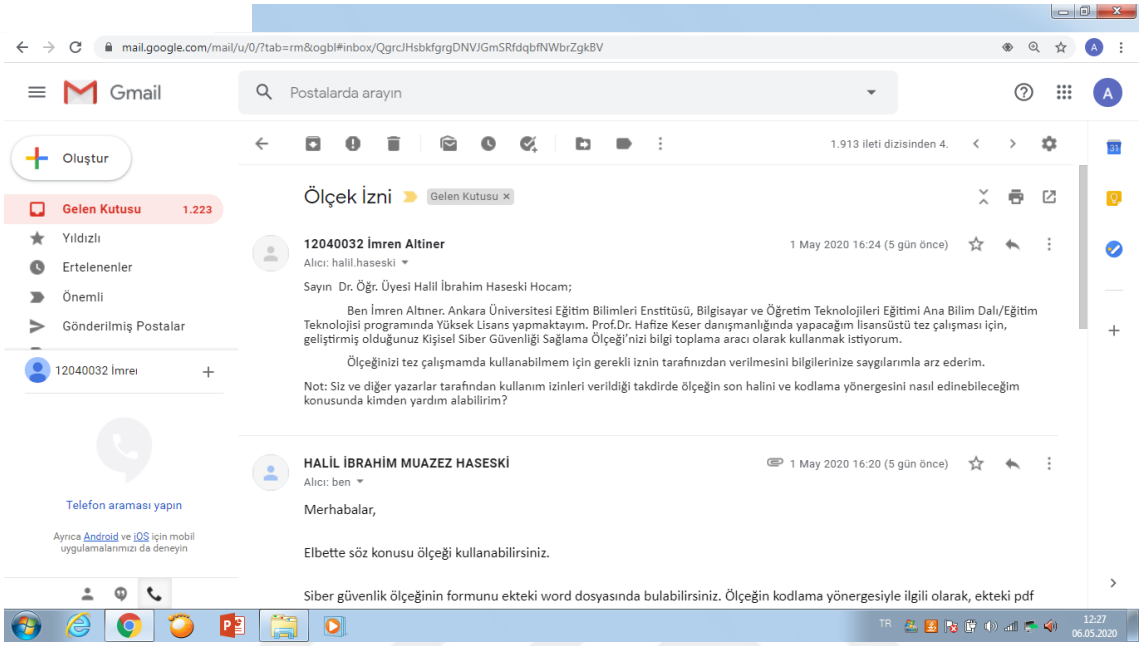
Kişisel Bilgiler Formu

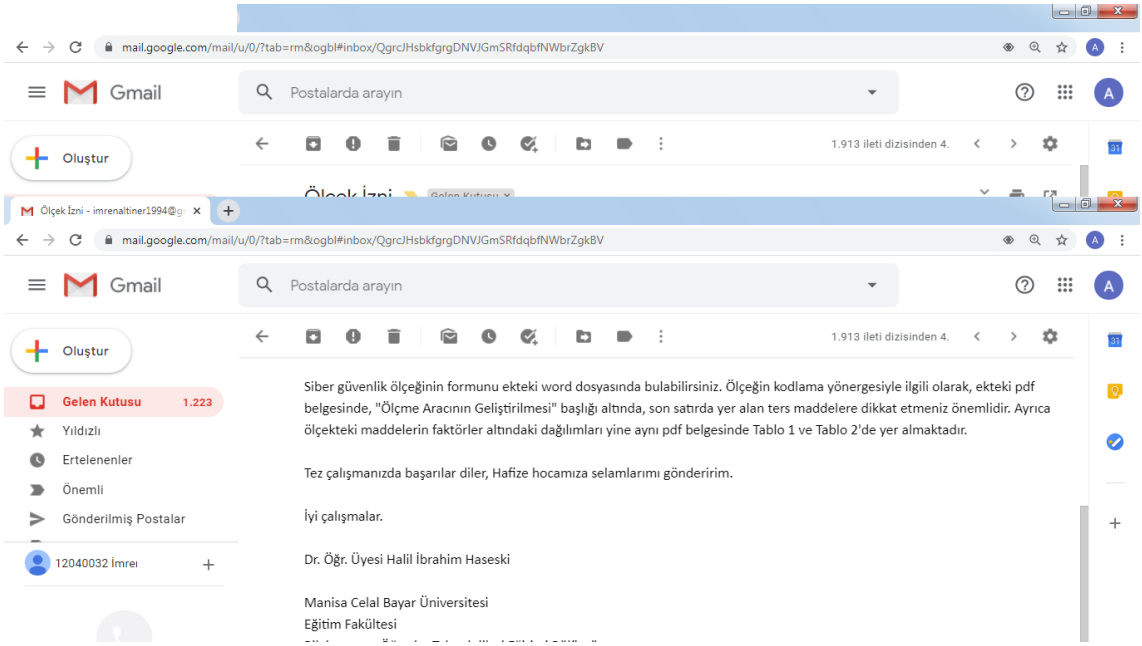
1. Cinsiyetiniz:				
2. Yaşınız:				
3. Mezun olduğunuz okul:				
4. Mesleğinizdeki görev yılınız:				
5. Görev yaptığınız okul türü:	☐ Genel Ortaokul		☐ İmam Hatip Ortaokulu	
6. Branşınız:	☐ Matematik ☐ Türkçe ☐ Fen Bilimleri ☐ Görsel Sanatlar ☐ Beden Eğitimi ☐ Sosyal Bilgiler ☐ Bilişim Teknolojileri ve Yazılım ☐ Diğer			
7. Daha önce bilişim teknolojileri konusunda eğitim (ders, kurs) aldınız mı?	☐ Evet		☐ Hayır	
8. Siber Güvenlik konusunda daha önce eğitim(ders, kurs) aldınız mı?	☐ Evet		☐ Hayır	
9. Sahip olduğunuz bilgi ve iletişim teknolojileri nelerdir? (Birden fazla işaretleyebilirsiniz.)	☐ Bilgisayar	☐ Tablet	☐ Akıllı Telefon	☐ Diğer
10. Hangi sosyal medya ortamlarına üyesiniz? (Belirtiniz, birden fazla yazabilirsiniz.)				
11. Bilgi iletişim teknolojilerini (bilgisayar, telefon, tablet, akıllı telefon vb.)hangi amaçlar için kullanıyorsunuz? (Birden fazla işaretleyebilirsiniz.)	☐ Oyun oynamak	☐ Alanım ile ilgili kendimi geliştirmek	☐ Sosyal medya kullanmak	☐ Gündemi takip etmek ☐ Diğer
12. İnterneti hangi amaçlar için kullanıyorsunuz? (Birden fazla işaretleyebilirsiniz.)	☐ Oyun oynamak	☐ Alanım ile ilgili kendimi geliştirmek	☐ Sosyal medya kullanmak	☐ Gündemi takip etmek ☐ Diğer
13. Siber güvenlik düzeyinin artırılmasına yönelik önerileriniz nelerdir? (Belirtiniz, birden fazla yazabilirsiniz.)				

