

**ÖĞRETMEN ADAYLARININ SİBER BİLGİ GÜVENLİĞİ
FARKINDALIKLARININ VE DİJİTAL VATANDAŞLIK
DÜZEYLERİNİN FARKLI DEĞİŞKENLER AÇISINDAN
İNCELENMESİ**

YÜKSEK LİSANS TEZİ

MURAT SOLMAZ

**MERSİN ÜNİVERSİTESİ
EĞİTİM BİLİMLERİ ENSTİTÜSÜ**

**BİLGİSAYAR VE ÖĞRETİM TEKNOLOJİLERİ
EĞİTİMİ ANABİLİM DALI**

**MERSİN
NİSAN - 2020**

**ÖĞRETMEN ADAYLARININ SİBER BİLGİ GÜVENLİĞİ
FARKINDALIKLARININ VE DİJİTAL VATANDAŞLIK
DÜZEYLERİNİN FARKLI DEĞİŞKENLER AÇISINDAN
İNCELENMESİ**

YÜKSEK LİSANS TEZİ

MURAT SOLMAZ

**MERSİN ÜNİVERSİTESİ
EĞİTİM BİLİMLERİ ENSTİTÜSÜ**

**BİLGİSAYAR VE ÖĞRETİM TEKNOLOJİLERİ
EĞİTİMİ ANABİLİM DALI**

**Danışman
Dr. Öğr. Üyesi Ali GÖK**

**MERSİN
NİSAN - 2020**

ETİK BEYAN

Mersin Üniversitesi Lisansüstü Eğitim-Öğretim Yönetmeliğinde belirtilen kurallara uygun olarak hazırladığım bu tez çalışmada,

- Tez içindeki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
- Görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlâk kurallarına uygun olarak sunduğumu,
- Başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,
- Atıfta bulunduğum eserlerin tümünü kaynak olarak kullandığımı,
- Kullanılan verilerde herhangi bir tahrifat yapmadığımı,
- Bu tezin herhangi bir bölümünü Mersin Üniversitesi veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı,
- Tezin tüm telif haklarını Mersin Üniversitesi'ne devrettiğimi

beyan ederim.

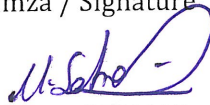
ETHIC DECLARATION

This thesis is prepared in accordance with the rules specified in Mersin University Graduate Education Regulation and I declare to comply with the following conditions:

- I have obtained all the information and the documents of the thesis in accordance with the academic rules.
- I presented all the visual, auditory and written informations and results in accordance with scientific ethics.
- I refer in accordance with the norms of scientific works about the case of exploitation of others' works.
- I used all of the referred works as the references.
- I did not do any tampering in the used data.
- I did not present any part of this thesis as an another thesis at Mersin University or another university.
- I transfer all copyrights of this thesis to the Mersin University.

6 Nisan 2020/6 April 2020

İmza / Signature



Murat SOLMAZ

ÖZET

ÖĞRETMEN ADAYLARININ SİBER BİLGİ GÜVENLİĞİ FARKINDALIĞI VE DİJİTAL VATANDAŞLIK DÜZEYLERİNİN ÇEŞİTLİ DEĞİŞKENLER AÇISINDAN İNCELENMESİ

Bu araştırmada devlet üniversitelerinin eğitim fakültelerinde öğrenim gören öğretmen adaylarının siber güvenlik farkındalık düzeyleri ile dijital vatandaşlık düzeylerinin farklı değişkenler açısından incelemesi amaçlanmıştır. İlişkisel tarama modeli olarak gerçekleştirilen çalışmada örneklemin belirlenmesinde uygun örnekleme yöntemi kullanılmıştır. Araştırmanın örneklemini Akdeniz Bölgesinde yer alan bir devlet üniversitesinin eğitim fakültesinde öğrenim gören 1155 öğretmen adayı oluşturmaktadır. Veri toplama aracı olarak “Siber Bilgi Güvenliği Farkındalığı Ölçeği” ve “Dijital Vatandaşlık Ölçeği” kullanılmıştır. Öğretmen adaylarının Siber Bilgi Güvenliği Farkındalıkları (SBGF) ve Dijital Vatandaşlıkları (DV) düzeyleri; cinsiyet, bölüm, sınıf, bilgisayar kullanım oranı, sosyal medya kullanım oranı, kişisel teknolojik aleti olup olmama durumu gibi değişkenlere göre incelenmiştir. Veri analizinde SPSS 20 programı kullanılmış; T-test, ANOVA ve Korelasyon analizleri gerçekleştirilmiştir. Araştırmada öğretmen adaylarının Siber Bilgi Güvenliği Farkındalıkları ve Dijital Vatandaşlık düzeylerinin ortalamasının üstünde bir seviyede olduğu sonucuna ulaşılmıştır. Araştırma bulguları daha detaylı analiz edildiğinde ise SBGF'nin cinsiyete göre erkeklerin lehine anlamlı farklılaştığı görülürken, DV düzeyinin cinsiyete göre farklılaşmadığı tespit edilmiştir. Ayrıca SBGF ve DV düzeyinin öğretmen adaylarının öğrenim gördükleri bölüme göre farklılaştığı sonucuna ulaşılmıştır. Farklılaşmanın hangi bölümler arasında olduğunu tespit etmek için ise Post Hoc analizi gerçekleştirilmiştir. SBGF ve DV düzeyleri arasında gerçekleştirilen korelasyon analizinde ise orta düzeyde bir ilişki tespit edilmiştir. Araştırmanın bulguları sonucunda; bilgi ve iletişim teknolojilerinin her alanda kullanıldığı çağımızda gelecek nesilleri yetiştirecek öğretmen adaylarının dijital vatandaşlık düzeyleri ve siber bilgi güvenliği farkındalık seviyelerinin daha da artırılabilmesi için eğitim fakültelerinde öğretmen adaylarının bu açıdan desteklenmeleri gerektiği ortaya çıkmıştır.

Anahtar Kelimeler: Siber bilgi güvenliği farkındalığı, bilgi güvenliği, dijital veri güvenliği, dijital vatandaşlık, öğretmen adayları

Danışman: Dr. Öğr. Üyesi Ali GÖK, Mersin Üniversitesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı, Mersin.

ABSTRACT

INVESTIGATION OF TEACHER CONDIDATES' CYBER SECURITY AWARENSS AND DIGITAL CITIZENSHIP

In this study, as terms of different variables, it was aimed to examine the cyber security awareness levels and digital citizenship levels of pre-service teachers studying at faculty of education in the public universities. In the study carried out as a correlational survey model, the convenience sampling model was used. The sample of the study consisted of 1155 pre-service teachers studying at faculty of education in an public university in Turkey's Mediterranean area. "Cyber Information Security Awareness Scale" and "Digital Citizenships Scale" were accompanied as data collection tools. Cyber information security awareness (CISA) and digital citizenship (DC) levels of pre-service teachers were examined according to variables such as gender, department, class, computer usage rate, social media usage rate, and availability of personal technology equipment. The data were analyzed with the help of SPSS 20 software, and inferential statistics such as T-test, ANOVA and correlational statistics were conducted. According to results of the study, mean of the Cyber Information Security Awareness and Digital Citizenship levels of pre-service teachers were above the average level. According to more detailed analysis in respect of gender, CISA of men pre-service teachers were significantly more than women pre-service teachers, while DC level of the pre-service teachers were not significantly different with respect to gender. Additionally, it was concluded that CISA and DC levels of the pre-service teachers were significantly different according to the departments where pre-service teachers study. Post Hoc analysis were conducted in order to determine differentiation between departments of the pre-service teachers. On the other hand, Furthermore, it was determined that medium level relationship between CISA and DC levels of pre-service teachers as a result of correlational analysis. Consequently, it has been revealed that pre-service teachers in faculty of education should be supported in order to increase levels of cyber information security awareness and digital citizenship of pre-service teachers who will retain the next generations during the age of information and communication technologies used in every field.

Key Words: Cyber information security awareness, information security, digital data security, digital citizenship, teacher candidates

Supervisor: Assist. Prof. Dr. Ali GÖK, Mersin University, Computer and Education Instructional Technology, Mersin.

TEŞEKKÜR

Yüksek lisansa başladığım günden bu güne kadar danışmanlığımı yapan, her türlü deneyimini benimle paylaşan, yoğun zamanlarında bile vermiş olduğu dönütler ile tez yazma sürecimde büyük emeği olan kıymetli hocam **Dr. Öğr. Üyesi Ali GÖK**' e en içten teşekkürlerimi sunuyorum.

Tez jüriliğimi yapan, sonrasında vermiş oldukları dönütler ile tezime büyük katkılar sağlayan değerli hocalarım **Doç. Dr. Hatice SANCAR TOKMAK** ve **Dr. Öğr. Üyesi Ömer Faruk İSLİM**' e teşekkürlerimi sunuyorum.

Gerek veri toplama sürecinde gerek veri analizleri sırasında yardımını esirgemeyen değerli hocam **Dr. Öğr. Üyesi Gülsüm GÖK**' e teşekkür ediyorum.

Yüksek lisans sürecim başladığı günden beri sürekli yanımda olan, kimi zaman fikirleri ile bana yol gösteren sevgili eşim **Çilem**' e, yüksek lisans tezimi bitirme hediyesi gibi gelen canım kızım **Elvin**' e ve tüm aile bireylerime sonsuz teşekkür ediyorum.

Yüksek lisans vasıtası ile tanıyıp sonrasında iyi bağlar kurmuş olduğumuz tüm arkadaşlarıma teşekkürlerimi sunuyorum.

Veri toplama sürecinde etmiş oldukları yardımlar ile işimi kolaylaştıran BÖTE, Fen, İngilizce, Matematik, Yabancı Dil, Türkçe, PDR ve Okul Öncesi bölümlerindeki hocalarıma teşekkür ediyorum.

Son olarak vermiş oldukları desteklerden dolayı görev yaptığım Bahriye Ortaokulu müdürüm Ersan ÜNAL' a ve diğer öğretmen arkadaşlarıma teşekkürlerimi sunuyorum.

Murat SOLMAZ

MERSİN, 2020

İÇİNDEKİLER

	Sayfa
İÇ KAPAK	
ETİK BEYAN	
ÖZET	i
ABSTRACT	ii
TEŞEKKÜR	iii
İÇİNDEKİLER	iv
ŞEKİLLER DİZİNİ	vii
TABLOLAR DİZİNİ	viii
KISALTMALAR	xiii
1. GİRİŞ	1
1.1.Araştırma Problemi	4
1.2. Araştırmanın Amacı	8
1.3.Araştırma Soruları ve Alt Soruları	8
1.4. Araştırmanın Önemi	9
1.5. Araştırma Sayıtları	12
1.6. Araştırma Kapsam ve Sınırlılıkları	13
2. KAYNAK ARAŞTIRMALARI/ İLGİLİ ARAŞTIRMALAR/ ALANYAZIN	14
2.1. Dijital Vatandaşlık	14
2.2. Siber Güvenlik	17
2.2.1. Siber Bilgi Güvenliği Farkındalığı	19
2.2. 2. Siber Saldırı	19
2.3. Siber Bilgi Güvenliği ile İlgili Kavramlar	20
2.4. Türkiye de Siber Güvenlik	25
2.5. İlgili Araştırmalar	26
2.5.1. Dijital Vatandaşlık İle İlgili Yapılan Çalışmalar	26
2.5.2 Siber Güvenlik İle İlgili Yapılan Çalışmalar	31
3. YÖNTEM	42
3.1. Araştırmanın Modeli	42
3.2. Araştırmanın Evren ve Örnekleme	42
3.3. Veri Toplama Aracı	45
3.4. Veri Toplama Süreci	46
3.5. Verilerin Analizi	47
3.6. Geçerlilik Güvenirlik	48
4. BULGULAR	49
4.1. Öğretmen Adaylarının Siber Bilgi Güvenliği Farkındalığı ve Dijital Vatandaşlık Düzeyleri	49
4.1.1. Öğretmen Adaylarının Siber Bilgi Güvenliği Farkındalıklarının ve Dijital Vatandaşlık Düzeylerinin Cinsiyete Göre İncelenmesi	50
4.1.2. Öğretmen Adaylarının Dijital Vatandaşlık Alt Boyutlarının Cinsiyet Değişkenine Göre İncelenmesi	50
4.2. Bağımlı Değişkenlerin Bölümlere Göre Karşılaştırılması Tek yönlü Varyans analizi	52
4.2.1. Siber Bilgi Güvenliği Farkındalığı Değişkeninin Bölümlere göre karşılaştırılması	52
4.2.2. Dijital Vatandaşlık Düzeyinin Bölümlere Göre Karşılaştırılması	58
4.2.2.1. Dijital Okuryazarlık Düzeylerinin Bölümlere Göre Karşılaştırılması	64
4.2.2.2. Dijital Yasa Düzeylerinin Bölümlere Göre Karşılaştırılması	69
4.2.2.3. Dijital Hak ve Sorumluluklar Düzeylerinin Bölümlere Göre Karşılaştırılması	70
4.2.2.4. Dijital İletişim Alt Boyutunun Bölümlere Göre Karşılaştırılması	71
4.2.2.5. Dijital Güvenlik Düzeylerinin Bölümlere Göre Karşılaştırılması	74

4.2.2.6. Dijital Ticaret Düzeylerinin Bölümlere Göre Karşılaştırılması	77
4.2.2.7. Dijital Erişim Düzeylerinin Bölümlere Göre Karşılaştırılması	78
4.2.2.8. Dijital Etik Düzeylerinin Bölümlere Göre Karşılaştırılması	82
4.2.2.9. Dijital Sağlık Düzeylerinin Bölümlere Göre Karşılaştırılması	85
4.3. Bağımlı Değişkenlerin Sınıf Düzeylerine Göre Farkı - Tek Yönlü Varyans Analizi (ANOVA)	86
4.3.1. Siber Bilgi Güvenliği Farkındalığı Değişkeninin Sınıf Düzeyine Göre Karşılaştırılması	86
4.3.2. Dijital vatandaşlık düzeyinin Sınıf düzeyine göre farkı	87
4.3.2.1. Dijital okuryazarlık alt boyutunu düzeyinin sınıf düzeyine göre farkı	88
4.3.2.2. Dijital yasa düzeyinin Sınıf düzeyine göre farkı	90
4.3.2.3. Dijital hak ve sorumluluk düzeyinin Sınıf düzeyine göre farkı	91
4.3.2.4. Dijital iletişim düzeyinin Sınıf düzeyine göre farkı	91
4.3.2.5. Dijital güvenlik düzeyinin Sınıf düzeyine göre farkı	92
4.3.2.6. Dijital ticaret düzeyinin Sınıf düzeyine göre farkı	93
4.3.2.7. Dijital erişim düzeyinin Sınıf düzeyine göre farkı	94
4.3.2.8. Dijital etik düzeyinin Sınıf düzeyine göre farkı	95
4.3.2.9. Dijital sağlık düzeyinin Sınıf düzeyine göre farkı	96
4.4. Değişkenlerin Günlük Toplam Teknoloji Kullanımına Göre Karşılaştırılması - Tek Yönlü Varyans Analizi (ANOVA)	97
4.4.1. Siber bilgi güvenliği farkındalığının günlük toplam teknoloji kullanımına göre karşılaştırılması	97
4.4.2. Dijital vatandaşlık düzeyinin günlük toplam teknoloji kullanımına göre karşılaştırılması	98
4.4.2.1. Dijital okuryazarlık alt boyutunun günlük toplam teknoloji kullanımına göre karşılaştırılması	101
4.4.2.2. Dijital yasa alt boyutunun günlük toplam teknoloji kullanımına göre karşılaştırılması	102
4.4.2.3. Dijital hak ve sorumluluk alt boyutunun günlük toplam teknoloji kullanımına göre karşılaştırılması	103
4.4.2.4. Dijital iletişim alt boyutunun günlük toplam teknoloji kullanımına göre karşılaştırılması	104
4.4.2.5. Dijital güvenlik alt boyutunun günlük toplam teknoloji kullanımına göre karşılaştırılması	106
4.4.2.6. Dijital ticaret alt boyutunun günlük toplam teknoloji kullanımına göre karşılaştırılması	107
4.4.2.7. Dijital erişim alt boyutunun günlük toplam teknoloji kullanımına göre karşılaştırılması	109
4.4.2.8. Dijital etik alt boyutunun günlük toplam teknoloji kullanımına göre karşılaştırılması	111
4.4.2.9. Dijital sağlık alt boyutunun günlük toplam teknoloji kullanımına göre karşılaştırılması	113
4.5. Değişkenlerin Günlük Sosyal Medya Kullanım(GSK) Sürelerine Göre Karşılaştırılması - Tek Yönlü Varyans Analizi (ANOVA)	115
4.5.1. Siber bilgi güvenliği farkındalığının günlük sosyal medya kullanım saatine göre karşılaştırılması	115
4.5.2. Dijital vatandaşlık düzeyinin günlük sosyal medya kullanım saatine göre karşılaştırılması	117
4.5.2.1. Dijital okuryazarlık düzeyinin günlük sosyal medya kullanım saatine göre farkı	118
4.5.2.2. Dijital yasa alt boyutunun günlük sosyal medya kullanım saatine göre karşılaştırılması	119
4.5.2.3. Dijital hak ve sorumluluk alt boyutunun günlük sosyal medya kullanım saatine göre karşılaştırılması	120

4.5.2.4. Dijital iletişim alt boyutunun günlük sosyal medya kullanım sürelerine göre karşılaştırılması	121
4.5.2.5 Dijital güvenlik alt boyutunun günlük sosyal medya kullanım sürelerine göre karşılaştırılması	123
4.5.2.6 Dijital ticaret alt boyutunun günlük sosyal medya kullanım sürelerine göre karşılaştırılması	124
4.5.2.7. Dijital erişim alt boyutunun günlük sosyal medya kullanım sürelerine göre karşılaştırılması	126
4.5.2.8. Dijital etik alt boyutunun günlük sosyal medya kullanım sürelerine göre karşılaştırılması	128
4.5.2.9. Dijital sağlık alt boyutunun günlük sosyal medya kullanım sürelerine göre karşılaştırılması	129
4.6. Öğretmen Adaylarının Siber Bilgi Güvenliği Farkındalığı ve Dijital Vatandaşlık Düzeyleri Arasındaki İlişkinin İncelenmesi	131
4.8.Siber Bilgi Güvenlik Farkındalığı ve Dijital Vatandaşlık Alt Boyutları Arasındaki İlişki	132
5.SONUÇ ve ÖNERİLER	134
5.1.Uygulamaya Yönelik Öneriler	142
5.2.Yapılacak Araştırmalara Yönelik Öneriler	143
KAYNAKLAR	145
EKLER	153
EK 1. Mersin Üniversitesi Araştırma İzin Yazısı	153
EK 2. Kişisel Bilgi Formu	154
EK 3. Siber Bilgi Güvenliği Ölçeği	155
EK 4. Dijital Vatandaşlık Ölçeği	156
EK 5.Öz Geçmiş	157

ŞEKİLLER DİZİNİ

	Sayfa
Şekil 1.1. Dünya Çapında Siber Güvenlik Teknolojisinin 2017-2023 Arası Büyüklüğü.	5
Şekil 1.2. İşletmelerin Bilgi Güvenliğine Harcadığı 2005-2017 Arası Bütçelerinin Yüzdesi.	6
Şekil 1.3. Siber Güvenlik Katmanları	10
Şekil 1.4. İnsan Siber Güvenlik Unsurları İlişkisi	10
Şekil 1.5. 2018'de X-Force IRIS Tarafından Gözlenen Phishing Kategorileri (IBM,2019)	11
Şekil 2.1 Siber Güvenlik ve Diğer Güvenlik Alanları Arası İlişki	24
Şekil 4.1. Bölümlere Göre Siber Bilgi Güvenliği Farkındalık Ortalamalarının Grafiği	53
Şekil 4.2. Bölümlere Göre Dijital Vatandaşlık Düzeyi Ortalamalarının Grafiği	58
Şekil 4.3. Sınıf Düzeyine Göre Siber Bilgi Güvenliği Farkındalık Ortalamalarının Grafiği	86
Şekil 4.4. Sınıf Düzeyine Göre Siber Bilgi Güvenliği Farkındalık Ortalamalarının Grafiği	87
Şekil 4.5. GTK Süresine Göre Siber Bilgi Güvenliği Farkındalık Ortalamalarının Grafiği	97
Şekil 4.6. GTK Süresine Göre Dijital Vatandaşlık Ortalamalarının Grafiği	98
Şekil 4.7. GSK sürelerine Göre Siber Bilgi Güvenliği Farkındalık Ortalamalarının Grafiği	115
Şekil 4.8. GSK sürelerine Göre Dijital Vatandaşlık Düzeyi Ortalamalarının Grafiği	117
Şekil 4.9. SBGF ile Dijital Vatandaşlık Arasındaki İlişki Grafiği	132

TABLOLAR DİZİNİ

	Sayfa
Tablo 2.1. YökTez Tarama Sonuçları	33
Tablo 3.1 Araştırmaya katılan öğretmen adaylarının bölümlere sayıları ve yüzdeleri	43
Tablo 3.2 Araştırmaya katılan öğretmen adaylarının cinsiyete göre sayıları	44
Tablo 3.3 Sınıf kademelerine göre Eğitim Fakültesine kayıtlı öğretmen adayı ve değerlendirmeye alınan öğretmen adayı sayıları	44
Tablo 3.4 Araştırmaya Katılan Öğretmen Adayların Teknolojik Alet Sahip Olma Durumları	44
Tablo 3.5 Araştırmaya Katılan Öğretmen Adayların Teknoloji Kullanım(GTK) ve Günlük Sosyal Medya(GSK) Kullanım Sürelerine Göre Sayıları	45
Tablo 4.1 Öğretmen Adaylarının Siber Bilgi Güvenliği Farkındalığı ve Dijital Vatandaşlık Düzeylerinin Ortalama, Standart Sapma Değerleri	49
Tablo 4.2 Siber Bilgi Güvenliği ve Dijital Vatandaşlık Seviyesinin Cinsiyete Göre Karşılaştırılması	50
Tablo 4.3 Dijital Vatandaşlığın 9 alt boyutunun cinsiyete göre karşılaştırılması	51
Tablo 4.4 Siber Bilgi Güvenliği Farkındalığının Bölümlere göre kişi sayısı, ortalama ve standart sapmaları	53
Tablo 4.5 Siber Bilgi Güvenliği Farkındalığının Bölümlere Karşılaştırılması	54
Tablo 4.6 BÖTE bölümünün diğer bölümlere göre Siber Bilgi Güvenliği Farkındalığı farkı- Post Hoc	54
Tablo 4.7 Fen Bilgisi Öğretmenliği bölümünün diğer bölümlere göre Siber Bilgi Güvenliği Farkındalığı farkı- Post Hoc	55
Tablo 4.8 Matematik öğretmenliği bölümünün diğer bölümlere göre Siber Bilgi Güvenliği Farkındalığı farkı- Post Hoc	55
Tablo 4.9 Sınıf öğretmenliği bölümünün diğer bölümlere göre Siber Bilgi Güvenliği Farkındalığı farkı- Post Hoc	56
Tablo 4.10 Okul öncesi öğretmenliği bölümünün diğer bölümlere göre Siber Bilgi Güvenliği Farkındalığı farkı- Post Hoc	56
Tablo 4.11 PDR bölümünün diğer bölümlere göre Siber Bilgi Güvenliği Farkındalığı farkı- Post Hoc	57
Tablo 4.12 Türkçe Öğretmenliği bölümünün diğer bölümlere göre Siber Bilgi Güvenliği Farkındalığı farkı- Post Hoc	57
Tablo 4.13 Yabancı Dil Öğretmenliği bölümünün diğer bölümlere göre Siber Bilgi Güvenliği Farkındalığı farkı- Post Hoc	58
Tablo 4.14 Dijital Vatandaşlık Düzeylerinin bölümlere göre kişi sayısı, ortalama ve standart sapmaları.	59
Tablo 4.15 Dijital Vatandaşlık Düzeylerinin bölümlere göre karşılaştırılması ANOVA	59
Tablo 4.16 BÖTE bölümünün diğer bölümlere göre Dijital Vatandaşlık Düzeyi farkı- Post Hoc	60
Tablo 4.17 Fen Bilgisi Öğretmenliği bölümünün diğer bölümlere göre Dijital Vatandaşlık Düzeyi farkı- Post Hoc	60
Tablo 4.18 Matematik Öğretmenliği bölümünün diğer bölümlere göre Dijital Vatandaşlık Düzeyi farkı - Post Hoc	61
Tablo 4.19 Okul Öncesi Öğretmenliği bölümünün diğer bölümlere göre Dijital Vatandaşlık Düzeyi farkı - Post Hoc	61
Tablo 4.20 Sınıf Öğretmenliği bölümünün diğer bölümlere göre Dijital Vatandaşlık Düzeyi farkı - Post Hoc	62
Tablo 4.21 PDR bölümünün diğer bölümlere göre Dijital Vatandaşlık Düzeyi farkı- Post Hoc	62
Tablo 4.22 Türkçe Öğretmenliği bölümünün diğer bölümlere göre Dijital Vatandaşlık Düzeyi farkı - Post Hoc	63

Tablo 4.23 Yabancı Dil Öğretmenliği bölümünün diğer bölümlere göre Dijital Vatandaşlık Düzeyi farkı - Post Hoc	63
Tablo 4.24 Dijital Okur Yazarlık Düzeylerinin; Bölümlere Göre Kişi Sayısı, Ortalama ve Standart Sapmaları	64
Tablo 4.25 Dijital Okur Yazarlık Alt Boyutunun Bölümlere Göre Karşılaştırılması	64
Tablo 4.26 BÖTE Bölümünün Diğer Bölümlere Göre Dijital Okur Yazarlık Düzeyi- Post Hoc	65
Tablo 4.27 Fen Bilgisi Öğretmenliği Bölümünün Diğer Bölümlere Göre Dijital Okur Yazarlık Düzeyi - Post Hoc	65
Tablo 4.28 Matematik Öğretmenliği Bölümünün Diğer Bölümlere Göre Dijital Okur Yazarlık Düzeyi - Post Hoc	66
Tablo 4.29 Sınıf Öğretmenliği Bölümünün Diğer Bölümlere Göre Dijital Okur Yazarlık Düzeyi- Post Hoc	66
Tablo 4.30 Okul Öncesi Öğretmenliği Bölümünün Diğer Bölümlere Göre Dijital Okur Yazarlık Düzeyi - Post Hoc	67
Tablo 4.31 PDR Bölümünün Diğer Bölümlere Göre Dijital Okur Yazarlık Düzeyi- Post Hoc	67
Tablo 4.32 Türkçe Öğretmenliği Bölümünün Diğer Bölümlere Göre Dijital Okur Yazarlık Düzeyi - Post Hoc	68
Tablo 4.33 Yabancı Dil bölümünün Diğer Bölümlere Göre Dijital Okur Yazarlık Düzeyi- Post Hoc	68
Tablo 4.34 Dijital Yasa Düzeylerinin Bölümlere göre kişi sayısı, ortalama ve standart sapmaları	69
Tablo 4.35 Dijital Yasa Alt Boyutunun Bölümlere Karşılaştırılması	69
Tablo 4.36 Dijital Hak ve Sorumluluk Düzeylerinin Bölümlere göre kişi sayısı, ortalama ve standart sapmaları	70
Tablo 4.37 Dijital Hak ve Sorumluluk Alt Boyutunun Bölümlere Göre Karşılaştırılması	70
Tablo 4.38 Dijital İletişim Alt Boyutunun Bölümlere göre kişi sayısı, ortalama ve standart sapmaları	71
Tablo 4.39 Dijital iletişim Alt Boyutunun Bölümlere Karşılaştırılması	71
Tablo 4.40 Dijital İletişim Altı Boyutunda Anlamlı Farklılaşma Olan Bölümler- Post Hoc	72
Tablo 4.41 Dijital Güvenlik Alt Boyutunun Bölümlere göre kişi sayısı, ortalama ve standart sapmaları	74
Tablo 4.42 Dijital Güvenlik Alt Boyutunun Bölümlere Karşılaştırılması	74
Tablo 4.43 Dijital Güvenlik Altı Boyutunda Anlamlı Farklılaşma Olan Bölümler- Post Hoc	75
Tablo 4.43 Dijital Güvenlik Altı Boyutunda Anlamlı Farklılaşma Olan Bölümler- Post Hoc(Devam)	76
Tablo 4.44 Dijital Ticaret Boyutunun Bölümlere göre kişi sayısı, ortalama ve standart sapmaları	77
Tablo 4.45 Dijital Ticaret Alt Boyutunun Bölümlere Karşılaştırılması	77
Tablo 4.46 Dijital Erişim Boyutunun Bölümlere göre kişi sayısı, ortalama ve standart sapmaları	78
Tablo 4.47 Dijital Erişim Alt Boyutunun Bölümlere Karşılaştırılması	78
Tablo 4.48 Dijital Erişim Altı Boyutunda Anlamlı Farklılaşma Olan Bölümler- Post Hoc	79
Tablo 4.48 Dijital Erişim Altı Boyutunda Anlamlı Farklılaşma Olan Bölümler- Post Hoc(Devam))	80
Tablo 4.49 Dijital Etik Alt Boyutunun Bölümlere göre kişi sayısı, ortalama ve standart sapmaları	82
Tablo 4.50 Dijital Etik Alt Boyutunun Bölümlere Karşılaştırılması	82
Tablo 4.51 Dijital Etik Altı Boyutunda Anlamlı Farklılaşma Olan Bölümler- Post Hoc	83
Tablo 4.51 Dijital Etik Altı Boyutunda Anlamlı Farklılaşma Olan Bölümler- Post Hoc(Devam)	84
Tablo 4.52 Dijital Sağlık Boyutunun Bölümlere göre kişi sayısı, ortalama ve standart sapmaları	85

Tablo 4.53 Dijital Sağlık Alt Boyutunun Bölümlere Karşılaştırılması	85
Tablo 4.54 Siber Bilgi Güvenliği Farkındalığının Sınıf Düzeyine Göre Kişi Sayısı, Ortalama ve Standart Sapmaları	86
Tablo 4.55 Siber Bilgi Güvenliği Farkındalığının Sınıf Düzeylerine Göre Karşılaştırılması	87
Tablo 4.56 Dijital Vatandaşlık Seviyelerinin Sınıf Düzeyine Göre Kişi Sayısı, Ortalama ve Standart Sapmaları	88
Tablo 4.57 Dijital Vatandaşlık Seviyelerinin Sınıf Düzeylerine Göre Karşılaştırılması	88
Tablo 4.58 Dijital Okuryazarlık Seviyelerinin Sınıf Düzeyine Göre Kişi Sayısı, Ortalama ve Standart Sapmaları	88
Tablo 4.59 Dijital Okuryazarlık Seviyelerinin Sınıf Düzeylerine Göre Karşılaştırılması	89
Tablo 4.60 Dijital Okuryazarlık Altı Boyutunda Anlamlı Farklılaşma Sınıf Düzeyi- Post Hoc	89
Tablo 4.61 Dijital Yasa Seviyelerinin Sınıf Düzeyine Göre Kişi Sayısı, Ortalama ve Standart Sapmaları	90
Tablo 4.62 Dijital Yasa Seviyelerinin Sınıf Düzeylerine Göre Karşılaştırılması	90
Tablo 4.63 Dijital Hak ve Sorumluluk Seviyelerinin Sınıf Düzeyine Göre Kişi Sayısı, Ortalama ve Standart Sapmaları	91
Tablo 4.64 Dijital Hak ve Sorumluluk Seviyelerinin Sınıf Düzeylerine Göre Karşılaştırılması	91
Tablo 4.65 Dijital İletişim Seviyelerinin Sınıf Düzeyine Göre Kişi Sayısı, Ortalama ve Standart Sapmaları	91
Tablo 4.66 Dijital İletişim Seviyelerinin Sınıf Düzeylerine Göre Karşılaştırılması	92
Tablo 4.67 Dijital Güvenlik Seviyelerinin Sınıf Düzeyine Göre Kişi Sayısı, Ortalama ve Standart Sapmaları	92
Tablo 4.68 Dijital Güvenlik Seviyelerinin Sınıf Düzeylerine Göre Karşılaştırılması	93
Tablo 4.69 Dijital Ticaret Seviyelerinin Sınıf Düzeyine Göre Kişi Sayısı, Ortalama ve Standart Sapmaları	93
Tablo 4.70 Dijital Ticaret Seviyelerinin Sınıf Düzeylerine Göre Karşılaştırılması	93
Tablo 4.71 Dijital Erişim Seviyelerinin Sınıf Düzeyine Göre Kişi Sayısı, Ortalama ve Standart Sapmaları	94
Tablo 4.72 Dijital Erişim Seviyelerinin Sınıf Düzeylerine Göre Karşılaştırılması	94
Tablo 4.73 Dijital Erişim Altı Boyutunda Anlamlı Farklılaşma Sınıf Düzeyi- Post Hoc	95
Tablo 4.74 Dijital Etik Seviyelerinin Sınıf Düzeyine Göre Kişi Sayısı, Ortalama ve Standart Sapmaları	95
Tablo 4.75 Dijital Etik Seviyelerinin Sınıf Düzeylerine Göre Karşılaştırılması	96
Tablo 4.76 Dijital Sağlık Seviyelerinin Sınıf Düzeyine Göre Kişi Sayısı, Ortalama ve Standart Sapmaları	96
Tablo 4.77 Dijital Sağlık Seviyelerinin Sınıf Düzeylerine Göre Karşılaştırılması	96
Tablo 4.78 Siber Bilgi Güvenlik Farkındalığının Günlük Teknoloji Kullanımı Süresine Göre; Kişi Sayısı, Ortalama ve Standart Sapmaları	97
Tablo 4.79 Siber Bilgi Güvenlik Farkındalığının Günlük Teknoloji Kullanımına Karşılaştırılması	98
Tablo 4.80 Dijital Vatandaşlık Seviyelerinin Günlük Teknoloji Kullanımı Sürelerine Göre; Kişi Sayısı, Ortalama ve Standart Sapmaları	99
Tablo 4.81 Dijital Vatandaşlık Seviyelerinin Günlük Teknoloji Kullanımına Göre Karşılaştırılması	99
Tablo 4.82 Dijital Vatandaşlık Düzeyi Bakımından Anlamlı Farklılaşma Olan GTK Süreleri- Post Hoc	100
Tablo 4.83 Dijital Okuryazarlık Seviyelerinin Günlük Teknoloji Kullanımı Sürelerine Göre; Kişi Sayısı, Ortalama ve Standart Sapmaları	101
Tablo 4.84 Dijital Okuryazarlık Düzeyinin Günlük Teknoloji Kullanımına Göre Karşılaştırılması	101

Tablo 4.85 Dijital Okuryazarlık Düzeyi Bakımından Anlamlı Farklılaşma Olan GTK Süreleri- Post Hoc	102
Tablo 4.86 Dijital Yasa Seviyelerinin Günlük Teknoloji Kullanımı Sürelerine Göre Kişi Sayısı, Ortalama ve Standart Sapmaları	102
Tablo 4.87 Dijital Yasa Düzeyinin Günlük Teknoloji Kullanımına Göre Karşılaştırılması	103
Tablo 4.88 Dijital Hak ve Sorumluluk Seviyelerinin Günlük Teknoloji Kullanımı Sürelerine Göre Kişi Sayısı, Ortalama ve Standart Sapmaları	103
Tablo 4.89 Dijital Hak ve Sorumluluk Düzeyinin Günlük Teknoloji Kullanımına Göre Karşılaştırılması	104
Tablo 4.90 Dijital İletişim Seviyelerinin Günlük Teknoloji Kullanımı Sürelerine Göre; Kişi Sayısı, Ortalama ve Standart Sapmaları	104
Tablo 4.91 Dijital İletişim Düzeyinin Günlük Teknoloji Kullanımına Göre Karşılaştırılması	105
Tablo 4.92 Dijital İletişim Düzeyi Bakımından Anlamlı Farklılaşma Olan GTK Süreleri- Post Hoc	105
Tablo 4.93 Dijital Güvenlik Seviyelerinin Günlük Teknoloji Kullanımı Sürelerine Göre; Kişi Sayısı, Ortalama ve Standart Sapmaları	106
Tablo 4.94 Dijital Güvenlik Düzeyinin Günlük Teknoloji Kullanımına Göre Karşılaştırılması	106
Tablo 4.95 Dijital Ticaret Seviyelerinin Günlük Teknoloji Kullanımı Sürelerine Göre; Kişi Sayısı, Ortalama ve Standart Sapmaları	107
Tablo 4.96 Dijital Ticaret Düzeyinin Günlük Teknoloji Kullanımına Göre Karşılaştırılması	107
Tablo 4.97 Dijital Ticaret Düzeyi Bakımından Anlamlı Farklılaşma Olan GTK Süreleri- Post Hoc	108
Tablo 4.98 Dijital Erişim Seviyelerinin Günlük Teknoloji Kullanımı Sürelerine Göre; Kişi Sayısı, Ortalama ve Standart Sapmaları	109
Tablo 4.99 Dijital Erişim Düzeyinin Günlük Teknoloji Kullanımına Göre Karşılaştırılması	109
Tablo 4.100 Dijital Erişim Düzeyi Bakımından Anlamlı Farklılaşma Olan GTK Süreleri- Post Hoc	110
Tablo 4.101 Dijital Etik Seviyelerinin Günlük Teknoloji Kullanımı Sürelerine Göre; Kişi Sayısı, Ortalama ve Standart Sapmaları	111
Tablo 4.102 Dijital Etik Düzeyinin Günlük Teknoloji Kullanımına Göre Karşılaştırılması	111
Tablo 4.103 Dijital Etik Düzeyi Bakımından Anlamlı Farklılaşma Olan GTK Süreleri- Post Hoc	112
Tablo 4.104 Dijital Sağlık Seviyelerinin Günlük Teknoloji Kullanımı Sürelerine Göre; Kişi Sayısı, Ortalama ve Standart Sapmaları	113
Tablo 4.105 Dijital Sağlık Düzeyinin Günlük Teknoloji Kullanımına Göre Karşılaştırılması	113
Tablo 4.106 Dijital Sağlık Düzeyi Bakımından Anlamlı Farklılaşma Olan GTK Süreleri- Post Hoc	114
Tablo 4.107 Siber Bilgi Güvenliği Farkındalığının Günlük Sosyal Medya Kullanımına Göre; Kişi Sayısı, Ortalama ve Standart Sapmaları	116
Tablo 4.108 Siber Bilgi Güvenliği Farkındalığının Günlük Sosyal Medya Kullanımına Göre Karşılaştırılması	116
Tablo 4.109 Dijital Vatandaşlık Düzeyinin Günlük Sosyal Medya Kullanımına Göre; Kişi Sayısı, Ortalama ve Standart Sapmaları	117
Tablo 4.110 Dijital Vatandaşlık Düzeyinin Günlük Sosyal Medya Kullanımına Göre Karşılaştırılması	118
Tablo 4.111 Dijital Vatandaşlık Düzeyinin Günlük Sosyal Medya Kullanımına Göre; Kişi Sayısı, Ortalama ve Standart Sapmaları	118
Tablo 4.112 Dijital Okuryazarlık Düzeyinin Günlük Sosyal Medya Kullanımına Göre Karşılaştırılması	118
Tablo 4.113 Dijital Yasa Düzeyinin Günlük Sosyal Medya Kullanımına Göre; Kişi Sayısı, Ortalama ve Standart Sapmaları	119

Tablo 4.114 Dijital Yasa Düzeyinin Günlük Sosyal Medya Kullanımına Göre Karşılaştırılması	119
Tablo 4.115 Dijital Hak ve Sorumluluk Düzeyinin Günlük Sosyal Medya Kullanımına Göre; Kişi Sayısı, Ortalama ve Standart Sapmaları	120
Tablo 4.116 Dijital Hak ve Sorumluluk Düzeyinin Günlük Sosyal Medya Kullanımına Göre Karşılaştırılması	120
Tablo 4.117 Dijital İletişim Düzeyinin Günlük Sosyal Medya Kullanımına Göre; Kişi Sayısı, Ortalama ve Standart Sapmaları	121
Tablo 4.118 Dijital İletişim Düzeyinin Günlük Sosyal Medya Kullanımına Göre Karşılaştırılması	121
Tablo 4.119 Dijital İletişim Düzeyi Bakımından Anlamlı Farklılaşma Olan GSK Süreleri-Post Hoc	122
Tablo 4.120 Dijital Güvenlik Düzeyinin Günlük Sosyal Medya Kullanımına Göre; Kişi Sayısı, Ortalama ve Standart Sapmaları	123
Tablo 4.121 Dijital Güvenlik Düzeyinin Günlük Sosyal Medya Kullanımına Göre Karşılaştırılması	123
Tablo 4.122 Dijital Ticaret Düzeyinin Günlük Sosyal Medya Kullanımına Göre; Kişi Sayısı, Ortalama ve Standart Sapmaları	124
Tablo 4.123 Dijital Ticaret Düzeyinin Günlük Sosyal Medya Kullanımına Göre Karşılaştırılması	124
Tablo 4.124 Dijital Ticaret Düzeyi Bakımından Anlamlı Farklılaşma Olan GSK Süreleri-Post Hoc	125
Tablo 4.125 Dijital Erişim Düzeyinin Günlük Sosyal Medya Kullanımına Göre; Kişi Sayısı, Ortalama ve Standart Sapmaları	126
Tablo 4.126 Dijital Erişim Düzeyinin Günlük Sosyal Medya Kullanımına Göre Karşılaştırılması	126
Tablo 4.127 Dijital Erişim Düzeyi Bakımından Anlamlı Farklılaşma Olan GSK Süreleri-Post Hoc	127
Tablo 4.128 Dijital Etik Düzeyinin Günlük Sosyal Medya Kullanımına Göre; Kişi Sayısı, Ortalama ve Standart Sapmaları	128
Tablo 4.129 Dijital Etik Düzeyinin Günlük Sosyal Medya Kullanımına Göre Karşılaştırılması	128
Tablo 4.130 Dijital Sağlık Düzeyinin Günlük Sosyal Medya Kullanımına Göre; Kişi Sayısı, Ortalama ve Standart Sapmaları	129
Tablo 4.131 Dijital Sağlık Düzeyinin Günlük Sosyal Medya Kullanımına Göre Karşılaştırılması	129
Tablo 4.132 Dijit Dijital Sağlık Düzeyi Bakımından Anlamlı Farklılaşma Olan GSK Süreleri- Post Hoc	130
Tablo 4.133 Siber Bilgi Güvenliği Farkındalığı ve Dijital Vatandaşlık Düzeyleri Arasındaki İlişkinin Çözümlemesi(Korelasyon)	131
Tablo 4.134 Siber Bilgi Güvenliği Farkındalığı ve Dijital Vatandaşlık Alt Boyutları Arasındaki İlişkinin Çözümlemesi(Korelasyon)	132