Ek 2. Kişisel Siber Güvenliği Sağlama Ölçeği

Kişisel Siber Güvenliği Sağlama Ölçeği	1- Hiçbir zaman	2- Naidren	3- Arasıra	4- Sıksık	5- Her zaman
1. Web sayfalarında güvenlik bağlantılarını (https://) ve sertifikalarını kontrol ederim					
2. Kullandığım yazılımları güncellerim					
3. Bilgisayarımda antivirus yazılımı bulundururum					
4. Şifrelerimi belirlerken basit dizilimler kullanmaktan kaçınırım					
5. İnternet şifrelerimin tümünün aynı olmasına dikkat ederim					
6. Web tarayıcımın güvenlik ayarlarını düzenlerim					
7. E- posta ile gelen kimlik doğrulama mesajlarını (kullanıcı adı, şifre vb. istekler) cevaplarım					
8. Şahsi bilgisayarım dışında kullanılan bilgisayarlarda bilgilerimin kalmamasına dikkat ederim					
9. İnternet üzerinden yapılan para ve kontör isteklerini dikkate almam					
10. Tanımadığım kişilerden gelen sosyal ağ arkadaşlık isteğini kabul etmem					
11. Güvenmediğim sitelere üye olmam					
12. Tanımadığım kişiler ile web kamerası kullanarak sesli ve görüntülü iletişim kurarım					
13. İnternet ortamında gerektiğinde kişisel bilgilerimi (TC No,Doğum tarihi,Gsm No vb.) paylaşırım					
14. Web geçmişimi temizlerim					
15. İnternet bankacığı işlemlerini şahsi bilgisayarımdan yaparım.					
16. Online alışveriş işlemlerini şahsi bilgisayarımdan yaparım					
17. Tanımadığım kişilerden gelen e-posta eklerini açarım					
18. Sosyal paylaşım sitelerinde kişisel bilgilerime yer veririm					
19. İnternet üzerinden yer bildirimi yaparım					
20. Sosyal ağlarda yer alan reklamlar üzerinden alışveriş yaparım					
21. Sosyal ağ - e-posta gibi hesaplarda işim bittiğinde oturumu kapatırım					
22. Güvenmediğim sitelerden dosya indirmem					
23. İnternette kullandığım (eposta, sosyal ağ vb.) şifreleri değiştiririm					
24. Unutmamak için akılda kalan kolay bir şifre belirlerim					
25. Banka, online alışveriş sitesi gibi sitelerden gelen e postalara (kart numarası, şifre vb. istekler) itibar ederim ve yanıtlarım					

Ek 3. Ölçek Kullanma İzni





Ek 4. Etik Kurul İzni

ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ALT ETİK KURULU
KARAR ÖRNEĞİ

Karar Tarihi : **25/05/2020**
Toplantı Sayısı : **4**
Karar Sayısı : **84**

84- Üniversitemiz Eğitim Bilimleri Enstitüsü Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı yüksek lisans öğrencisi **İmren Altıner**'in "Öğretmenlerin Kişisel Siber Güvenlik Farkındalık Düzeylerinin Farklı Değişkenlere Göre Değerlendirilmesi" başlıklı tezi ile ilgili 07/05/2020 tarihli "İnsan Üzerinde Yapılan Klinik Dışı Araştırmalar Başvuru Formu" Etik Kurulumuzca incelendi.