KISALTMALAR VE SİMGELER

Kısaltma/ Simge	Tanım
ABD:	Amerika Birleşik Devletleri
ARPANET:	Advanced Research Projects Agency Network(Gelişmiş Araştırma Projeleri Dairesi Ağı)
SBGF:	Siber Bilgi Güvenliği Farkındalığı
DV:	Dijital Vatandaşlık
DSİ:	Devlet Su işleri
EARN/BITNET:	European Academic and Research Network(Avrupa Akademik Araştırma Ağı) /Because It's Time Network
İTÜ:	İstanbul Teknik Üniversitesi
NATO:	Kuzey Atlantik Antlaşması Örgütü
OECD:	Ekonomik Kalkınma ve İşbirliği Örgütü
OTDÜ:	Orta Doğu Teknik Üniversitesi
BTK	Bilgi Teknolojileri ve İletişim Kurumu
YÖK	Yüksek Öğretim Kurumu
MEB	Milli Eğitim Bakanlığı
TCP/IP:	Transmission Control Protocolİletim(İletim Kontrol Protokolü)/ Internet Protocol(İnternet Protokolü)
TDK:	Türk Dil Kurumu
TÜİK :	Türkiye İstatistik Kurumu
TÜBİTAK:	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
TÜVEKA:	Türkiye Üniversiteler ve Araştırma Kurumları Ağı
ITU:	Uluslar Arası Telekomünikasyon Birliği
DV:	Dijital Vatandaşlık
GSK:	Günlük Sosyal Medya Kullanım Süresi
GTK:	Günlük Teknoloji Kullanım Süresi
(IoT):	Internet of Things (Nesnelerin İnterneti)
TR-BOME	Türkiye Bilgisayar Olayları Müdahale Ekibi
USOM	Ulusal Siber Olaylara Müdahale Merkezi
BEC	Business Email Compromise(İşletme E-posta Güvenliği)
SCADA	Supervisory Control And Data Acquisition(Merkezi Denetleme Kontrol ve Veri Toplama)
TMT	Teknoloji Medya Telekomünikasyon
STM:	Savunma Teknolojileri Mühendisliği
AECT	Association for Educational Communications and Technology
SSL:	Secure Sockets Layer-Güvenli Giriş Katmanı

1.GİRİŞ

Kesin bir cevabı olmayan “Bilgi nedir?” sorusuna tarih boyunca çeşitli tanımlar yapılsa da aslında bu soru felsefi bir problem olarak ele alınabilir. Alan yazına bakıldığında kimine göre kesin ispatlanmış olan bilgi iken, kimine göre de bilgi sadece bir inançtır. Bilgiyi gerçekleştirilmiş bir inanç olarak tanımlayan Krogh ve diğerlerine (2005) göre insan kendi deneyimleri sonucu doğruya ulaşır. Bu deneyimleri her geçen gün artar ve daha fazla bilgiye ulaşır. Bu artış, tarihin her döneminde farklı hızlarda gerçekleşse de özellikle teknolojinin gelişmesi, hayatımıza bilgisayarların ve internetin girmesi ile birlikte en üst seviyelere ulaşmıştır. İnsanoğlu; bu hızlı gelişmeye toprağı işlemeye ve ateşi kullanmaya başladığı andan itibaren sürekli katkı yapmış, bilgi üretmiştir (Karabulut, 2015). Özellikle 18. ve 19. yüzyıldaki buluşlar “Sanayi Devrimini” tetiklemiş yeni teknolojik aletler geleneksel üretimin yerini alarak üretimde mükemmel artışlar gözlenmiştir (İşevi ve Çelme,2005). Sanayi Devrimi ile hızlanan teknolojik gelişmeler, 2.Dünya Savaşı sonrası doruk noktalara ulaşmıştır. Savaş esnasında kullanılan, radar sistemleri, uçak teknolojileri, roket sistemlerindeki çalışmalar, telefon ve telgraf sistemlerindeki tecrübeler “Bilgi Çağının” ve “Bilgi Toplumunun” doğmasını sağlamıştır (Ünal, 2009). Bilgi Toplumuna geçişin temelini teknoloji oluşturmuş ve bilgi, toplum için bir güç haline gelmiştir (Tandoğan ve diğerleri, 1998). Bilgisayar teknolojileri ve yoğun bilgi üretimi değer kazanmış, bilgi ve iletişim teknolojileri modern yaşam tarzı için vazgeçilmez bir hal almıştır (Klimburg, 2012). Bununla birlikte bilgi de ekonominin vazgeçilmezi haline gelmiş, bilgi ve bilgi üretme yeteneğine sahip insan çağın en önemli servetlerinden biri olmuştur (Berberoğlu, 2010). Bilgi ve iletişim ağlarının yaygınlaştığı; bu amaçla kullanılan teknolojilerin, kitle iletişim araçlarının, bilgisayarların arttığı, sanayi toplumunun uzantısı olarak kabul edilen topluma ise “Bilgi Toplumu” denilmiştir (Rukancı ve Anameriç, 2004). Bilgi Toplumu’na geçen ilk ülke ise Amerika Birleşik Devletleri (ABD) olmuştur. Teknolojik gelişmelere bağlı olarak ilk defa bedensel emeği kullanan “Mavi Yakalılar” zihinsel emeği kullanan “Beyaz Yakalılara” sayısal üstünlüğü kaptırmıştır (Bayraktaroğlu, Özdemir, Aras, ve Özdemir, 2015).

Vatandaşlık kavramının doğuşu ise bilgi toplumundan çok daha eski dönemlere dayanmaktadır. İnsanların toplu halde yaşadıkları dönemlerde temeli atılan bu kavram ilk kez Yunan şehir devletlerinde ortaya çıkmış, günümüz tanımına kavuşması ise Fransız İhtilali ile olmuştur (Nalbant, 2014). Başlarda bir aile soyuna dayanan bu terim daha sonralarda eğitim yolu ile kazandırılabilen ülkesine bağlı bireyler olarak tanımlanmıştır. Bu nedenle ülkeler doğan çocukları kendi ihtiyaçları doğrultusunda vatandaşlık modellerine göre eğitmeye başlamıştır(Turan ve Avcı, 2018). Günümüze doğru gelindiğinde ise vatandaşlığın tanımı teknolojik gelişmeler sonucu ülke sınırlarının ortadan kalkması, her türlü iletişimin internet ortamları ile sağlanmasından etkilenerek farklı boyular kazanmıştır. Bu boyutların en önemlisi

ise vatandaşlığın bir alt boyutu olan “Dijital Vatandaşlık” kavramının doğması ile olmuştur. Alan yazın incelendiğinde dijital vatandaş kavramının da tıpkı vatandaşlıkta olduğu gibi farklı tanımlama süreçlerinden geçtiği görülmektedir. Geçmişteki tanımlar dijital vatandaş daha çok interneti yasa dışı işler için kullanıp kullanmama veya teknolojiyi kullanılabilirlik düzeyi yönünden ayırmıştır (Ribble, 2009). Günümüze doğru gelindiğinde ise özellikle sosyal medyanın yaygınlaşması ile dijital vatandaşlığın çerçevesinin bir hayli genişlediği görülmektedir. Şimşek ve Şimşek (2013) ‘in belirttiği gibi en genel tanımı ile teknolojiyi ve kitle iletişim amaçlarını amacı doğrultusunda en iyi kullanan vatandaşlara dijital vatandaş denilmektedir.

Bu tanımlamalar eşliğinde 20.yüzyılın ortalarına gelindiğinde ise ABD ile Sovyet Sosyalist Cumhuriyet Birliği (SSCB) arasında teknolojik alanda büyük yarış başlamıştır. 1957’de SSCB’nin Sputnik’i başlatmasına karşılık ABD ise JCR Licklider öncülüğünde 1960’larda Advanced Research Projects Agency Network (ARPANET) sistemini üzerine çalışmalara başlamıştır (Hauben, 2007). Daha sonralarda internet adı verilecek olan bu sistem başlarda ABD Savunma Bakanlığı tarafından olası savaş durumunda iletişimin kesintisiz devam etmesi için tasarlanırsa da zamanla büyük firmaların ve şirketlerin kendi ağ yapılarını ARPANET sistemine bağlamasıyla hızla büyümeye başlamıştır (Metin, 1999). Aynı ağ üzerinde geliştirilen TCP/IP (Transmission Control Protocol-İnternet Protocol) sistemi 1983’te ARPANET sisteminde kullanılmaya başlanırsa da halka açık hale gelmesi 1990’ları bulmuştur (Parlak, 2005).

Türkiye’ye bilgisayarların gelişi ise 1960’ları bulmuştur. İlk olarak 30 Ekim 1960 yılında Karayolları Genel Müdürlüğünde bilgisayar kullanılmaya başlanırken daha sonra 1961 yılında İş Bankası’nda, 1963’te Ticaret Bankasında kullanılmıştır. İstanbul Teknik Üniversitesi (İTÜ) ve Ortadoğu Teknik Üniversitesinin(ODTÜ) 1964 yılında bu alanda çalışmalar yaptığı gözlenmiştir (Küçük,2005, akt. Çukurçayır ve Çelebi,2009). İnternetin Türkiye’ye gelişi de Avrupa’da ortaya çıkmasından bir hayli sonra olmuştur. İnternetin genel olarak ilk defa Orta Doğu Teknik Üniversitesine geldiği bilirse de Türkiye’deki ilk geniş alan ağı 1986’da EARN/BITNET(European Academic and Research Network/Because It’s Times Network)’e bağlı Türkiye Üniversiteler ve Araştırma Kurumları Ağı (TÜVEKA) ’dır (“Dünya’da İnternet İnternetin Gelişimi”, 2020). ODTÜ’ye gelişi 1991 yılında Türkiye Bilimsel ve Teknolojik Araştırma Kurumu(TÜBİTAK) ile başlattıkları projenin 1993 yılında sonuçlanması ile olmuştur. 64 Kbps’lik ilk bağlantı yine TCP/IP protokolü üzerinden gerçekleşmiştir (Parlak,2005). 2000’li yıllara gelindiğinde ise evlerde bilgisayarların ve internetin hızla yaygınlaştığı görülmüştür.

Farklı amaçlar doğrultusunda her yaş grubuna hitap eden bilgi ve internet teknolojisi; evde, iş yerinde, okulda ve hayatımızın birçok farklı alanında kullanılmaya başlanmış; hayatımızın vazgeçilmez haline gelmiştir. Öyle ki günümüzde birçok bilimsel içerikli yazıda bile elektronik ortamdaki kaynaklara atıflar yapılmaya başlanmıştır (Henkoğlu ve Mahiroğlu, 2015). Yani basılı

materyallerin yerini yavaş yavaş elektronik ortamlar almaya başlamıştır. Bunun nedeni olarak yaşanan hızlı bilgi artışı gösterilmektedir. Üretilen bilginin her yıl %30 oranında arttığı düşünülecek olunursa, bilginin toplamda her üç yılda bir iki katına çıktığını söylemek yanlış olmayacaktır (Henkoğlu ve Mahiroğlu, 2015). Bilgi ve belgenin hızla artıyor olması ve kontrolde yaşanan zorluklar bilgilerin saklanması dijital ortamları zorunlu kılmıştır (Aslıyüksek, 2017). Bu durum bilgilerin çok az miktarının basılı ortamlarda saklanması, büyük oranın ise dijital ortamlara kaymasını sağlamıştır. Artık üniversiteler, devlet kurumları, özel şirketler, askeri kurumlar vb. birçok kurum ve kuruluş bilgilerini basılı ortamlar yerine dijital ortamlarda tutmayı tercih etmeye başlamıştır. Bilgilerin dijital ortamlara kayması, bilgiye internet üzerinden daha kolay ulaşılabilir olması ve bilgi çeşitliliğinin fazla olması; bilgiye ulaşmada bu ortamların tercih edilmesinin temel nedeni olarak görülmektedir. Bu da beraberinde internet ortamlarının kullanım oranlarında hızlı bir artış meydana getirmiştir.

Europa 2018 verilerine göre 2007 yılında Avrupa ülkelerinde internet kullanım oranı %57 iken 2017 yılında bu oran %84'lere ulaşmıştır. Türkiye'de ise bu oran %27'den %65'e çıkmıştır. Dünya geneline bakıldığında ise 2017 yılında 3.71 milyar internet kullanıcısı bulunduğu gözlenmiştir. Yine aynı kurum tarafından paylaşılan oranlara göre; dünya genelinde 2.8 milyar sosyal medya kullanıcısı bulunmaktadır. Bu da yaklaşık dünya nüfusunun %50'si demektir. Gün içerisinde sosyal medya kullanım sürelerine bakıldığında ise; insanların ortalama 2 saat 19 dakika geçirdiği görülmektedir. Ayrıca 4.92 milyar mobil kullanıcı, 1.61 milyar e-ticaret kullanıcısı mevcuttur ("wearesocial", 2017). 2019 sonu 2020 başı Çin'in Wuham kentinde ortaya çıkan Covid-19, bilinen adı ile Corona virüsü dünya genelinde birçok dengenin de değişmesine neden olmuştur. Tüm dünyada olduğu gibi ülkemizde de resmi kurumlarca insanların dışarı çıkmaması yönünde çağrılar yapılmıştır. Alışveriş mağazalarına gitmekten çekinen insanlar birçok ihtiyacını uzaktan karşılamak zorunda kalmıştır. Bu da beraberinde e-ticarette büyük bir sıçramayı getirmiştir. Muratoğlu (2020) bu salgın sonrası e-ticaret sitelerinden yapılan alışverişin kısa süre içinde %80 arttığını belirtmiştir. Yaşanan bu gelişmeler dijital ortamın hayatımızın içine ne kadar girdiğini bir kez daha göstermiştir. Özellikle e-ticaret sistemlerinde alışveriş yapabilmek için kişisel bilgilerin ve banka bilgilerinin paylaşılması gerekmektedir. Gerek sosyal medya kullanım oranları gerek ise internet kullanım oranları düşünüldüğünde dijital ortamlarda kişisel bilgilerin paylaşımının hızla arttığını görmek mümkündür.

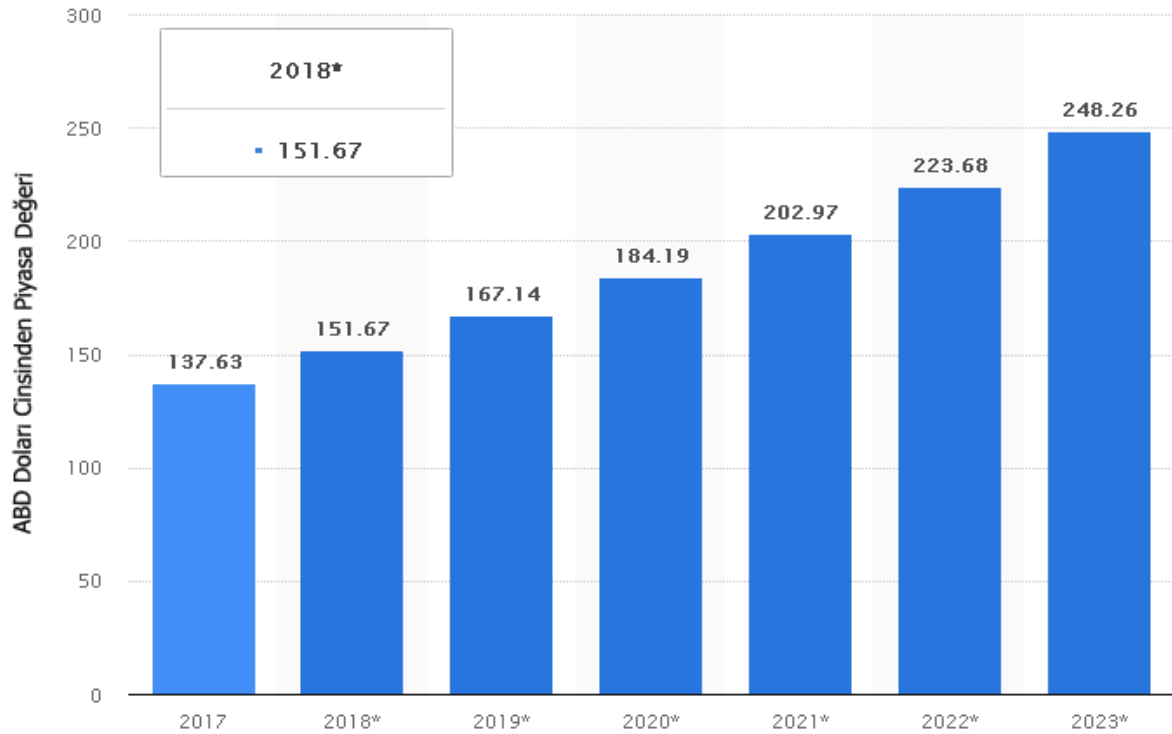
Dijital ortamlar bilgiye ulaşma hızı ve çeşitliliği olarak düşünüldüğünde büyük kolaylık sağlasa da beraberinde büyük bir problem olarak "dijital ortamlara uzaktan erişim" konusunu gündeme getirmiştir. İlk başta avantaj gibi görünse de, bu ortamlarda saklanan bilginin değerinin artması ile birlikte dezavantaj haline dönüşebilmektedir. Çünkü dijital ortamlardaki verilere onlarca farklı yoldan erişmek mümkündür. İnsanların oturduğu yerden işlerini kolayca gördüğü,

iletişim ortamlarının bu kadar yaygınlaştığı ve dijitalleşmenin hızla geliştiği çağda elektronik ortamlardaki bilgilerin değerinin her geçen gün artması kaçınılmaz olmuştur. Dijital ortamda saklanan ya da üretilen bilginin değeri arttıkça; bilgiye ulaşma, onu elde etme isteği ve çabası da bir o kadar artmıştır. Artık dijital ortamlardaki bilgi önemli bir güç haline gelmiştir. Bu gücü elinde tutmak isteyenler çağın teknolojik imkânlarını sonuna kadar kullanma isteğinde olmuşlardır (Evrin ve Demirer, 2011). Özellikle dijital ortamlardaki bilgiye uzaktan erişim imkânının olması güvenlik açıklarının oluşacağı gerçeğini de beraberinde getirmiştir (Vural ve Sağiroğlu, 2018). Bu güvenlik açıklarını bertaraf etmek için çeşitli teknik veya fiziki önlemler alınsa da Barrett (2003)'e göre güvenlik halkasının en zayıf halkası olan insanı aşmak her zaman mümkündür. Peki ama insanlar buna ne kadar hazır? İnsan zaaflarını hedef alan 2005 yılında ortaya çıkmaya başlayan Phishing (sazan avlama ya da oltalama) yöntemi ve Sosyal Mühendislik yöntemlerinin günümüzde kurumlara halen ciddi zararlar yaşatması bu soruya cevap niteliğindedir. Munro'ya (2008) göre sosyal mühendislik sanatı teknik yöntemlere göre daha tehlikeli sonuçlar doğurabilir. Dijital ortamlardaki verinin korunması konusunda bilgi sahibi olmayan insanlara yönelik olan bu iki yöntemin günümüzde de halen çok etkili olmasının en önemli nedeni siber güvenlikte "İnsan" faktörünün göz ardı edilmesinden kaynaklanmaktadır (Erol, 2016). 2018 yılında Savunma Teknolojileri Mühendisliği (STM) tarafından yayınlanan raporda; siber güvenlik olaylarının %34'ünden fazlasının oltalama veya kurum çalışanlarına gönderilen zararlı e-postalar aracılığı ile olduğu vurgulanmıştır (STM, 2018). Bu raporda da vurgulandığı üzere fiziksel önlemlerin hiç biri sosyal mühendislikten korumada yeterli olmayacaktır. Çünkü saldırganların hedefinde güvenlik duvarları ya da web sunucuları yoktur, hedef insandır (Mitnick, Simon ve Wozniak, 2003). Eminağaoğlu'nun (2009) belirttiği gibi; güvenlik önlemleri için fiziki ve teknolojik alt yapılardan daha çok "İnsan" faktörüne yatırım yapılmalıdır. Tüm bu önlemler, yatırımlar ve bilgiyi koruma çabaları "Siber Bilgi Güvenliği " kavramını beraberinde getirmiştir. Çünkü artık bilgiyi korumak, bilgiye erişmek kadar değerli olmuştur (Pekel,2010).

1.1 Araştırmanın Problemi

Bilgi ve iletişim teknolojilerinde yaşanan baş döndürücü hızlı değişim sonrası dijital ortamlar ve internet vazgeçilmezimize haline gelmiştir. İnsanların; alışveriş yaparken, araştırma yaparken, uzaktan iletişim kurarken, arkadaşlıklar edinirken, paylaşımlar yaparken, resmi işlemlerini gerçekleştirirken dijital ortamlardaki verilerden yararlandığı görülmektedir. Fakat bu ortamları kullanırken genellikle çok fazla kişisel bilgilerimizi paylaşıyor olmamız beraberinde bazı problemleri de getirmiştir.

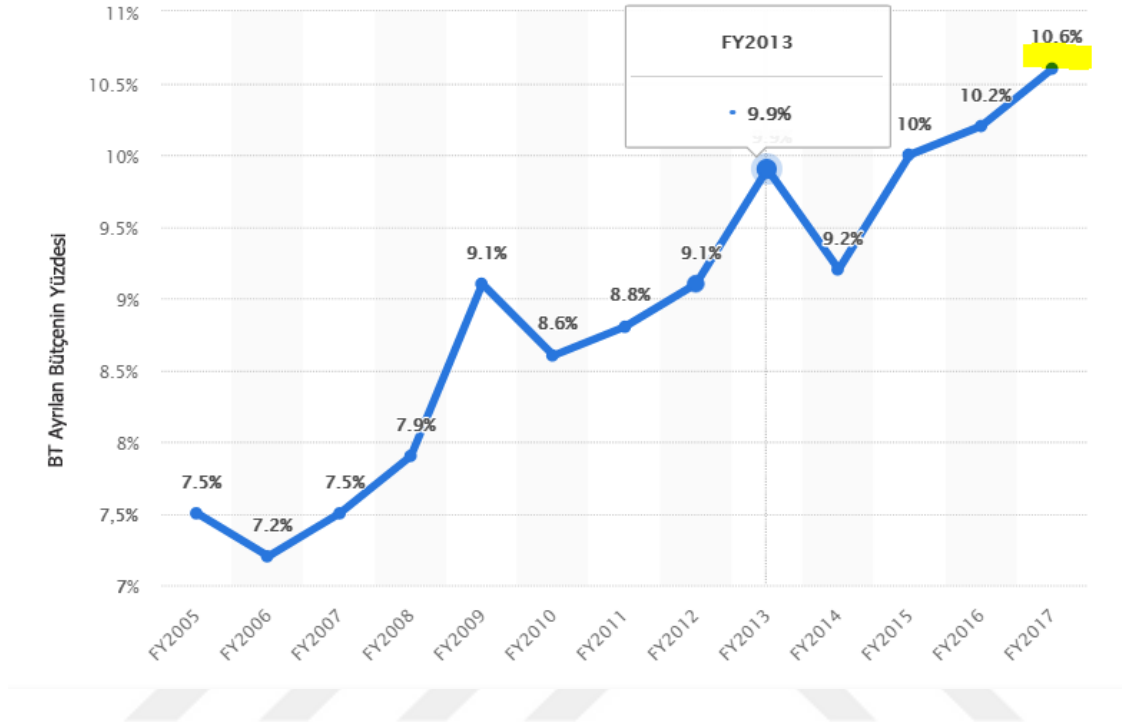
Alan yazın incelendiğinde dijital ortamlardaki verilere yetkisiz kişilerce birçok farklı yoldan erişmemin mümkün olduğu görülmektedir. Bu yollardan en önemlisi günümüzde de günceliğini halen koruyan “Oltalama” dır. Bu yöntemde hedef siber güvenlik konusunda bilgi sahibi olmayan kullanıcıdır. Dijital ortamdaki verilere erişmek için bu yöntemin dışında; kullanıcı bilgisayarlarına virüs yerleştirme, sistem açıklarından yararlanarak bilgisayarlara uzaktan bağlanma veya ele geçirilmek istenen bilgisayara casus yazılımlar kurma gibi daha birçok yöntem sıralanabilir. Oluşabilecek en küçük güvenlik zafiyetleri çok büyük kayıplara yol açabilmektedir. Bu amaçla siber bilgi güvenliğini sağlamak için kurum ve kuruluşlar büyük çabalar sarf etmekte ve bütçelerinden ciddi oranda “Siber Bilgi Güvenliğine” paylar ayırmaktadırlar. Şekil 1.1’de de görüldüğü gibi dünya genelinde “Siber Bilgi Güvenliği ” büyük bir pazara sahiptir.



Şekil 1.1 Statista,2019 Dünya çapında Siber Bilgi Güvenliği Teknolojisinin 2017-2023 arası büyüklüğü (Milyar Dolar)[31]

Statista'nın verilerine göre de siber güvenlik teknolojisi pazarının sürekli artış gösterdiği görülmektedir. Ayrıca bu pazarın 2023 yılında 248 Milyar dolarlar civarına çıkması beklenmektedir. Çünkü dünya çapında kurumlar Siber Bilgi Güvenliği konusunda ciddi tehditler yaşamaktadır. Yine Statista 2017 verilerine göre sadece ABD içerisinde 1478 güvenlik olayı tespit edilmiştir. Dünya çapında ise Siber Bilgi Güvenliği olaylarının 12 aylık maliyeti 578 milyar ABD dolarını bulmuştur. Büyük firmalar ise bunu fırsata çevirmeyi bilmiş, siber güvenlik açıklarına yönelik hizmetlerden ciddi kârlar elde etmiştir. IBM firması 2016 yılında siber güvenlik açıkları

hizmetinden 778 Milyon Dolar kâr elde ettiğini duyurmuştur (Statista,2017). Veriler şirketlerin Ocak 2018 itibarı ile toplam bütçesinin yaklaşık yüzde 10,6'sını siber bilgi güvenliğine harcadığını ve 2006'dan beri nispeten bu bütçe harcamasının artış eğiliminde olduğunu göstermektedir.



Şekil 1.2. İşletmelerin Siber Bilgi Güvenliğine Harcadığı 2005-2017 arası Bütçelerinin Yüzdesi
(Statista,2019) [31]

Bu büyük pazarda her ne kadar fiziki veya teknolojik önlemler alınsa da Eminağaoğlu'nun (2009) üstünde durduğu insan faktörünü göz ardı etmek uzun vadede olumsuz sonuçlar doğuracaktır. İnsan kaynaklı tehditlerin kimisi istemsizce gerçekleşirken, kimisi de kötü niyetli kişiler tarafından bilinçli olarak gerçekleşmektedir. İstemsiz gerçekleşen tehditlerin geneli bilgisizlik, dikkatsizlik veya ihmalkârlık sonucu gerçekleşirken; kötü niyetli kişiler tarafından gerçekleşen tehditlerin birçoğu kurum içindeki personelin yetkisini kötüye kullanması sonucu ortaya çıkmaktadır. Bu kişilere "yerel saldırgan" adı verilmektedir (Güldüren, 2015). Yerel saldırganlar kimi zaman o kuruma bu saldırıyı gerçekleştirmek amacı ile sızmış personeller olurken, kimi zaman da dışardan bu iş için belirli vaatler ile ikna edilmiş personellerden oluşmaktadır. Teknolojik olarak ne kadar önlem alınırsa alınsın insan faktöründen kaynaklı tehditleri tamamen ortadan kaldırmak pek mümkün değildir. Fakat minimize etmek için sadece teknolojik önlemler almak da yeterli değildir. Çünkü Barrett' in (2003) de belirttiği gibi siber güvenlik boyutlarından en zayıf halka halen insandır. Deloit firmasının Teknoloji Medya Telekomünikasyon(TMT) Küresel araştırma 2011 raporuna göre son yıllarda şirketler

güvenlikleri için daha fazla para harcaması gerekirken, ekonomik kriz gibi nedenlerle ayırdıkları bütçeleri azaltmışlardır. Diğer yandan yine bu firmanın yapmış olduğu bir araştırmada “Kurumunuz 2011 yılı içindeki siber güvenlik girişimi nedir?” sorusuna çalışanların sadece %27 “siber güvenlik eğitimi farkındalığı” cevabını vermiştir(s.8). Kurumlar ekonomik olarak bir şeylerden kısması durumunda kaldıklarında tercihlerini güvenlik önlemlerine ayırdıkları bütçeden yana kullanabilmektedir. Dahası kurum çalışanlarının yarısına bile siber bilgi güvenliği farkındalığı eğitimleri vermeyi düşünmemektedir. Oysa insana yapılan yatırımların fazladan bir maliyetmiş gibi görülmemesi gerekmektedir. Siber bilgi güvenliğinin sağlanması için toplumun bilinçlendirilmesi, farkındalık eğitimlerinin gerçekleştirilmesi gerektiği belirtilmektedir (Eminağaoğlu, 2009). Siber bilgi güvenliğe yüksek maliyetler harcamak ve yüksek teknolojik imkânlar kullanmak yerine; insanların bilinçlendirilmesinin daha önemli olduğu vurgulanmaktadır (Puhakainen,2006). Yine Hekim ve Başbüyük (2013) de siber bilgi güvenliği konusunda insanlara eğitimler verip bilinçlendirilmesi gerektiğini vurgulamıştır.

Siber bilgi güvenliği konusunda bilgi sahibi olmayan insanların güvenlik sürecini aksatma ihtimalleri oldukça yüksektir. Bu da siber bilgi güvenliği zafiyetinin yol açtığı sonuçlar açısından fazladan mali yük demektir. Bunun önüne geçilebilmesi için eğitim sisteminde toplumu oluşturan bireylerin siber bilgi güvenliği ve dijital vatandaşlık konusunda eğitilmesi ve siber güvenlik açısından bilgi ve beceri sahibi bireyler olarak yetiştirilmesi önerisini ortaya çıkarmaktadır. Bu eğitimi ilköğretim kademesinden başlayarak ortaokul ve lise seviyesinde yeni nesillere aktaracak olan öğretmenlere büyük rol düşmektedir. Milli Eğitim Bakanlığı(MEB) görevde bulunan öğretmenlerine Siber Bilgi Güvenliği Farkındalığı anketi uygulamış, sonuçlar görevde bulunan öğretmenlerin de siber güvenlik farkındalıklarının düşük olduğunu göstermiştir (MEB,2012). Gökmen (2015) ise aynı yıl Bilgisayar ve Öğretim Teknolojileri Eğitimi öğretmen adaylarının bilişim güvenliği eğitimi vere bilme yeterliliklerini ölçtüğü çalışmada Bu konuda eğitim vermede yeterli olmadıkları sonucuna ulaşmıştır. Kaya'nın (2014) öğretmen adaylarının dijital vatandaşlık algılarını ölçtüğü çalışmada, öğretmen adaylarının bu kavramın tanımını tam olarak bilmediği sonucuna varmıştır. Alan yazında buna benzer çalışmalar olmasına rağmen farklı bölümden öğretmen adaylarının dijital vatandaşlık düzeylerinin ve siber güvenlik farkındalıklarının birlikte ölçüldüğü çalışmaya rastlanmamıştır. Dijital vatandaşlığı 9 alt boyuta ayıran Ribble ve Mike (2011) bu boyutlardan birinin de siber güvenlik olduğunu vurgulamıştır. Dolayısı ile siber bilgi güvenliği farkındalığı ile dijital vatandaşlık arasında bir ilişki olup olmadığı araştırılması gereken bir konudur. Bu amaçla gelecek nesillerin yetiştirilmesinde büyük ölçüde sorumlu öğretmen adaylarının siber bilgi güvenliği farkındalıklarının ve dijital vatandaşlık düzeylerinin ölçülmesi, aralarındaki ilişkinin tespit edilmesi oldukça önemlidir. Çıkacak sonuçlara göre dijital vatandaşlık ve siber bilgi güvenliği konusunda yapılacak en önemli yatırımın insan olduğu düşünülerek

gerekli eğitimlerin verilmesi gerekmektedir. Türkiye de yapılan çalışmaları destekler nitelikte Almanya da Beyer ve Westendorf (2009)' tarafından siber güvenlik ve internet güvenliği konusunda yapılan çalışma sonucunda; öğretmenlere riskler ve bunların olası sonuçları ile ilgili eğitimler verilmesi gerektiğine vurgu yapılmıştır. Yine Mahabi (2010) Florida Eyalet Üniversitesinde siber güvenlik üzerine yapmış olduğu çalışmasının sonucunda; kullanıcıların saldırılara karşı bir farkındalık eğitimine ihtiyaçları olduğunu görmüştür.

1.2. Araştırmanın Amacı

Bilgi toplumuna geçiş, vatandaşlık kavramının farklı boyutlar kazanmasına neden olmuştur. Dijital vatandaşlık da bu boyutlardan bir tanesidir. Dijital vatandaşlık kavramının alt boyutları incelendiğinde ise siber güvenlik yer almaktadır. Bilginin her yıl bir önceki yıla göre %30 arttığı bir çağda verilerin dijital ortamlar dışında saklanması zor bir hal almıştır. Bu kadar hızlı bilgi artışı ve dijitalleşme beraberinde birçok problemi de getirmiştir. Bu problemlerin başında “ Siber Bilgi Güvenliği” gelmektedir. Gerekli fiziki önlemler alınmasına karşın siber bilgi güvenliğinin tamamen sağlanması pek mümkün değildir. Çünkü güvenliğin en zayıf halkası insandır ve bu zayıf halkayı aşmak mümkündür (Barrett, 2003). Bu araştırmanın amacı; insan üzerinde küçük yaşlardan itibaren büyük etkilere sahip öğretmen adaylarının Siber Bilgi Güvenliği Farkındalıkları ile Dijital Vatandaşlık seviyelerinin çeşitli değişkenler açısından belirlenmesi ve iki değişken arasındaki ilişki durumunun tespit edilmesidir. Bu amaçlar doğrultusunda aşağıdaki sorulara cevaplar aranacaktır.

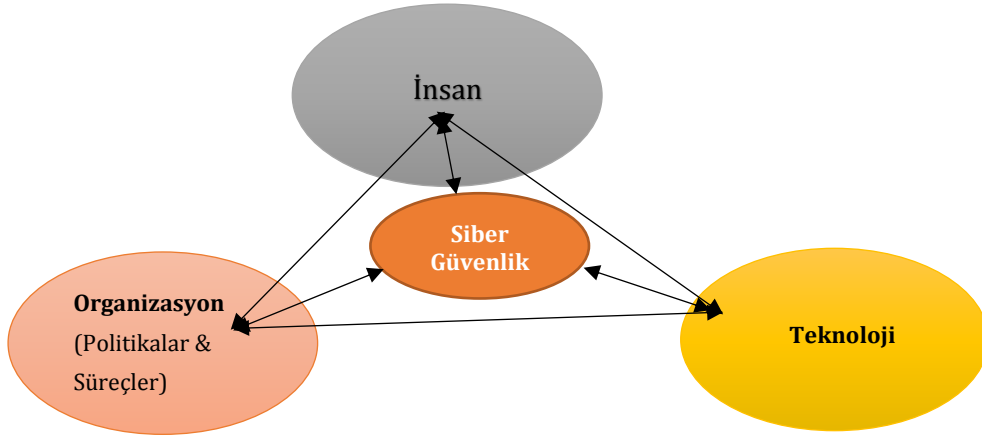
1.3. Araştırma Soruları ve Alt Araştırma Soruları

1. Öğretmen adaylarının siber bilgi güvenliği farkındalıkları ne düzeydedir?
 - a. Öğretmen adaylarının siber bilgi güvenliği farkındalıklarında cinsiyetlerine göre anlamlı bir fark var mıdır?
 - b. Öğretmen adaylarının siber bilgi güvenliği farkındalıklarında öğrenim gördükleri kademeye göre anlamlı bir fark var mıdır?
 - c. Öğretmen adaylarının siber bilgi güvenliği farkındalıklarında öğrenim gördüğü bölümlere göre anlamlı bir fark var mıdır?
 - d. Öğretmen adaylarının siber bilgi güvenliği farkındalıklarında günlük teknoloji kullanım süresilerine göre anlamlı bir fark var mıdır?
 - e. Öğretmen adaylarının siber bilgi güvenliği farkındalıklarında günlük sosyal medya kullanım süresilerine göre anlamlı bir fark var mıdır?

2. Öğretmen adaylarının dijital vatandaşlık ve seviyeleri ne düzeydedir?
 - a. Öğretmen adaylarının dijital vatandaşlık düzeyleri ve alt boyutları açısından cinsiyetlerine göre anlamlı bir fark var mıdır?
 - b. Öğretmen adaylarının dijital vatandaşlık düzeyleri ve alt boyutları açısından öğrenim gördükleri kademeye göre anlamlı bir fark var mıdır?
 - c. Öğretmen adaylarının dijital vatandaşlık düzeyleri ve alt boyutları açısından öğrenim gördüğü bölgelere göre anlamlı bir fark var mıdır?
 - d. Öğretmen adaylarının dijital vatandaşlık düzeyleri ve alt boyutları açısından günlük teknoloji kullanım süresilerine göre anlamlı bir fark var mıdır?
 - e. Öğretmen adaylarının dijital vatandaşlık düzeyleri ve alt boyutları açısından günlük sosyal medya kullanım süresilerine göre anlamlı bir fark var mıdır?
3. Öğretmen adaylarının siber bilgi güvenliği farkındalık puanları ile dijital vatandaşlık puanları arasında istatistiksel olarak anlamlı bir ilişki var mıdır?

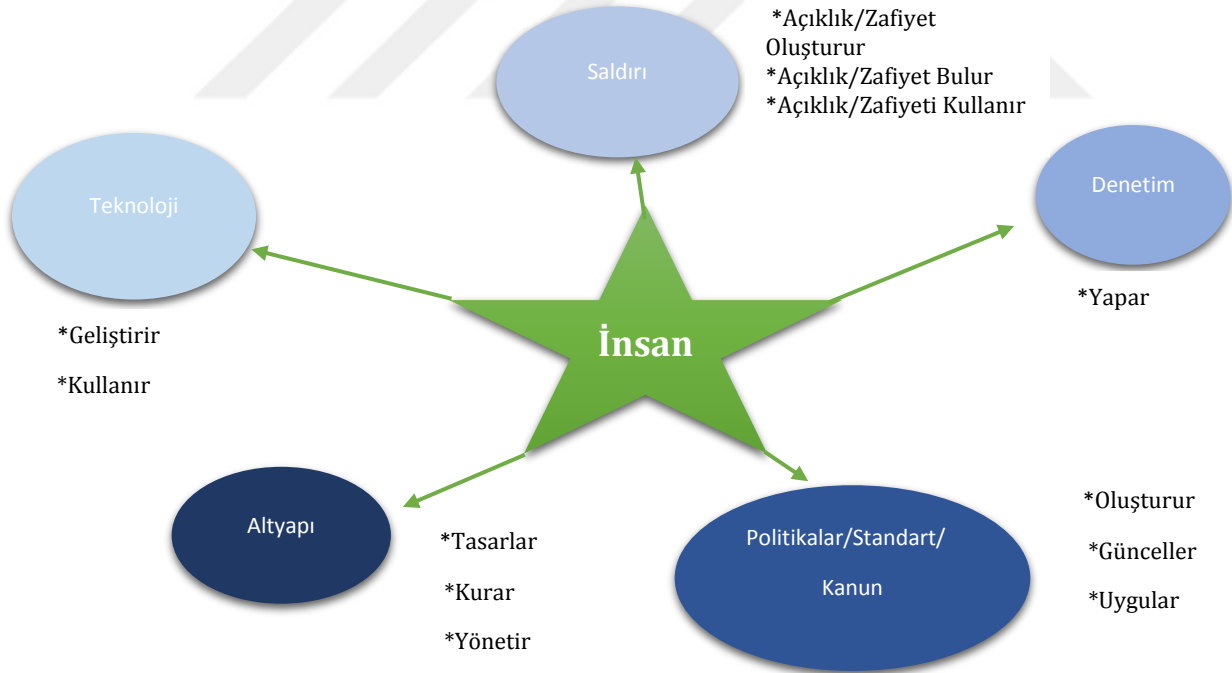
1.4.Araştırmanın Önemi

Bilgi toplumuna geçişin temelini teknoloji oluşturmuş, bilgi ise toplum için bir güç haline gelmiştir. Bilgisayar teknolojileri ve yoğun bilgi üretimi değer kazanırken; bilgi ekonominin önemli faktörlerinden olmuştur. Hızla gelişen internet teknolojisi sonucu; 1990'lı yılların başında tüm telekomünikasyon ağlarının yalnızca %1 i üzerinden bilgi transferi gerçekleşirken, 2000 yılında bu oran %51'e 2007 de ise %97 ye çıkmıştır (Warnes ve Kathy, 2017). Teknolojide yaşanan gelişmeler bilginin dijital ortamlarda depolanmasına ve bilgiye uzaktan erişilmesine imkân vermiştir. Özellikle bu tür ortamlarda saklanan bilginin değeri arttıkça, kötü niyetli kişilerin bilgiyi elde etme çabaları da bir o kadar artmıştır. Birçok işini dijital ortamda sürdüren şirket ve devlet kurumları için bu ciddi bir tehlike haline gelmiştir. Bu tehlikenin farkında olan şirket ve devlet kurumları "siber bilgi güvenliği" sağlamak için maddi anlamda ciddi yatırımlar yapmaya başlamıştır. Siber bilgi güvenliğine bütçelerinden büyük oranlar ayırmışlardır. Fakat genel olarak fiziki önlemler almayı tercih etmişler, insan faktörünü ikinci plana atmışlardır(Sağiroğlu, 2018). Oysa IBM firmasının 2015 yılında yayınladığı raporda yaşanan siber güvenlik ihlallerinin %95 'inin insan kaynaklı olduğu vurgulanmıştır. Literatürde bu raporu destekleyecek birçok çalışmanın olması insan faktörünün ne denli önemli olduğunu göstermektedir. Rao ve Nayak (2014) siber güvenlik organizasyonunda insanın rolünü gösteren şemada; insanı yapıyı oluşturan ayaklardan biri olarak göstermiş, Şekil 1.3 te gibi şu şekilde özetlemiştir.