Üniversitemiz Eğitim Bilimleri Enstitüsü Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı yüksek lisans öğrencisi **İmren Altıner**'in "Öğretmenlerin Kişisel Siber Güvenlik Farkındalık Düzeylerinin Farklı Değişkenlere Göre Değerlendirilmesi" başlıklı tezinin, araştırma protokolüne uyulması ve etik onay tarihinden itibaren geçerli olması koşuluyla uygulanmasının etik açıdan uygun olduğuna oy birliği ile karar verildi.

Ek 5. Millî Eğitim Bakanlığı Araştırma İzni

T.C.
ANKARA ÜNİVERSİTESİ REKTÖRLÜĞÜ
Eğitim Bilimleri Enstitüsü Müdürlüğü
Enstitü Sekreterliği
ÖĞRENCİ İŞLERİ

Sayı : 98761816-302.08.01-E.37491 12.02.2021

Konu : İmren ALTINER'in Uygulama İzni Hk.

ANKARA İL MİLLİ EĞİTİM MÜDÜRLÜĞÜNE

İlgi : İmren ALTINER'in 05.02.2021 tarihli başvurusu.

Enstitümüz Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı Yüksek Lisans Programı öğrencisi İmren ALTINER Doç.Dr.Özlem ÇAKIR danışmanlığında yürüttüğü "Öğretmenlerin Kişisel Siber Güvenlik Farkındalık Düzeylerinin Farklı Değişkenlere Göre Değerlendirilmesi" konulu tez çalışması kapsamında Ankara İlinde bulunan Milli Eğitim Bakanlığına bağlı ekli listede belirtilen okullarda çalışma yapmak istemektedir.

Bilgilerinizi ve adı geçen öğrenciye yapacağı tez çalışması için gereken iznin verilmesi hususunda gereğini saygılarımla arz ederim.

e-imzalıdır
Prof. Dr. Yasemin KEPENEKCİ
Müdür

Ek : Dilekçe ve Ekleri (1 Takım)

BENZERLİK BİLDİRİMİ

"Öğretmenlerinin Kişisel Siber Güvenlik Farkındalık Düzeylerinin Farklı Değişkenlere Göre Değerlendirilmesi" başlıklı tezimin ana bölümü (ön bölüm, kaynaklar ve ekler hariç) Turnitin İntihali Engelleme Programı aracılığıyla incelenmiş ve ilgili rapor danışmanım tarafından da kontrol edilmiştir. Kontrol sırasında (1) "Yedi sözcükten daha az olan benzeşmeler" (2) "Kaynaklar" (3) "Doğrudan Alıntılar" dışarıda tutulmuştur. Benzerlik kontrolüne ilişkin rapordan elde edilen sonuçlar aşağıda sunulmuştur.

Rapor Tarihi	: 21.10.2021
Gönderim Numarası	: 1679952651
Sayfa Sayısı	: 81
Sözcük Sayısı	: 21409
Karakter Sayısı	: 155042
Benzerlik Oranı	: %10
Savunma Tarihi	: 10.09.2021

Yukarıda belirtilen sonuçları gösteren Turnitin İntihali Engelleme Programı'na ilişkin orijinal raporu, sonuçlarda herhangi bir değişiklik yapmaksızın bu beyanım ekinde Enstitüye teslim ettiğimi, tezimin %10'dan fazla benzerlik oranı içerdiğinin belirlenmesi durumunda, bundan doğabilecek tüm yasal sorumluluğu kabul ettiğimi bildirir, saygılarımı sunarım.

Öğrencinin Adı Soyadı: İmren ALTINER

Tarih: 21.10.2021

İmza:

ÖZGEÇMİŞ

Kişisel Bilgiler

Adı ve Soyadı : İmren ALTINER

E-Posta Adresi :

Akademik Bilgiler

Öğrenim Durumu:

Derece	**Bölüm/Program**	**Üniversite**	**Yıl**
Yüksek Lisans	Bilgisayar ve Öğretim Teknolojileri Eğitimi	Ankara Üniversitesi	2021
Lisans	Bilgisayar ve Öğretim Teknolojileri Eğitimi	Ankara Üniversitesi	2016