Şekil 1.3. Siber Güvenlik Katmanları[140]

Rao ve Nayak (2014) tarafından oluşturulan şemada görüldüğü gibi siber güvenlik katmanlarının ayaklarından birisi insandır. Dolayısı ile bu katmanda yaşanacak herhangi bir aksaklığın tüm güvenlik sürecini aksatacağı söylenebilir. Sağiroğlu ve Erol (2018) ise siber bilgi güvenliği sürecinde insan faktörünü Şekil 1.4'te özetlemiştir.

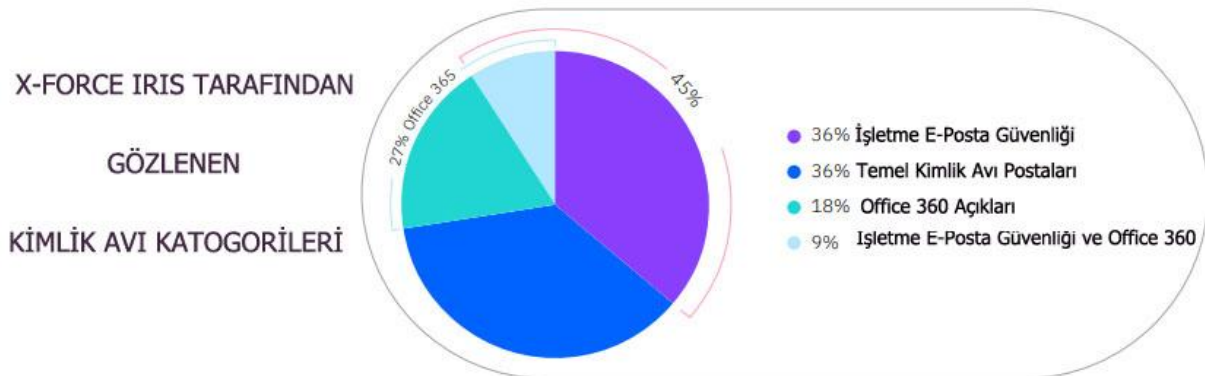


Şekil 1.4. İnsan Siber Güvenlik Unsurları İlişkisi[141, s.111]

Sağiroğlu ve Erol'un (2014) yukarıdaki şekilde de özetlediği gibi insanın siber güvenlik sürecinin bir parçasından daha çok sürecin temel unsuru olduğunu söylene bilir. Siber bilgi güvenliği sürecindeki; teknolojinin geliştirip kullanılması, alt yapının tasarlanıp-kurulup-yönetilmesi, politika standartlarının ve kanunun oluşturulması-güncellenip-uygulanması, denetimin yapılması, saldırılarda zafiyetin yaratılması-zafiyetin bulunması-zafiyetin kullanılması insan faktörüne bağlıdır. İnsanın siber güvenlik organizasyonunda merkezde yer aldığı düşünüldüğünde tek başına fiziksel önlemlerin yeterli olmayacağını söylemek mümkündür.

Yakın zamanlarda fiziki önlemler almanın tek başına yeterli olmadığını anlaşılmasıyla birlikte insan faktörüne de yatırımlar yapılmaya başlanmıştır. Bu da şirketlere ve devlet kurumlarına fazladan bir maliyet getirmiştir. Fakat bilinmesi gereken internet teknolojisinin yayılması ile birlikte ülke sınırları haritalardan ibarettir. İnsanlar yerleşik hayata geçmesinden bu yana buldukları toprakları hep koruma içgüdüsünde olmuştur. Toprak kimi toplulara göre namus ile nitelendirirlerken, kimi toplularda ise gücün simgesi olmuştur. Günümüzde toplumlar bilişim toplumlarına dönüşmüşken, topraklar da dijital topraklara dönmüştür. Dolayısı ile saldırılar da siber saldırı olarak gerçekleştirilmektedir. Dünya genelinde anlık siber saldırıları görüntüleyebildiğimiz "cybermap.kaspersky.com.tr" sitesi anlık verileri incelendiğinde Türkiye en çok saldırı alan 18. ülke konumundadır (Kaspersky, 2019). Gerek devletlerin gerekse üst düzey finansal güce sahip şirketlerin verileri saldırılara maruz kalmaktadır. Özellikle gelişen bulut teknolojileri verilerin sanal ortamlarda depolanmasına imkân verse de beraberinde bazı sorun getirmiştir. Fakat güvenli olmayan bulut veri tabanları, yanlış yapılandırılmış bulut sunucuları 2018 yılında 990 milyon kaydın ortaya çıkmasına neden olmuştur (IBM, 2018).

Bunun yanı sıra Şekil 1.3'te görüldüğü gibi insan zaaflarından yararlanılarak gerçekleştirilen siber güvenlik olayları da oldukça fazladır.



Şekil 1.5. 2018'de X-Force IRIS Tarafından Gözlenen Phishing Kategorileri (IBM, 2019) [30]

2018 yılında X-Force IRIS tarafından açıklanan ortalama kategorilerine göre %36 oranında Business Email Compromise(İşletme E-posta Güvenliği)(BEC) ilk sırada yer almaktadır. Bu saldırı genellikle yurt dışına yüklü miktarda para transferi yapan şirketleri veya yöneticilerini hedef alır. Yetki sahibi kişilerin bilgisayarına Office programları üzerinden sahte giriş bağlantıları yollar. Kişiler bağlantıya tıklayıp giriş yaptıklarında hesapları ele geçirilmiştir. Daha sonra bu yetkili kişilerin hesaplarını kullanarak müşterilerine meşru görümlü e-postalar gönderip farklı banka hesaplarına para yatırması istenir. Bu durum hem müşterilerin hem de kurumların mağdur olmasına neden olmuştur. Zira Federal Bureau of Investigation(FBI) son yıllarda Amerika'da ve Dünya da yaşanan BEC saldırılarının 12,5 milyar dolar olduğunu belirtmiştir. Kimlik avı saldırılarının ikinci sırasında ise %36 Basic Phishing Emails gelmektedir. Daha sonra onu sırasıyla %18 Office 365 Compromises ve BEC and Office 365 Mix gelmektedir (IBM,2018). Ülkeler ve kurumlar bu kadar siber güvenlik olayları ile karşı karşıya iken ülkemizde olayın ehemmiyeti yeni anlaşılmaya başlamıştır. Sevri ve Topaloğlu (2016)' ya göre ülkemizin 20.000 siber güvenlik uzmanına ihtiyacı olduğu ön görülmektedir. Ülkemizde en büyük sorunlardan bir tanesi yetişmiş uzman eksikliğidir.

İnsan kaynaklı saldırıların bu kadar fazla olduğu toplumlarda geçmişten gelen toprakları koruma içgüdüsünün siber toprakları koruma güdüsü olarak devam etmesi oldukça önemlidir. Bilgiye sahip olmanın çok değerli olduğu bilişim toplumlarında, yeni nesillerin dijital vatandaşlık seviyelerinin yüksek olması istenen bir durumdur. Yeni nesiller bu özelliklere sahip olurlarsa bilgi çağı ve bilişim toplumu diye adlandırılan günümüzde kendilerini ve buldukları çevrimiçi ortamları olası siber saldırılara karşı daha iyi koruyabileceklerdir. Bu nesillerin dijital vatandaşlık ve siber bilgi güvenliği farkındalık seviyelerini yükseltecek olanlar ise öğretmenler ve öğretmen adaylarıdır. Özellikle öğretmen adaylarının siber bilgi güvenliği farkındalık ve dijital vatandaşlık seviyelerinin belirlenmesi ve buna göre aksiyon planlarının yapılması gerekmektedir. Bu çalışmada öğrencilerin erken yaşta siber güvenlik konusunda eğitilmelerinde önemli rol oynayabilecek geleceğin öğretmenleri olan öğretmen adaylarının (eğitim fakültesi öğrencilerinin) siber güvenlik farkındalıklarının ve dijital vatandaşlık seviyelerinin belirlenmesi amaçlanmaktadır. Bunu sağlamak için en uygun ve en az maliyetli yol ise; küçük yaşlardan beri toplumun neredeyse her kesimine dokunan öğretmenleri bu işe dâhil etmektir. Bu çalışma ile henüz fiilen öğretmenlik görevine başlamamış öğretmen adaylarının siber bilgi güvenliği farkındalıkları ve dijital vatandaşlık düzeyleri belirlenmiş, aralarındaki ilişki tespit edilmiştir.

1.5.Araştırmanın Sayıtları

- ✓ Veri araçlarına verilen cevapların doğru ve samimi olduğu.

1.6. Araştırmanın Kapsam ve Sınırlılıkları

- ☐ Araştırma Akdeniz Bölgesinde yer alan bir Devlet Üniversitesinin Eğitim Fakültesi'nde öğrenimine devam eden öğretmen adayları ile sınırlıdır.
- ☐ Araştırma 2019-2020 eğitim öğretim yılı ile sınırlıdır.
- ☐ Araştırma Akdeniz Bölgesinde yer alan bir Devlet Üniversitesinin Eğitim Fakültesi'nde öğrenci kabul eden 8 bölüm ile sınırlıdır.



2.KAYNAK ARAŞTIRMALARI/ ALAN YAZIN

Bu bölümde DV, SBG ve SGBF kavramlarına ve araştırma kapsamında ön plana çıkmış bazı tanımlara yet verilmiştir.

2.1. Dijital Vatandaşlık

İlk kez Yunan devletlerinde kullanılmaya başlayan vatandaşlık kavramı Fransız İhtilali ile birlikte günümüzdeki şeklini almıştır. (Nalbant, 2014). Vatandaşlık kavramını genel anlamda toplumda üzerine düşen vazifeleri yerine getiren, toplumla uyumlu, çağa ayak uyduran birey olarak tanımlamak mümkündür (Sarıbay, 1992). Dijital vatandaşlık ise; teknolojinin hızla ilerlediği, birçok işlemin dijital mecralar aracılığı ile yapıldığı çağımızda yeni bir terim olarak ortaya çıkmıştır. Dijital vatandaşlık aslında geçmişten günümüze süre gelen vatandaşlığın bir biçimi olarak karşımıza çıkmaktadır. Bilgi edinmek adına teknolojiyi ve kitle iletişim araçlarını doğru bir şekilde kullanan bireylere ise “Dijital Vatandaş “ denilmektedir (Şimşek ve Şimşek, 2013). Mossberger (2007) İnternet’i düzenli kullanan, topluma çevrimiçi yollar ile katılan bireylere dijital vatandaş derken; Farmer (2010) ise İnternet aracılığı ile bilgilere kolay bir şekilde ulaşan, dijital ortamları etkin kullanan, günlük hayatta kendinden beklenenleri dijital mecralarda da sergileyen bireylere dijital vatandaş demiştir.

Ohler (2011) okullarda nasıl uzun yıllardır vatandaşlık eğitimleri veriliyor ise dijital vatandaşlık eğitimlerinin de verilmesinin gerekliliği belirtilmektedir. Zira teknolojiyi gerek eğitim ortamlarında gerek ise dışarda olumsuz yönde kullanma oranı her geçen gün artmaktadır (Kaya ve Kaya, 2014). Son yıllarda kullanımı hızla artan sosyal medya dijital vatandaşlık kavramında da değişmelere neden olmuştur. Farmer’ın (2010) yapmış olduğu tanıma bir de sosyal medyayı etkili ve doğru kullanan kavramları eklenmiştir. Özellikle sosyal medya kullanım yaşının hızla düştüğü son yıllarda öğrencilerin dijital vatandaşlık konusunda bilinçsizliği olası tehditleri de beraberinde getirmektedir. Farmer’a (2014) göre öğrencilere teknolojiyi doğru şekilde kullanmaları konusunda verilecek eğitimler onların dijital vatandaş olmalarına yardımcı olacaktır. Dijital vatandaşlık farkındalığı eğitiminin verilmesi için eğitim ortamlarının düzenlenmesi ve toplumun birçok kesimine hitap eden öğretmenlerin bu hususta farkındalıklarının oluşturulması gerekmektedir. Bunun için de henüz göreve başlamadan eğitim fakültelerinde öğretmen adaylarının dijital farkındalık düzeyleri ölçülerek gerekli çalışmalar yapılmalıdır. Kaya ve Kaya’nın (2014) öğretmen adaylarının dijital vatandaşlık algılarını ölçmeye yönelik yapmış oldukları çalışma da göstermektedir ki; öğretmen adayları dijital vatandaşlık kavramını tam olarak bilmemekte, bu kavramı tanımlarken “dijital” ve “vatandaş” kavramlarının tanımından yola çıkarak bir çıkarım yapmaktadır.

Ribble ve Mike (2011) yayınlamış oldukları kitapta; iyi bir dijital vatandaş olabilmek için teknolojiyi en iyi şekilde kullanmanın gerekliliğini vurgulamıştır. Dijital vatandaşlık kavramının

sadece çocuklar için değil herkes için önemli olduğu üzerinde durulmuş, özellikle toplum geneline yaygınlaştırılmak için erken yaşlarda buna yönelik eğitimlerin verilmesi gerekliliğinden bahsedilmiştir. Bu sayede uygunsuz teknolojik davranışların nerede olunursa olsun fark edilebileceği vurgulanmıştır. Ayrıca dijital vatandaş olan bireylerin başkalarının teknolojiyi olumlu ve doğru bir şekilde kullanmasına yardımcı olacağına değinilmiştir. Yaratılan farkındalığın herkesi daha iyi bir dijital vatandaş yapacağı, teknolojiyi kullanırken keyif alan bireyler oluşturacağını vurgulamışlardır. Dijital vatandaşlığı dokuz boyuta ayırarak bu boyutların anlaşılmasının dijital vatandaşlık kavramını anlamada ve kazanmada oldukça önemli olduğunu belirtmişlerdir. Bu dokuz boyut;

1.Dijital Güvenlik: Bu boyutta daha çok verilerin elektronik ortamda korunması konusunda gerekli önlemler alınıyor mu, bilgileri korumak için gerekli zaman ayırıyor mu sorularının üzerinde durulmuştur. Siber güvenlik kavramı Klimburg (2012)'e göre ise dijital ortamları, interneti ve sunucuları korumak amacı ile alınan önemlerdir. Tanımdan da anlaşılacağı gibi bu iki kavramın birbiri yerine kullanılmaktadır. Bilginin dijital ortamlara kayması ile birlikte alınan güvenlik önlemleri de bu yöne doğru eğilim göstermiştir. İyi bir dijital vatandaş olabilmenin şartlarından birisi de siber ortamlardaki bilgilerin değiştirilmesi, kaybolması, çalınmasına karşı farkındalık sahibi olmaktır.

2.Dijital Erişim: Bu topluma katılımın sağlanması ile ilgilidir. Yani istenirse dijital topluma gerekli olan seviyede katılım sağlanabilir mi ile ilgili bir kavramdır. Kırık, Bölükbaş ve Cengiz (2019) dijital erişimi; dijital vatandaşlığın bir gereksinimi olarak belirtmiş, her vatandaşın teknolojiye erişmesi ve onu yaygınlaştırması gerektiğini vurgulamıştır. Çubukçu (2013)'ya göre bir dijital vatandaşın çeşitli zararlı ortamlara erişim sağlayabilir, bu ortamlar aracılığı ile zarar görebilir. Bu yüzden iyi dijital vatandaş olmanın kurallarından birisi de sanal ortamlardan doğru ve güvenilir bilgiye ulaşmaktır.

3.Dijital Ticaret: Kullanıcılar güvenli e-ticaret ve alışveriş konusunda yeteri kadar bilgi sahibi olup olmamaları ile ilgilidir. Son yıllarda alışverişlerin sanal ortamlara kayması dijital vatandaşlığın boyutlarını da genişletmiştir. Dünya genelinde yaklaşık 1.61 milyar e-ticaret kullanıcısı olduğu bilinmektedir(wearesocial, 2017). Bu kullanıcıların dijital ticaret konusunda bilgi sahibi olmaları onların dijital vatandaşlık seviyelerini de etkilemektedir. Bu yüzden dijital ticaret iyi bir dijital vatandaş olmanın basamaklarından biridir. İyi bir dijital vatandaş; dijital bankacılığı kullanırken ve dijital ortamlar vasıtası ile ticaret yaparken her hangi bir güvenlik zafiyeti yaratmamalıdır.

4.Dijital İletişim: Elektronik bilgi alışverişi ile ilgili olan bu boyutta kitle iletişim araçlarının doğru kullanımı konusunda gerekli özenin gösterilmesi beklenmektedir. Son yıllarda gelişen farklı iletişim mecraları iletişim yöntemlerini ve çeşitlerini de etkilemiştir. Yeni medya

teknolojilerinin gündeme gelmesi, insanların iletişim sürecine doğrudan dâhil olmasını sağlamıştır. Bu iletişim sürecinden köklü değişmelere neden olmuş, hedefin de kaynağa bilgi aktardığı bir yapıya dönüşmüştür (Bayrak, 2018). Özellikle sosyal medya gibi herkese açık ortamlarda kişisel bilgilerin paylaşılıyor olması çeşitli güvenlik ihlallerini de beraberinde getirmiştir(Çubukçu,2013). Bu tür ortamlarda kurulan iletişimlerde karşı taraftaki kişilerin gerçek kimliğini sakladığı da görülmektedir. Özellikle sosyal medya gibi herkese açık iletişim ortamlardaki kullanıcı sayılarının hızla artıyor olması dijital iletişim boyutunun önemini artırdığını söylemek mümkündür.

5.Dijital Okuryazarlık: Teknolojinin kullanımı ile ilgili öğrenme ve öğretme sürecidir. Kişilerin teknoloji kullanımı için harcadıkları zaman ve bununla ilgili bilgilerini başkaları ile paylaşımları ile ilgilidir. Ayrıca dijital okuryazarlık bireyin sadece teknolojiyi iyi kullanma becerileri yanı sıra onun bilişsel, duyuşsal, motor, sosyolojik ve psikolojik durumlarını da içermektedir (Eshet, 2004). Son yıllarda doğan çocukların normal okul yazarlık hayatına başlamadan dijital araçlar ile tanıştığı görülmektedir. Bireylerin bu tür ortamlarla çok erken yaşlarda tanışması onları çok daha savunmasız kılmaktadır. Bu karşılaşacakları riskleri en aza indirmek adına dijital okuryazarlık boyutuna önem verilmesi gerekmektedir.

6.Dijital Etik: Teknoloji kullanıcılarının elektronik ortamları kullanırken başkalarının haklarını düşünmesi ve hak ihlallerinde bulunmaması ile ilgilidir. Çakmak (2016) dijital etiği; dijital ortamları kullanırken diğer kullanıcıların hoşuna gitmeyecek davranışlardan kaçınma olarak tanımlamıştır. Dijital etik kavramı; etik kavramında olduğu gibi evrensel felsefi prensipler üzerine kurulmuştur. Sonuca giden her yol doğrudur felsefesini reddetmektedir.(Mahmutoğlu, 2009). Dijital etiği ihlal eden bazı davranışlar Ocak (2013) tarafından;

- Yanlış bilgi yayma
- Kişisel verilerin izinsiz elde edilmesi
- Siber zorbalık davranışları
- Özel yaşam ihlalleri
- Telif hakkı ihlalleri
- İntihal olarak sıralanmıştır(s.21).

İyi bir dijital vatandaş olmanın yolunun dijital etik boyutundan da geçtiği görülmektedir. Dijital etik kavramı insanların sadece kaçınması gereken davranışları içermemektedir. Bunun yanı sıra kendi iradesi ile gerçekleştirmesi gereken olumlu davranışları da içermektedir.

7.Dijital Hukuk: Dijital ortamlarda yapılanların elektronik sorumluluğu ile ilgilidir. Kullanıcı teknolojiyi kullanırken uyması gereken kuralların farkında olmalarına odaklanılmaktadır. Kimi zaman bireylerin geçek hayatta uymakta zorluk çekmediği kurallara dijital ortamlarda uymakta zorlandığı görülmektedir. İyi bir dijital vatandaşta aranan

özelliklerden birisi de gerçek hayatta suç olan davranışlarının dijital ortamlarda suç olduğunu bilmesidir.

8.Dijital Hak ve Sorumluluklar: Dijital ortamların kullanımında kişiler sahip olduğu hakların farkında olup olmadığı ile ilgili kavramdır. Birey dijital ortamda paylaştığı, bir içerikten veya yaptığı davranıştan sorumlu olduğunu bilmelidir. Kendi bir hak ihlaline uğradığında da şikâyet hakkını kullanmasını bilmelidir (Çubukçu, 2013). İyi bir dijital vatandaş hangi davranışın suç olduğunu bilmeli, ne gibi sonuçlar doğuracağını farkında olmalıdır. Dijital ortamları kullanırken özgürlük alanını ve sınırlarını doğru tespit etmelidir. Diğer bireylere karşı sorumlulukların farkında olmalı, bu sorumlulukları yerine getirmek için çaba harcamalıdır.

9.Dijital Sağlık: Dijital ortamların kullanımı sırasında gerek fiziksel gerek ise psikolojik riskler göz önüne alınıyor mu sorusuna cevap arar. Dijital ortamların kullanımında en önemli problemlerin başında fiziksel ve ruhsal sorunlar gelmektedir. Bilinçsiz teknoloji kullanımı sonucu yaşanan; göz bozukluğu, duruş bozuklukları, ergonomik oturmama nedenli kas ağrıları, eklem ağrıları gibi fiziksel sorunlarla karşılaşmam mümkündür. Bunun yanı sıra teknoloji bağımlılığı, şiddete meyil, stres gibi ruhsal sorunlarla da karşılaşmak mümkündür. Ayrıca temelinde internetin bilinçsiz kullanımının yattığı yeni nesil hastalıklar olarak adlandırılan bazı hastalıklarda dijital sağlık kapsamına girmektedir (Özsoy, 2009).

Tüm bu boyutlar birleşerek dijital vatandaşlığın kendisini oluşturmaktadır. Bunlar birbirinden bağımsız düşünülemez ve birinde yaşanan olumsuz dijital vatandaşlık kavramını olumsuz etkiler.

2.2.Siber Bilgi Güvenliği

Dijital Vatandaşlığın bir boyutu olarak kabul edilen Siber Güvenlik kavramı içerisinde birçok etmeni barındırır. Klimburg'e (2012) göre siber güvenlik; bilgi ve iletişim teknolojileri, internet güvenliği, ağ güvenliği, bilgi güvenliği, kritik bilgi ve alt yapı güvenliği kavramlarının merkezinde bulunan bir çekirdek görevini üstlenir. İlk ortaya çıkışı 2000 yıllarda milenyum yazılım hatasının gündeme gelmesi ile olmuştur. Siber güvenlik kavramının tanımını geniş çapta belirleyen ülkelerden bir tanesi de Hollanda idi. Hollanda Güvenlik ve Adalet Bakanlığı siber güvenliği; dijital ortamda depolanan verilerin bozulma, yanlış kullanımdan kaynaklı hasar görme, bilginin gizliliğinin ihlali veya bilginin bütünlüğünün bozulmasına karşı alınan tedbirler olarak tanımlamıştır. Yine Uluslar Arası Telekomünikasyon Birliği'nin (ITU) yaptığı tanıma göre siber güvenlik; kullanıcıların ve kuruluşların elektronik ortamdaki doküman, belge, kişisel veri gibi çeşitli önemli bilgileri korumak adına yapılan uygulamalar ve geliştirilen politikaların bütünü olarak açıklanmaktadır (Aytekin, 2015). Görüldüğü üzere siber güvenlik tek bir yapının korunması anlamına gelmemektedir. Aksine birçok sistemin eşgüdüm halinde olmasını zorunlu

kılmıştır. Günümüz şartları düşünüldüğünde birçok tehdittin siber ortamlar aracılığı ile geldiğini görmek zor olmayacaktır. Gerek bilgilerin çalınması, gerek ise zarar vermek amaçlı yapılan saldırılara karşı hazırlıklı olmak günümüzde siber güvenliğin sağlanması adına oldukça önemlidir.

Tarih boyunca güvenlik açıkları kaynaklı birçok siber saldırı meydana gelmiştir. 1982 yılında Sibiryaya da yaşanan doğal gaz boru hattına siber saldırı düzenlenmiş, Rusların çaldıklarını sandıkları bilginin içindeki Truva atı virüsünü sistemlerine bulaştırmıştır. Tarihin nükleer olmayan en büyük patlamasına sebep olmuştur (Clarke, 2011). ABD tarafından 1990 yılında Körfez Savaşı sırasında o güne kadar dünyanın en büyük 5. kara ordusuna sahip Irak'ın hava savunma sistemlerini ve iletişim sistemlerini devre dışı bırakan siber saldırı gerçekleştirilmiş, savaşın seyri değişmiştir. Yine ABD Irak'ı 2003 yılında işgal etmeden önce Irak veri tabanını kullanarak üst düzey komutanların e-posta hesabına e-posta atarak teslim olmalarını kendilerine zarar verilmeyeceğini, sonradan tekrar görevlerine döneceği yönünde e-posta atmışlardır. Bu büyük oranda karşılık bulmuş, komutanların birçoğu savaşmak yerine askerleri izne göndermiştir (Kara, 2013). Yakın tarihe gelindiğinde; Haziran 2010 yılında İran nükleer santraline sızmayı başaran "Stuxnet" gibi bir virüs dünya çapında ses getirecek siber güvenlik olayına neden olmuştur. 2010 yılında İran'da ortaya çıkması ile kendinden söz ettiren Stuxnet virüsü; girdiği sistemlere entegre olarak kimi zaman sistemlerin çalışmasını engellemekte kimi zaman ise amacı dışında çalışmasını sağlamaktadır (Langner, 2011). Sistem içerisinde ki her hangi bir bilgisayara takılan USB ile bulaşması mümkün olan bu virüs, nükleer santralin reaktörlerinin aşırı ısınmasına yol açarak İran'ı nükleer anlamda 2 yıl geriye götürmüştür. 60.000'den fazla bilgisayara da bulaştığı düşünülen bu virüsten en çok İran etkilenmiştir (Farwell ve Rohozinski, 2010).

Dijitalleşen dünya, ekonomide de yeni eğilimlere yol açmıştır. 2016 verilerine göre internet, dünya ekonomisine 4 Trilyon dolar katkı yapmış, dünya nüfusunun yarısını birbirine bağlayarak son 15 yılda kullanıcı sayısı olarak 45 kat artmıştır (Jackson ve diğerleri, 2016). Özellikle 2000'li yılların hemen başında hızla büyüyen sosyal medya ile birlikte kullanıcı sayısının ve ekonomisinin hızla artması internet ortamını bir hayli cazip bir pazar haline getirmiştir. Statista'nın (2019) yayınlamış olduğu rapora göre Temmuz 2019'da dünya genelinde 5 milyar insandan 4 milyar 333 kişi internet kullanıcısı iken, 3 milyar 534 kişisi ise aktif sosyal medya kullanıcısıdır. Çin (829 milyon), Hindistan (560 milyon) ve ABD (292.89 milyon) en fazla internet kullanıcısı olan ülkeler olurken, Türkiye ise 69.11 milyon kullanıcı ile dünyada en fazla kullanıcı sıralamasında 12. sıradadır. Bu denli dijitalleşme hali ile beraberinde bazı güvenlik sorunlarını da getirmiştir.

2.2.1. Siber Bilgi Güvenliği Farkındalığı

Sosyal mühendislik ve ortalama gibi insan zaaflarını hedef alan siber güvenlik olayları günümüzde güncelliğini korumaktadır. Bunun en önemli nedeni olarak insanlarda siber bilgi güvenliği farkındalığının oluşturulamaması gösterilebilir. Siber Bilgi Güvenliği Farkındalığı Şahinaslan ve diğerleri (2009) tarafından; kişilerin geçmiş veya güncel ne tür tehlikeler olduğu konusunda bilgilendirilmesi, bu tehlikelerin olası etkilerinden nasıl korunacağı konusunda bilgilendirilmesi olarak tanımlanmıştır. Sağiroğlu ve Erol (2018) ise Siber Bilgi Güvenliği Farkındalığını, kişilerin, kurumların veya devletlerin siber güvenliğin sağlanmaması durumunda karşılaştıkları etkilerden haberdar olması olarak tanımlamıştır. Alan yazındaki diğer tanımlardan da yola çıkacak olursak siber bilgi güvenliği farkındalığını; geçmişte yaşanmış siber güvenlik olaylarından ders çıkarma, anlık siber güvenlik olaylarına karşı müdahalede bulunabilecek donanıma sahip olma, gelecekte yaşanması muhtemel siber güvenlik olaylarına karşı hipotezler geliştirebilme olarak tanımlamak mümkündür.

2.2.2.Siber Saldırı

Siber güvenlik kavramı siber saldırıların ortaya çıkmasıyla ilk defa gündeme gelmeye başlamıştır. Siber saldırılar ise İnternetin ortaya çıkması kadar eskilere dayanmaktadır. Bilinen ilk siber saldırı ise Apple firmasının kurucusu Steve Jobs ve Steve Wozniak tarafından bilgisayarlı telefon sistemlerine yapılmıştır. Gerçekleştirdikleri saldırı ile bilgisayarlı telefon sistemini devre dışı bırakmış, daha uzun mesafe görüşmeleri yapmışlardır (Warnes ve Kathy, 2017). Ardından siber güvenlik açıklarını hedef alan 26 Mart 1999'da ortaya çıkan "Melissa" virüsü büyük ses getirmiştir ("f-secure", 2018). Hemen ardından 2000 yılında Filipinlerde ilk olarak görülen "I love You" virüsünün yaklaşık 45 milyon bilgisayarı etkilediği ve 10 milyar dolarlık zararlara yol açtığı bilinmektedir (Ünver, Canbey ve Mirzaoğlu, 2011). Fakat 2009 yılında SCADA sistemlerinde çalışmak üzere tasarlanmış, siber güvenliğin ne kadar önemli olduğunun bir kez daha anlaşılmasına yol açan "Stuxnet" virüsü bunlar içinde en fazla ses getiren olmuştur. İran nükleer santrallerine bulaşmayı başaran bu virüs nükleer santrallere büyük zararlar vermiştir (Warnes ve Kathy, 2017).

Schmitt (2013)'in önderliğinde birçok hukukçunun katıldığı siber uzay ile ilgili kuralları içeren en kapsamlı yayın olan "Tallinn El Kitabı" siber saldırıyı şu şekilde tanımlamıştır; insanların veya nesnelerin yok olup zarar görmesine neden olan, siber uzayda yaşanan zararlı eylemlerdir. Önaçan ve diğerleri (2016) ise siber saldırıyı "Siber uzayda yer alan her türlü insani ve yazılımsal açıklıklar vasıtasıyla varlıklara erişim, varlıkların niteliğinin değiştirilmesi, varlıklara zarar verilmesi vb. sağlayan etkenler" olarak tanımlamıştır(s. 2).

Yine Keskin(2017) siber saldırıyı ;

“Bilgisayar ve internet alanında uzmanlaşmış hacker diye tabir edilen hack veya hacker gruplarının; genellikle bankalar, devlet kurumları, savunma sanayii, kritik altyapılar, ticari işletmeler, bankacılık ve finans sektörü, sivil toplum kuruluşları, önemli bilgiye sahip şahıs veya kurumlara ait sistemler ile kurumların internet sitelerine zarar vermek amacı ile yaptıkları saldırılardır” olarak tanımlanmıştır(s.1).

Genellikle zarar vermek ya da bilgi çalmak amacı ile gerçekleştirilen siber saldırılar çok hızlı gerçekleşir. Az maliyet ile çok fazla zarar verebilir. Bu nedenledir ki çoğu büyük saldırılar şahıs olarak gerçekleşmez. Devletler gerek saldırıları önlemek gerekse bazı durumlarda saldırılar yapmak için özel birimler yetiştirir ve oluşturur

Özellikle 2000’li yılların başında adını hızla duymaya başladığımız Internet of Things (IoT) yani “Nesnelerin İnterneti” siber saldırılara adeta davetiye çıkarmıştır. Nesnelerin interneti; bilgisayarların, arabaların, beyaz eşyaların ve birçok elektronik cihazın birbirine bağlanmasını ve uzaktan kontrol edilebilmesini kapsamaktadır(Turak, 2015). Günümüz akıllı ev sistemleri veya her hangi bir beyaz eşyaya siber saldırı yöntemleri ile erişmek ve güvenlik zafiyeti yaratmak mümkündür. Savunma Teknolojileri Mühendisliği’nin (STM) 2018 yılında yayınlamış olduğu rapora göre; 2017 yılında IoT saldırılarının 2016’ ya göre %600 oranında arttığı görülmüştür. Bu saldırılara sırasıyla Çin (%21), ABD (10,6) ve Brezilya (%6,9) en çok kaynaklık ederken %4.1 ile ülkemiz yedinci sırada yer almaktadır. Bu oranlar hiç de azımsanacak seviyede değildir. Bundan dolayı siber saldırılara karşı insanlar erken yaşlarda bilinçlendirilerek olası tehditler daha az maliyet ile bertaraf edilebilir.

2.3.Siber Bilgi Güvenliği ile İlgili Kavramlar

Siber Güvenlik: Sistemleri, ağları ve programları saldırılardan koruma; hassas bilgilere erişimi engelleme, güvende kalmasını sağlama işidir (Cisco, 2018). Digital Guardian ise siber güvenliğini; bilgi teknolojisi güvenliği olarak tanımlamıştır(2018).

Siber Toprak: Ülkelerin siber uzaydaki; ekonomik, kültürel, kamusal, teknolojik ve askeri olarak sahip olduğu alana verilen isimdir.

Phishing (Oltalama): Phishing, password kelimesi ile fishing sözcüklerinin birleşmesi sonucu ortaya çıkmış bir sözcüktür (Özbilgin, 2018). Phishing (Oltalama) genellikle kullanıcıya gönderilen sahte e-posta ile başlar. Kullanıcıların gerçek ara yüze benzer internet sitelerine giriş yapmaları sağlanır(Delialioğlu, 2011). Böylelikle girmiş oldukları kullanıcı adları ve şifreleri saldırıyı gerçekleştirenlerin eline geçmiş olacaktır.

Sosyal Mühendislik: Social-engineer.org (2018) internet sitesinde Sosyal mühendislik bilim, psikoloji ve sanatın bir karışımı olarak ifade edilmektedir. Genellikle Bilgi Güvenliği

konusunda bilgisiz insanları hedef alan bu yöntemde amaç elde edilmesi güç olan bilgilerin kandırma, ikna etme yöntemi ile elde edilmesi yöntemidir. Bu yöntemin asıl çıkış noktası iyi niyettir. Günlük hayatta aile içinde bir araya gelmek veya iletişim kurmak için kullanılan prensipler kötü niyetli kişiler tarafından bilgi hırsızlığı için kullanılmaktadır.

Malware: Bilgisayar korsanları tarafından cihazlara zarar vermek, bilgi hırsızlığı yapmak veya para çalmak için kullanılan, dijital ağırları etkilemeye çalışan her hangi bir yazılımdır(Avast, 2018).

Spam: Kullanıcıların e-posta kutularına istemleri dışında düşen birden çok reklam, resim veya videolardan oluşan gönderen kişisi belli olmayan kötü niyetli elektronik postalarıdır(Öztürk,2009).

Bilgisayar Virüsleri: Girdikleri bilgisayarları veya sistemleri yavaşlatmayı, bozmayı, verilere zarar vermeyi amaçlayan özel olarak hazırlanmış kötü niyetli programlarıdır(Şanlısoy,1999).

Anti Virüsler: Bilgisayar virüslerinin yıkıcı ve zarar verici etkisini yavaşlatmak, saldırganlar tarafından bilgisayarlara erişimi engellemek, kullanıcıların online işlemlerini güvenli yapmasını sağlamak amacı ile geliştirilmiş yazılımlardır (Eset, 2018).

Worm(Solucan): Solucanları bilgisayar virüslerinden ayıran en önemli yönü; çalışması, kendini kopyalaması, çoğalması için ana program gerekmemesidir. İnsan yardımı olmadan kendini kopyasını oluşturabilir. Bilgisayar virüsünün aktif olması için ise ana programın aktive edilmesi devreye girmesi gerekmektedir (Kaspersky, 2018).

Truva Atı(Trojan): Siber hırsızlar veya bilgisayar korsanları tarafından genellikle sosyal mühendislik yöntemi kullanılarak sisteme yüklenen meşru yazılım kılığında kötü amaçlı yazılımlardır. Truva atlarının diğer bir özelliği kendi kendine çoğalamamalarıdır. Fakat siber hırsızlar tarafından arka planda takip edilme, verileri silme, verileri değiştirme, bilgisayar performanslarını düşürme gibi olumsuz etkileri vardır (Kaspersky, 2018).

Keylogger: Keyloggerlar, klavyeden bilgisayara gönderilen karakterleri / sayıları yakalayan donanım veya yazılım araçlarıdır(Tuli ve Sahu,2013). Bilgisayara bağlı bir cihaz veya yazılım ile yapılan işlemleri şifreleri, girilen siteleri, belgeleri kayıt eden yazılım veya donanımdır. Genellikle kötü niyetli kişiler tarafından kullanılan keylogger bazen de aileler çocuklarını

Zorbalık: Elektronik araçlar kullanılarak gerçekleştirilen(cep telefonu, internet, bilgisayar) zorbalığa “Siber Zorbalık” denir (Smith ve diğerleri, 2008).

Spyware(Casus Yazılım): Kullanıcı etkinliklerini çevrim içi ve çevrim dışı olarak takip edip; kullanıcı hedefli reklamlar sağlayan, kullanıcıların istemediği türden reklamlarla karşılaşmasına neden olan, kimi zaman da kullanıcı bilgilerini haberi dışında paylaşan yazılımlardır(Good, ve diğerleri, 2005).

Siber Suç: Her kes tarafından kesin kabul görmüş bir tanım olmamasına karşın en geçerlisi Avrupa Ekonomik Topluluğu Uzmanlar Komisyonu'nun 1983 tarihinde yaptığı tanımdır. Bu tanıma göre siber suç ya da bilişim suçu olarak ta nitelendirilen şey "Bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde gayri kanuni, gayri ahlaki veya yetki dışı gerçekleştirilen her türlü davranış" olarak nitelendirilmiştir (Ünal, 2012, s.32). Saini ve diğerleri (2012) ise siber suç terimini; yasaklanan, yasalara aykırı olarak gerçekleştirilen, bilgisayar veya bilgisayar veri tabanların izinsiz giriş yapma eylem olarak tanımlamıştır.

İnternet Bağımlılığı: İnternetin çok yoğun kullanılması, kullanımının kontrol altına alınamaması, insanların bu sebeple yaşamında ciddi sıkıntılar çekmesi olayına denir (Martin ve Schumacher, 2000 Akt. Özcan ve Buzlu,2005).

Telif Hakları: Telif hakları kanunları ülkeden ülkeye değişse de genel tanımı; yazar veya sanatçının kendi eseri üzerindeki hakkının kanunla ifade edilmesidir (UNESCO, 1987, Akt. Acun, 2000). Yine Türk Dil Kurumu'na(TDK) göre; bir fikir veya sanat eserini yaratan kişinin, bu eserden doğan haklarının hepsidir.

Adware (Reklam Yazılımı): Arama yaptığınız web sitelerine tekrardan yönlendirme yapmak, ziyaret ettiğiniz web sitesinin türüne göre özelleştirilmiş reklamlar sunmak, ziyaret edilen sitelerle ilgili pazarlama verileri toplamak amacı ile oluşturulan yazılımlardır(Kaspersky, 2018). Bu yazılımları Trojen casus ile karıştırmamak gerekmektedir. Trojen casus yazılımı izininiz olmadan arka planda bilgi toplar. Adware ise bilgi topladığını size önceden bilgi verir.

Siber Saldırı: Önemli bilgilerin olduğu ağlara bilgileri çalmak, zarar vermek ya da onları değiştirmek amacı ile gerçekleştirilen insan kaynaklı eylemlerdir (Göçoğlu, 2018).

Bulut Bilişim: Kurumların işlerinin yürütülüşü sırasında ihtiyaç duyulan, uygulama, veri saklama, yedekleme, geliştirme, işleme gibi hizmetlerin üçüncü taraflardan alınması işlemidir (Yıldız, 2010).

Mavi Yakalılar: İşi yaparken beden gücünü kullanan çalışanlar, işçi Sınıfı olarak nitelendirmek mümkündür (Bayraktaroğlu ve diğerleri, 2015).

Beyaz Yakalılar: Daha çok ofis ortamında çalışan iş yerinde beyaz giyecek kadar az beden gücü kullanan, daha çok zihin gücünü kullanan personel olarak tanımlanmaktadır (Bayraktaroğlu ve diğerleri, 2015).

Yerel Saldırgan: Her hangi bir sebepten dolayı iş yerine kızgın veya küskün, hiçbir beklentisi olmadan görev ve sorumluluğu bilinçli olarak kötüye kullanan personele verilen isimdir (Güldüren, 2015).

Hacker: TDK'ya (2019) göre bilgisayar korsanı olarak çevrilen bu terim, File'e(2003) göre ise birden çok anlama gele bilmektedir. Bunlar;

1. Bir sistemi tersine programlaya bilen, bilgisayar yapılarının işleyişini öğrenmekten zevk alan, kendi yeteneklerini geliştirmekten zevk alan kişi.

2. Hızlı bir şekilde kendi programlarını oluşturan, her hangi bir şeyin uzamanı olan kişidir.
3. Etrafındaki hassas bilgileri elde etmeye çalışan kötü niyetli kişi.
4. Dijital sistemleri amacı dışında kullanan kişi olarak tanımladığı hacker için "Kırıcı" tabirini kullanmıştır. Ayrıca bir kişinin sadece bilgisayar alanında hacker olmasına gerek yoktur. İlgi duyduğu bir şeyle fazlaca ilgilenen kişilere de hacker denilebilir.

E-Ticaret: E-ticaret hukuk müşaviri olan Canpolat (2001) tarafından şu şekilde tanımlanmıştır. "Tüketicilerin, işletmelerin ve kamu kurumlarının elektronik ortamda (internet ya da intranet) yazı, ses ve görüntü şeklindeki sayısal bilgilerin işlenmesi, iletilmesi ve saklanması yoluyla, bilgilenmesi ve araştırma yapması, taahhüde girmesi, mal ve hizmetlerin müşteriye teslim edilmesi, bedelinin ödenmesi, satış sonrası bakım ve destek hizmetlerinin yerine getirilmesi eylemleri sürecidir. (s.3).

Bilgi Güvenliği: Alan yazın incelendiğinde kimi yazarlar tarafından siber güvenlik ve bilgi güvenliğinin tanımı aynı verilmiştir. Fakat bilgi güvenliği verilerin nerede ve ne şartlarda depolandığına bakılmaksızın değiştirilmesinin, bozulmasının önüne geçme eylemidir (Klimburg, 2012). Yani basılı ortamda veya dijital ortamdaki verilerin korunma eylemidir. Niekerk ve Solms (2013) tarafından yayınlanan makalede siber güvenlik ile bilgi güvenliği kavramlarının birbiri yerine kullanılmasına rağmen bazı noktalarda ayrıldığını vurgulamışlardır. Bilgi güvenliğinin amacının varlık olan bilginin çeşitli tehditlerden korunması olduğunu söylemiştir. Siber güvenlik için daha çok somut olmayan bilgilerin ve siber uzayda çalışanların da korunması olarak tanımlamıştır. Bilgi güvenliğinin ve siber güvenliğinin tam olarak birbirinin yerine kullanılamayacağı fakat ortak paydalarının bilgi ve iletişim teknolojileri olduğunu belirtmiştir. Klimburg (2012) bilgi güvenliği, bilgi ve iletişim teknolojileri güvenliği, siber güvenlik, ağ güvenliği, internet güvenliği, kritik bilgi alt yapısı güvenliği kavramlarını Şekil 2.1 de özetlemiştir.



Şekil 2.1 Siber Güvenlik ve Diğer Güvenlik Alanları Arası İlişki[11]

Bilgisayar Güvenliği: Bilgisayar tarafından saklanan verilerin ne olduğuna bakmaksızın, bilgisayar sisteminin kullanılabilirliğini ve doğru çalışmasını sağlama işidir (Klimburg, 2012).

SCADA (Supervisory Control and Data Acquisition- Merkezi Denetleme Kontrol ve Veri Toplama): Çoğu zaman endüstriyel sistemlerde kullanılan SCADA sistemi aslında elektronik sistemlerin bir merkezden kontrol edilebildiği yazılım sistemleridir (Daneels ve Salter, 1999). Aslında SCADA sistemi için elektronik sistemlerin bilgisayarlaştırılması dememek mümkündür. SCADA sistemi içerisine elektrik alt yapısı doğal gaz sistemleri, mobil bankacılık, alarm sistemleri, bilgisayarlar, akıllı telefonlar gibi birçok elektronik sistem girmektedir.

Siber Uzay: İnsanların birbirine bağlantılı olan sistemlerle etkileşim içinde olduğu, aynı zamanda bilişim sistemlerinin de kendi arasında ve insanlar ile etkileşim içinde olduğu ortamlardır (Bıçakçı, 2014). Whittaker'e (2004) göre ise tüm bilgi ve iletişim ağlarına yön veren uzaydır.

Siber Savaş: Bilgi ve iletişim sistemleri kullanılarak bir ülkeye maddi ve manevi zarar vermeyi hedefleyen organize saldırıların tamamına denir (Tatar ve Matarcioğlu, 2010 Akt. Bayraktar, 2015).

Sosyal Medya: Sosyal medya, web 2.0 teknolojilerinin nin üzerine kurulmuş, kullanıcıların bilgi alış verişi yapabildiği, temeli 1979'lardaki Usenet ve Bruce ve Susan tarafından ortaya çıkan "Open Diary" ye dayanan internet uygulamalarıdır(Haenlein ve Kaplan,2010).

2.4.Türkiye’de Siber Güvenlik

Dünya genelinde önemi gittikçe artan siber güvenliğe yönelik Türkiye’deki ilk adım 1989 yılında kanun tasarısı hazırlama çalışması ile olmuş fakat bu deneme başarısız olmuştur(TBMM, 2012). Bu tasarı ile bilişim sistemlerinin, önemli bilgi altyapılarının ve internet şebekesinin her türlü tehdit, siber saldırı ve müdahaleden korunmasını sağlamak üzere bilişim sistemlerine ilişkin güvenlik usul ve esaslarının belirlenmesi amaçlanmıştır(TBMM, 2012). Anayasal düzeyde ise siber suçların 6 Haziran 1991 yılında 3756 sayılı kanun Ceza kanununun bazı maddelerinde yaşanan değişikliklerle olmuştur.

“MADDE 525 a. — Bilgileri otomatik olarak işleme tabi tutmuş bir sistemden, programları, verileri veya diğer herhangi bir unsuru hukuka aykırı olarak ele geçiren kimseye bir, yıldan üç yıla kadar hapis ve bir milyon liradan on beş milyon liraya kadar ağır para cezası verilir. Bilgileri otomatik işleme tabi tutmuş bir sistemde yer alan bir programı, verileri veya diğer herhangi bir unsuru başkasına zarar vermek üzere kullanan, nakleden veya çoğaltan kimseye de yukarıdaki fıkrada yazılı ceza verilir”(Resmigazete,1991, s.6).

Daha sonra 2004 yılında yürürlüğe giren 5237 sayılı kanun ile çerçevesi genişletilmiştir (Ünver,Canbey ve Mirzaoğlu, 2011). Bu madde çerçevesinde kişisel verilerin başka birisi ile paylaşılması izinsiz kaydedilmesi, silinmesi suç sayılmış, işlediği suçun niteliğine göre hapis cezaları getirilmiştir.

“(1) Bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun; münhasıran bu Bölümde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için yapılması veya oluşturulması durumunda, bunları imal eden, ithal eden, sevk eden, nakleden, depolayan, kabul eden, satan, satışa arz eden, satın alan, başkalarına veren veya bulunduran kişi, bir yıldan üç yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır(TCK,2004). “

İlerleyen yıllarda kanun değişiklikleri ile siber güvenlik kavramlarının kapsamı genişletilmiş, sadece kanun olarak kalmamış fiili eylemlerde de bulunulmuştur. Olası siber güvenlik saldırılarına karşı 2008, 2011, 2013 ve 2015 yıllarında siber güvenlik tatbikatları gerçekleştirilmiştir. 2008 yılında Türkiye Bilgisayar Olayları Müdahale Ekibi (TR-BOME) tarafından düzenlenen tatbikat sonrasında TÜBİTAK ve BTK tarafından da çeşitli tatbikatlar düzenlenmiştir (Ergün, Bıçakçı ve Çelikkpala, 2015). Son olarak ülkemizde yaşanması olası siber saldırıların belirlenmesi, oluşacak tehditlere önlem alınması ve olası saldırılara anında müdahale gerçekleştirilmesi için Ulusal Siber Olaylara Müdahale Merkezi (USOM) kurulmuştur. Bu birim hem kendisine ulaşacak ihbarları değerlendirecek hem de ulusal ve uluslararası tatbikatlar

düzenleyerek kamu kurum ve kuruluşlarının Siber Bilgi Güvenliği Farkındalığının artırılmasını sağlamaktadır (USOM,2020).

Tüm bu gelişmelere rağmen BTK 2009 yılında yayınlamış olduğu bir raporda; güvenlik teşkilatının, yargı biriminin ve teknik uzmanların siber güvenlik alanında yetersiz olduğunu belirtmiştir (Ünver, Canbey ve Mirzaoğlu, 2011). Milli Eğitim Bakanlığı (MEB) tarafından 2012 yılında çalışanlarına bilgi güvenliği farkındalığı anketi uygulanmıştır. Uygulanan bu anket sonuçlarına göre katılımcıların bilgi güvenliğini önemli gördükleri tespit edilse de, katılımcıların %67,92'sinin antivirüs programına sahip olmadığı, %42,22'sinin güvenli şifre oluşturma standartlarına uyarak şifre oluşturduğu tespit edilmiştir. Ayrıca sadece personelin %7,91'inin kaynağı belli olmayan e-postaları açmadığı belirlenmiştir (MEB,2012). Bu sonuçlar göstermektedir ki, Türkiye'de eğitimin temelini atıldığı kurum olan MEB çalışanlarında bile siber bilgi güvenliği farkındalığı yeteri kadar gelişmemiştir. Öğretmenlerin de MEB bünyesinde çalıştığını düşündüğümüzde, meslek hayatlarına başlamadan siber bilgi güvenliği farkındalıklarının ölçülmesi ve elde edilen sonuçlara göre bir yol haritası çizilmesi doğru olacaktır.

2.5.İlgili Araştırmalar

Alan yazın incelendiğinde dijital vatandaşlık ile alakalı yapılan çalışmaların çoğunluğunun üniversite düzeyinde olduğu gözlenmiştir. Yapılan çalışmalarda farklı değişkenlerin dijital vatandaşlık üzerindeki etkisi incelenmiştir. Siber bilgi güvenliği ile ilgili yapılan çalışmalar incelendiğinde farklı meslek gruplarının siber bilgi güvenliği farkındalıklarını tespit etmeye yönelik çalışmalara rastlanmıştır. Hem dijital vatandaşlık hem de siber güvenlik ile ilgili çalışmaların çok eskilere dayanmadığı tespit edilmiştir.

2.5.1.Dijital Vatandaşlık İle Alakalı Yapılan Çalışmalar

Harrison Yang, Sha Zhu ve Shun Xu (2019) üniversite öğrencilerinin 21. yy becerileri ile dijital vatandaşlıkları arasındaki ilişkiyi araştırmak için Çin'de bulunan devlet üniversitesinde toplam 962 öğrenci ile çalışma yapmıştır. 21.yy beceriler ölçeği ve Dijital vatandaşlık ölçeği uyguladığı çalışmasının sonunda iki beceri arasında pozitif yönlü bir ilişki tespit etmiştir. Çalışma sonuçlarına dayanarak üniversite öğrencilerine temel medya okuryazarlığı üzerine eğitimler verilmesi gerektiği vurgulanmıştır. Ayrıca Bilgi ve İletişim Teknolojileri(BİT) ile ilgili eğitimlerin verilmesi gerektiği, eğitimcilerin üniversite öğrencilerinin gerçek hayattaki problemleri çözmesi ve çevrim içi ortamları daha güvenli kullanmak konusunda bilgilendirilmesi gerektiği vurgulanmıştır.

Yine Dan Ke ve Shun Xu'nun (2017)' nun Çin'de bir devlet üniversitesinde yapmış oldukları çalışmada; öğrencilerin bilgisayar öz yeterlilikleri, internet tutumu ve bilgisayar

deneyimlerinin dijital vatandaşlık üzerindeki etkisini incelemiştir. Huang Gang Normal Üniversitesi'nde (HGNU) 115 öğrenci ile yaptıkları bu çalışmaya göre; bilgisayar deneyiminin dijital vatandaşlık düzeyleri üzerinde etkisi olmadığı, fakat internet tutumunun ve bilgisayar öz yeterliliklerinin önemli bir etkiye sahip olduğu görülmüştür. Yüksek bilgisayar öz yeterliliğine sahip öğrencilerin daha yüksek dijital vatandaşlık düzeyine sahip olduğu sonucuna varılmıştır.

Lisa M Jones ve Kimberly J Mitchell (2015) yapmış oldukları çalışmada; ABD'nin Northern New England bölgesinde beş ortaokul ve 1 lisede çevrimiçi anket yoluyla dijital vatandaşlık ile ilgili veri toplamışlardır. Ayrıca bu anket ile, çevrimiçi saygı ve çevrimiçi taciz gibi iki alt boyut hakkında da bilgi toplamayı amaçlamışlardır. Lise 10. Sınıf ve ortaokul 6. Sınıf öğrencilerine uyguladıkları anket sonuçlarına göre; dijital vatandaşlık puanları ile dijital saygı puanlarının yaşla doğru orantılı olarak azaldığı gözlenmiştir. Kız öğrencilerinin dijital vatandaşlık ölçeğinden aldığı puanların ise erkeklere göre daha yüksek çıktığı görülmüştür. Dijital vatandaşlık ile çevrimiçi taciz arasındaki ilişkiyi inceledikleri madde sonuçlarına göre ise; dijital vatandaşlık puanları yüksek olanların daha az çevrim içi taciz mağduriyeti yaşadığı görülmüştür. Yine bu çalışmada öğrencilerin internetten gelecek olumsuz şeylere karşı korunmaya istekli fakat yönlendirilme konusunda eksik oldukları gözlenmiştir. Yapmış oldukları bu çalışma sonucunda eğitim müfredatlarına dijital vatandaşlık eğitimlerinin ve internet güvenliği eğitimlerinin girmesi gerekliliği vurgulanmıştır.

Sullivan (2016) yayınlamış olduğu makalede dijital vatandaşlık kavramının hukuki ve insani yönden incelemiş bazı önerilerde bulunmuştur. Yazar çalışmasında, temel hak olarak kabul edilen kimlik hakkı gibi dijital kimlik hakkının da olması gerektiği, hukuki olarak kesin bir tanım yapılmasının gerekliliğinden bahsetmiştir. Çalışmasında Avusturalya'nın dijital vatandaşlığı tanımlayan ilk ülke olduğuna değinmiş, ülkenin dijital vatandaşlık konseptini incelemiştir. Fakat çalışmasında tüm ülkelerin dijital vatandaşlık konusunda gerekli hukuki statüleri tanımlamaları gerektiğini vurgulanmıştır.

Hollandsworth ve diğerlerinin (2017) yayınlamış oldukları makale; Association for Educational Communications and Technology (AECT) tarafından 2010 yılında K-12 deki öğrencilerin dijital vatandaşlık durumunu ortaya koyan araştırma ile ilgilidir. 2010 yılında yapılan araştırmada ailelerden, öğretmenlerden ve öğrencilerden anketler yolu ile veri toplanmıştır. Bu anketten elde edilen verilere göre; okulların neredeyse yarısında (%47) dijital vatandaşlığın birçok kademe ve konu alanında öğretildiği görülmüştür. %18 lik bir oranda ise sadece bir kademe öğretildiği görülmüştür. Ankete katılanların %35 i dijital vatandaşlığı müfredatın bir parçası olarak öğretilmediğini vurgulamıştır. Ankete katılan eğitimcilerin birçoğu dijital vatandaşlık eğitimlerinin erken yaşlarda verilmesine inanmaktadır. Ankete katılanların %14 lük kısmı 5.Sınıf ve üzeri yaşlarda dijital vatandaşlık eğitiminin, %21'i okul öncesi, %33'ü 1.

Sınıf ve 2. Sınıfta, %32'si 3. ve 4.sınıfta başlanması gerektiğini vurgulamıştır. Ayrıca aynı anket sonuçlarına göre yöneticilerin dijital vatandaşlık seviyelerinin (%75) öğretmenlerden(%58) daha yüksek olduğunu göstermiştir. Yine aynı araştırmada "İnternetin güvenliği için neler yapılıyor?" sorusuna tamamına yakını filtreleme ve güvenlik duvarı cevabını vermiştir. Genelde güvenlik için fiziki önlemler alınıyor olması dijital vatandaşlık ve alt boyutu olan siber güvenlik konusunda farkındalıkların düşük olmasını da destekler niteliktedir. Araştırmacılar araştırma sonunda dijital vatandaşlık konusunda öğrenciler kadar eğitimcilerin de eğitim alması gerektiğini vurgulamıştır.

Dağhan ve diğerleri (2017) Hacettepe Üniversitesi Eğitim Fakültesi Bilgisayar ve Öğretim Teknolojileri Öğretmenliği (BÖTE) bölümünde yapmış oldukları Bilişim Teknolojileri Öğretmen Adaylarının Bakış Açısından 21.Yüzyıl Öğrenen Ve Öğretmen Özellikleri adlı çalışmalarında; öğretmenlik uygulamasına gelen 63 öğretmen adayının 21. yüzyıl öğrenen özelliklerine ait temalar belirlenmiş bu temalara göre yeterlilikleri incelenmiştir. İncelenen 8 tema; bilgi okuryazarlığı, bilişsel beceriler, sosyal özellikler, kişisel özellikler, dijital vatandaş olma, ahlaki özellikler, öğrenme tercihi ve medya okuryazarı olma şeklindedir. Öğrenenlerin sahip olması gereken özelliklere göre elde edilen bulgulara göre; eleştirel ve yaratıcı düşünebilen, problem çözme becerisine sahip, etkili iletişim kurabilen, teknolojiyi etkili kullanabilen ve işbirlikli öğrenme becerilerine sahip bireyler olması gerektiğine değinilmiştir. Çalışma sonucunda öğretmen adaylarının öğrenen ve öğretmen açısından farklılığa sahip olduğu gözlenmiştir. Öğrenen özelliklerine göre elde edilen bulgulara göre; oluşturulan bilgi okuryazarlığı, bilişsel beceriler ve sosyal özellikler temalardan en fazla işaretlenen temanın bilişsel beceriler olduğu görülmüştür. Bilişsel beceriler temasının fazla işaretlenmesi; başarılı olmada 21.yy becerilerinden eleştirel düşünme, yaratıcı düşünme gibi zihinsel süreçlerin önemli olduğunun göstergesi olarak yorumlanmıştır. Ayrıca öğretmen adaylarının 21.yy becerilerinden bilgi okuryazarlığına önem verdiği görülmüştür. Öğretmen adayları 21.yy öğretmenlerinde olması gereken özellikleri ise; teknolojiyi etkin kullanan, işbirlikli çalışma becerisine sahip, kendini geliştirmeye açık, alanında uzman ve rehberlik etme yeteneğine sahip bireyler olarak sıralamıştır.

Elçi'nin (2015) bilişim teknolojileri ve yazılım dersi öğretim programına yönelik öğrenci görüşlerini dijital vatandaşlık bağlamında incelemiştir. Toplam 264 öğrenci ile yapılan bu çalışmada; Bilişim Teknolojileri dersinde dijital vatandaşlık ölçeği kullanılarak veri toplanmıştır. Sonuçlara göre; Bilişim teknolojileri dersi ile dijital vatandaşlık ölçeği puanları arasında sınıf düzeyi ve cinsiyete göre anlamlı bir fark bulunamamıştır. Fakat evinde bilgisayarı olan öğrencilerin lehine bir sonuca ulaşılmıştır. Ayrıca test sonuçlarından elde edilen veriler bilişim teknolojileri dersinin öğretim programının öğrencilerin dijital vatandaşlığın alt boyutlarıyla ilgili bilgi, beceri ve kazanmada etkisinin orta düzeyde olduğu şeklinde yorumlanmıştır. Ayrıca Bilişim teknolojileri dersinin içeriğinin dijital vatandaşlık konusuna odaklanarak genişletilmesi

durumunda gündelik hayatta ve okul hayatında en yüksek seviyede verim alınacağı belirtilmiştir. Fakat ilkokullarda bulunan bilişim teknolojileri dersinde yapılan sık değişikliklerin dersten alınacak verimi etkilemiş olabileceği vurgulanmıştır. Yine bu çalışmada dijital etik-kanun ve buna bağlı hak ve sorumluluklar boyutuna ait elde edilen puan dijital okuryazarlık, dijital güvenlik ve dijital iletişim boyutlarına göre daha yüksek çıkmıştır. Bu ise dijital etik-kanun ve buna bağlı hak ve sorumluluklar boyutunun öğretmenlerce diğer boyutlara göre daha fazla önemsendiği şeklinde yorumlanmıştır. Bilişim teknolojileri dersinin dijital güvenlik boyutuna katkısı ise orta düzeyde tespit edilmiştir.

Kaya ve Kaya (2014) Bilgisayar ve Öğretim Teknolojileri Eğitimi 3. ve 4.sınıf öğretmen adaylarının dijital vatandaşlık algılarını ölçmek amacı ile yapmış oldukları yarı yapılandırılmış görüşmelerin sonuçlarına göre öğretmen adaylarının çoğunluğu dijital vatandaşlık kavramını; bireyin yaşamını kolaylaştırması amacı ile teknolojiyi doğru kullanma olarak tanımlamışlardır. Ayrıca öğretmen adaylarının tamamına yakını teknolojinin doğru kullanılabilmesi için dijital vatandaşlıkla ilgili okullarda eğitimlerin verilmesi gerektiği vurgusunu yapmıştır. Elde edilen sonuçlara göre; öğretmen adaylarının büyük çoğunluğu dijital vatandaşlığın alt boyutu olan dijital güvenlik konusunda bilgi sahibidir. Zamandan tasarruf sağlaması ve daha ucuz olması dolayısı ile birçoğu çevrimiçi alışveriş yapmakta, alışveriş esnasında site güvenliğine özen göstermektedir. Öğretmen adayları düzenli olarak sosyal medya da zaman geçirmektedir. Bu ise dijital vatandaşlığın alt boyutu olan dijital iletişimi etki olarak kullandıkları olarak yorumlanmıştır. Öğrencilerin dijital vatandaşlığı bireyin hayatını kolaylaştırmasına yardımcı olan bir etken olarak tanımlaması; dijital vatandaşlığın alt boyutları hakkında bilgi sahibi olmadıkları şeklinde yorumlanmıştır. Ayrıca çalışmaya katılan öğretmen adaylarının büyük çoğunluğu BÖTE bölümünde dijital vatandaşlık adında bir dersin olması gerektiğini ve bunun neticesinde eğitim kurumlarına atandıklarında yol göstericilik rolünü üstlenmeleri gerektiğini vurgulamışlardır.

İşman ve Güngören (2013) öğretmen adaylarının dijital vatandaşlık düzeylerini tespit etmek için ölçek çalışması geliştirmiştir. Ölçeğin geçerlilik ve güvenilirlik çalışmalarını yaptıktan sonra eğitim fakültesinden 141 erkek 98 kız olmak üzere 239 öğretmen adayından veri toplamışlardır. Veri toplanan bölümler; okul öncesi, sınıf öğretmenliği, din kültürü öğretmenliği ve Türkçe öğretmenliği olarak belirlenmiştir. Dijital vatandaşlık düzeyleri farklı değişkenler açısından incelenmiş sonuç olarak; dijital vatandaşlık seviyesi ile cinsiyet arasında anlamlı bir fark bulunamamıştır. Dijital vatandaşlık ile sınıf seviyesi arasında anlamlı fark bulunamamıştır. Yine bilgisayara sahip olma, bilgisayarda geçirilen süre ve internet kullanıp kullanmama arasında anlamlı bir fark bulunamazken internette kalma süresi ile olumlu yönde anlamlı bir fark tespit edilmiştir. Bu sonuç internette veya sosyal medyada fazla vakit geçiren bireylerin dijital vatandaşlık seviyeleri yüksek olarak yorumlanmıştır.

Ünver'in (2012) iki aşamalı yüksek lisans çalışmasının ilk aşamasında, Gaziosmanpaşa Üniversitesi Eğitim Fakültesi'nde ölçeğin geçerlilik ve güvenilirlik çalışması yapılmıştır. Diğer aşamasında ise geliştirilen ölçek Karadeniz Teknik Üniversitesi Fatih Eğitim Fakültesi'nde öğretmen adaylarına uygulanmıştır. Sonuç olarak cinsiyet değişkenine göre erkek öğretmen adaylarının lehine olacak şekilde anlamlı bir fark bulunmuştur. Yaş değişkeninde ise 23 yaş üstü öğretmen adaylarının lehine bir sonuç bulunmuştur. Öğretmen adayları ile bölümler arasında manidar bir fark bulunmuş olup Türkçe öğretmenliği lehine bir sonuca rastlanmıştır. Yine 9 yıl ve üzeri internet kullanım süresine sahip kişilerin lehine olacak şekilde anlamlı bir farka rastlanmıştır. Öğretmen adaylarının e-posta adresi kullanıp kullanmama ile dijital vatandaşlık ölçeğinden aldıkları puanlar arasında anlamlı bir fark bulunmuştur. Bu bulguları; dijital vatandaşlık düzeyi ile cinsiyet, yaş, okuduğu bölüm, e-posta adresi kullanıp kullanmama durumu arasında manidar bir farkın olduğu şeklinde yorumlamak mümkündür.

Vural ve Kurt (2018) tarafından Anadolu Üniversitesinde yapılan çalışmada; üniversite öğrencilerinin dijital vatandaşlık düzeylerini ölçmeye yönelik 625 öğrencinin katılımı ile bir ölçek geliştirilmiştir. Geliştirilen ölçek farklı devlet üniversitelerinden öğrencilerin de olduğu bir örnekleme uygulanmıştır. Ölçek ile öğrencilerin dijital vatandaşlık düzeyleri bazı değişkenlere göre incelenmiştir. Sonuç olarak dijital vatandaşlık düzeyi ile cinsiyet arasında anlamlı fark bulunmuştur. Bu fark, dijital vatandaşlık düzeyinin kadın üniversite öğrencilerin lehine olacak şekilde farklılaştığı şeklinde yorumlanmıştır. Araştırmada ölçeğin uygulandığı üniversite ve dijital vatandaşlık seviyesi arasında almalı bir fark tespit edilmişken, fakülteler arasında anlamlı bir fark tespit edilmemiştir. Bu sonuç ise farklı üniversitelerde öğrenim gören öğrencilerin dijital vatandaşlık seviyeleri farklılık göstermiş, öğrenim gördüğü fakülte ile dijital vatandaşlık düzeyi arasında farklılık göstermemiş şeklinde yorumlanmıştır. Sınıf düzeylerine karşılaştırıldığında ise dijital vatandaşlık ortalamalarının sınıf düzeyi arttıkça arttığı, internet kullanım sıklıkları ve aylık gelirleriyle genel ortalamaları arasındaki bağıntıların ise anlamlı olduğu gözlenmiştir. Bu sonuç ise İnternet kullanım süresi ve gelir düzeyi arttıkça dijital vatandaşlık düzeyi de artmaktadır şeklinde yorumlanabilir

Aydın (2015) Dijital Vatandaşlık Kurumu (Global Digital Citizen Foundation) tarafından hazırlanan Dijital Vatandaşlık Sözleşmesini Türkçe'ye kazandırmayı amaçlamıştır. Dijital Vatandaşlık Sözleşmesi çevrimiçi ortamda nasıl davranması gerektiğine ilişkin temel ilkeleri içermektedir. Bu ilkeler;

1. Kendine karşı saygı
2. Kendine karşı sorumluluk
3. Başkalarına karşı saygı
4. Başkalarına karşı sorumluluk

5. Entelektüel mülkiyet haklarına karşı saygı
6. Entelektüel mülkiyet haklarına karşı sorumluluk olarak belirlenmiştir.

2.5.2. Siber Güvenlik İle Alakalı Yapılan Çalışmalar

Siber Güvenlik ve Dijital Vatandaşlık Türkiye’de ve Dünyada yeni bir çalışma alanı olarak karşımıza çıkmaktadır. Bu yüzden yapılan çalışmaların da çok geçmişe dayanmadığını görülmektedir. Bu bölümde Yüksek Öğretim Kurulu(YÖK) sitesi, Scholar Google ve Mersin Üniversitesi Kütüphanesi veri tabanı kullanılarak alan yazın taraması yapılmıştır. Yabancı kaynaklardan yapılan taramaların sonuç ve önerilerinde ortak olarak siber güvenlik vurgusu yaparken “insan” faktörüne değinildiği gözlenmiştir. Mahabi (2010) tarafından Florida Eyalet Üniversitesinde kullanıcı kaynaklı yaşanan siber güvenlik sorunlarını azaltmak için yapılan çalışmada kullanıcıların siber saldırılara karşı kendini koruyabilme farkındalığı ölçülmüştür. Yapılan çalışma sonucunda kullanıcıların siber saldırılara karşı kendilerini koruyabilmeleri için eğitime ihtiyaç duyduğu görülmüştür. Yaşanan güvenlik olaylarında insan faktörünün ihmal edildiği, artık insan faktörünün dikkate alınma zamanının geldiği vurgulanmıştır.

Luo ve diğerleri (2012) phishing saldırılarının başarılı olmalarının altında yatan psikolojik nedenlerin araştırıldığı çalışmasında, phishing üzerine yapılmış bazı çalışmalardan ve sonuçlarından da destek alarak bu konunun önemine dikkat çekmeye çalışmıştır. 2010 yılında Indiana Üniversitesinde yüksek lisans öğrencilerine verilen bilgi güvenliği dersi kapsamında yapılan çalışmada 105 kişiye üniversite e-postası aracılığı ile phishing e-postası gönderilmiştir. Henüz 22 dakika geçmesine rağmen e-posta linkine 38 kişinin tıkladığı, 16 kişinin de kullanıcı adı ve şifre bilgilerini paylaştığı tespit edilmiştir. Phishing saldırıların başarılı olmasını; insanın bilişsel ön yargılarından yararlanmanın, teknolojik zafiyetleri kullanmaktan daha etkili olduğunun anlaşılmasına bağlamıştır. Ayrıca bu tür saldırıların önüne geçilmesi için halkın phishing saldırılarına karşı bilinçlendirilmesi gerektiği vurgulanmıştır.

Pusey (2011) Florida Atlantic Üniversitesi lisans bölümünde öğretmen adayları ile yapmış olduğu çalışmada Siber Etik, Siber Güvenlik ve Siber Koruma farkındalıklarını geliştirdikleri anket ile ölçmüştür. Toplamda 318 öğretmen adayı ile yapılan çalışmada Siber Etik, Siber Güvenlik ve Siber Korumayı öğretebilme yeterliliklerini derecelendirmesi istenmiştir. Çalışma her öğretmen adayının almak zorunda olduğu teknoloji entegrasyon dersinde gerçekleştirilmiştir. 2 yıl boyunca 98 maddeden oluşan bu ölçek öğretmen adaylarına belli aralıklarla uygulanmıştır. Ölçek maddeleri siber etik, siber güvenlik, siber koruma farkındalıklarını tespit etmeye yönelik bölümlere ayrılmıştır. Elde edilen sonuçlara göre; öğretmen adaylarının %60’ı verilen 70 konu başlığını öğretmede kendini yeterli görmez iken sadece % 40’ı bu konuda kendini yeterli bulmuştur. Bu sonuç öğretmen adaylarının bu üç başlıkla ilgili sınırlı bilgiye sahip olduğu,

öğretme konusunda yeterli olmadıkları şeklinde yorumlanmıştır. Öğretmen adaylarının bu üç başlık ile ilgili farkındalık seviyelerinin yüksek olması gerektiği ve daha fazla eğitime ihtiyaç duydukları vurgulanmıştır.

Jang-Jaccard ve Nepal (2014) siber güvenlik konusunda ortaya çıkan tehditler ile ilgili yapmış olduğu çalışmada mevcut güvenlik açıklarını kapsamlı şekilde incelemiştir. Gelişmekte olan teknolojilerde yeni siber güvenlik saldırı modellerinin analizini yapmayı, siber güvenliğin gelecekteki araştırılması gereken yönlerinin tespitini sağlamayı amaçladığı çalışmada, Symantec'in (2012) verilerini de kullanarak çeşitli analizler gerçekleştirmiştir. Siber saldırıların gelişmesinin nedeninin fiziksel saldırıdan çok daha ucuz olduğunu belirttiği çalışmada, özellikle son yıllarda gelişen akıllı telefonların bu saldırılara davetiye çıkardığını vurgulamıştır. Ayrıca hızla büyüyen sosyal medya ile birlikte saldırıların bu alana kaydığını ve bu alandaki saldırıların çoğu zaman kullanıcı kaynaklı olduğunu belirtmiştir. Bunun yanı sıra çoğu şirketin çalışanlarının sosyal medyada çok fazla bilgi paylaştığını ve bunların kendileri için tehdit olduğunu düşünerek, bu konuda eğitimler verilmesi gerektiğini vurgulamıştır.

Eloff ve Delamini'nin (2009) yapmış olduğu çalışmada bilgi güvenliğinin doğuşu ve günümüzde geldiği noktalara değinilmiştir. Siber bilgi güvenliği ile alakalı yapılan anketlere ve sonuçlarına yer verdiği makalesinde, bu güne kadar yapılmış çalışmalarda göz ardı edilen konular ile hiç ele alınmamış konulara değinilmiştir. Ayrıca çalışmada tarihte bilinen ilk bilgisayar virüsünün nasıl ortaya çıktığına ve siber güvenlikle ilişkisine yer verilmiştir. Siber bilgi güvenliğinin aslında insanın yazıyı ilk bulması ile ortaya çıktığının vurgulandığı çalışmada, bilgisayarların icadı ile bu kavramın daha çok dijital ortamlar için kullanıldığından bahsedilmiştir. Ayrıca anket sonuçlarının değerlendirildiği çalışmada; günümüz siber bilgi güvenliği sorunlarının çoğunun örgütsel yapılar ve insan boyutundan kaynaklandığı sonucuna varılmıştır.

Weeden, Cooke ve McVey (2013) 13 yaşından küçük 3. sınıf ile 9. sınıfı arası 199 öğrenciler ile araştırma gerçekleştirmiştir. Öğrencilerin sosyal medya kullanım davranışlarını, güvenlik riskleri değerlendirme becerileri araştırılmıştır. Araştırma sonuçlarına göre öğrencilerin büyük çoğunluğu 9 lu yaşlarda sosyal medya kullanmaya başlamaktadır. Ayrıca öğrencilerin gizlilik ayarları yapma, güvenlik risklerini değerlendirme konusunda yetersiz olduğu sonucuna ulaşmıştır. Öğrencilerin çok erken yaşlarda sosyal platformlara üye olduğu, bunun ciddi sorunlara yol açabileceği vurgusu yapılmıştır. Çalışma sonunda sosyal ağlarda gizlilik ve güvenlik konusunda öğretmenlere ve velilere de roller düştüğü vurgusu yapılmış, bu konuda farkındalıklarının artırılması gerektiği belirtilmiştir.

Schaik, Jeske, Onibokun, Coventry, Jansen ve Kusev (2017) tarafından yapılan çalışmada ABD'li ve İngiliz 436 üniversite öğrencisi ile günlük hayatta karşılaşılması muhtemel 16 güvenlik tehlikesi karşılaştırılmıştır. Araştırmada çevrim içi anket ile veri toplanmıştır. Öğrencilerin dijital

güvenlik zararı kapsamında çevrimiçi risk alma algıları ve bu tehditlerden kaçınma eğilimleri araştırılmıştır. Katılımcılardan toplanan veriler analiz edildiğinde; katılımcılara göre en riskli olan dijital tehlike, kimlik hırsızlığıdır. En az riskli olan ise, çerezler ve e-posta edinmektir. Araştırmaya katılanların anti virüs yazılımı kullanma, işletim sistemi güncellemeleri ve güvenlik yazılımı kurma gibi dijital güvenlik becerilerinin ortalamasının üstünde olduğu bulunmuştur. Araştırmaya katılanlar, geçmişte yaşadıkları olumsuz deneyimlerin risk algılarını artırdığını belirtmişlerdir. Araştırma sonunda öğrencilerin siber güvenlik konusunda eğitilmesinin risk algılarını arttıracığı belirtilmiştir.

Alan yazın incelendiğinde ülkemizde siber güvenlik ile yapılan çalışmaların çok eskilere dayanmadığı görülmektedir. Yapılmış çalışmaların bir birçoğu mühendislik alanındadır. Birçok fakülteden ve bölümden tez çalışması varken, Eğitim Fakültesi ve BÖTE bölümünden siber güvenlik ile alakalı tezin olmadığı YÖK tez merkezinin sistemi tarama neticesinde de ortaya çıkmıştır. Tablo 2.1 'de 2013-2020 arası siber güvenlik ile alakalı yapılmış tezlere yer verilmiştir.

Tablo 2.1
YÖK Tez sisteminden Ulaşılan Siber Güvenlik çalışmaları.

Alan/Bölüm	Tez Türü	Yayın Yılı	Yayın Sayısı
Bilgisayar Mühendisliği	Yüksek Lisans	2013-2020	15
Bilişim Sistemleri mühendisliği	Yüksek Lisans	2013-2020	1
Uluslar Arası İlişkiler	Yüksek Lisans	2013-2020	6
Sosyoloji	Yüksek Lisans	2013-2020	1
Bilgi ve İletişim Teknolojileri	Yüksek Lisans	2013-2020	1
Kamu Yönetimi	Yüksek Lisans	2013-2020	2
Hukuk	Yüksek Lisans	2013-2020	1
Siyasal Bilimler	Yüksek Lisans	2013-2020	1
Kamu Yönetimi	Doktora	2013-2020	1
İstatistik/İşletme	Doktora	2013-2020	1
Uluslar Arası İlişkiler	Doktora	2013-2020	2

Türkiye’de siber güvenlik alanında yapılan ilk çalışma Filiz (2012) tarafından Bilgisayar Mühendisliği bölümünde yapılmış olup, biyometrik yöntemler ve yüz tanıma problemi üzerinde kullanılan yöntemler incelenmiştir. Nesnelere eşleştirmek için kullanılan yöntemlerden olan Scale Invariant Feature Transform-Ölçekten Bağımsız Özellik Dönüşümü(SIFT) yöntemi yüz tanıma sisteminin işleyişini anlamak adına farklı veri tabanları kullanılarak denenmiştir. Doğru yüz tanıma sistemi nasıl olmalı sorusuna cevap aranmıştır. Sonuç olarak iyi bir yüz tarama sisteminde

kullanılması gereken algoritmalara ve yüz tarama sisteminde olması gereken özelliklere dair önerilerde bulunulmuştur.

Sarı (2013) yaptığı çalışmada öncelikle uluslararası hukuk açısından siber saldırı, siber casusluk, siber savaş ve siber suç gibi kavramların tanımlanması tartışmalarına yer vermiştir. Bu kavramların doğru şekilde tanımlanmaması durumunda hukuksal bir boşluk oluşacağına değinilmiştir. Türk hukuk sisteminde de siber suçun tanımlanması ve cezalandırılması konusunda eksikliklerin olduğuna değinilmiştir. Hukuk sistemimizde yapılan eylemin niteliğinden çok, bırakmış olduğu etkiye göre cezalandırıldığı vurgulanmıştır. Sonuç olarak bilişim sisteminde ortaya çıkan suçlara karşı mücadelenin en önemli noktasının, bilişim sistemlerinin karmaşık yapıları olduğuna, bu suçlarla mücadele için ülkeler arası iş birliğinin önemine ve insanların bu konuda bilinçlendirilmesine vurgu yapmıştır. Akyıldız ve Yiğit (2013) ise sızma testi üzerine yaptığı çalışmasında bir uygulama benzetimi hazırlamış, gerçek hayatta karşılaşılan saldırıların uygulamaları yapılmıştır. Böylelikle sızma testlerin öneminin vurgulanması amaçlanmıştır. Sonuç olarak; ağlara erişimde fiziksel önlemlerin yeterli olmadığı, ağa girildiğinde şifrelerin kolayca devre dışı bırakılabildiği tespit edilmiştir. Ayrıca şifrelemede tahmin edilmesi kolay şifrelerin kullanılmasının ağda güvenlik zafiyetleri getirdiği vurgulanmıştır. Özellikle muhtemel siber saldırılara karşı hem çalışanların hem de kullanıcıların Siber Bilgi Güvenliği Farkındalığının artırılması gerektiğine değinilmiştir. Ercan (2015) "Kritik Alt yapıların Korunmasına İlişkin Belirlenen Siber Güvenlik Stratejileri" adıyla yapmış olduğu yüksek lisans tezinde, kritik alt yapı kontrol sistemlerinde kullanılan BİT'in maruz kaldığı siber saldırılara karşı alınması gereken önlemler için tavsiyelerde bulunmayı amaçlamıştır. Araştırma neticesinde kritik alt yapılarda bulunan personellerin siber güvenlik konusunda eğitilmesi gerektiği vurgulanmıştır. Ayrıca siber güvenliğin devlet politikasına dönüştürülerek; Kuzey Atlantik Antlaşması - North Atlantic Treaty Organization (NATO), Ekonomik Kalkınma ve İşbirliği Örgütü - The Organisation For Economic Co-Operation And Development - (OECD), Avrupa Birliği (AB), Amerika Birleşik Devletleri'nde (ABD) yapılan çalışmalarla örtüşecek yasal mevzuatların oluşturulması gereği üzerinde durulmuştur. Aytekin (2015) Türkiye'nin siber güvenlik strateji ve eylem planı ile ilgili yapmış olduğu çalışmada, siber güvenliği derinlemesine incelemiş olup Türkiye'nin siber güvenlik strateji planının eksikleri tespit ederek çözüm önerileri sunmuştur. Ayrıca siber güvenlik stratejileri uygulamalarında önde gelen ülkeler olan İngiltere ve ABD ile Türkiye'nin stratejik planlamaları karşılaştırmıştır. Siber güvenlik konusunun stratejik seviyede planlanması gereğinin özel sektör ve kamuda yeteri kadar önemselenmediği ortaya çıktığını vurgulamıştır. Siber güvenlik ve siber güvenlik strateji planlanmasının kamu ve özel sektör tarafından yeteri kadar ciddiye alınmadığı gözlenmiştir. Sonuç olarak; virüs programları, ağ protokolleri vb. fiziksel güvenlik önlemlerinin hiç birinin uluslararası siber güvenlik tehditlerini bertaraf etmede tek başına yeterli olmayacağı,

disiplinler arası bir iş birliği içinde olunması gerektiği önerisinde bulunulmuştur. Meral (2015) SCADA sistemi üzerinde yapmış olduğu çalışmada bu sistemlerin yaratacağı siber güvenlik açıkları hakkında farkındalık yaratmayı amaçlamıştır. Dünyada ve Türkiye’de bu sistemlere sürekli saldırıların olduğu, kimi zaman bu saldırıların farkında bile olunmadığı üzerinde durmuş; çözüm olarak milli yazılımların gerçekleştirilmesi ve Ar-Ge’ye ayrılan paranın artırılması gerektiği belirtilmiştir. Siber saldırıların siber saldırılara baskın geldiği bir zamanda yaşadığımız belirtilmiş, bugün karşımıza çıkan teknik anlamda aksaklık gibi görünen şeylerin ilerleyen yıllarda siber saldırı aracı olabileceğine değinilmiştir. Sistemlerin saldırılardan minimum seviyede zarar görmesi veya saldırıların engellenmesi için kullanıcılarda siber güvenlik farkındalıklarının artırılmasının büyük önem arz ettiği belirtilmiştir.

Erol (2016) Gazi Üniversitesi Bilgi Güvenliği Mühendisliği Anabilim Dalında Siber Bilgi Güvenliği Farkındalığı için ilk kez yetenek tabanlı dinamik bir model geliştirmiş olup, modelin doğrulanması için bir durum değerlendirilmesi yapmıştır. Siber güvenlik olaylarında en fazla zafiyetin insan faktöründen kaynaklandığından yola çıkarak siber güvenlik, farkındalıktan daha çok bir problem olarak ele alınmıştır. Siber güvenlik olaylarına sosyal mühendislik yönünden bakan Barışkan (2017) ise çalışması için geliştirilen 19 maddelik genel bilgi anketini katılımcılara uygulamıştır. Araştırmaya katılanların %54’ünün siber güvenlik konusunda bilgisinin oldukça düşük olduğu gözlenmiştir. Ayrıca katılımcıların %18’i hiç bilgiye sahip değilken, sadece %28’i kendisine bu alanda yeterli görmektedir. Yine sonuçlar incelendiğinde araştırmaya katılanların çok az bir kısmının sosyal mühendislik gibi insan kaynaklı açıklardan haberdar olduğu görülmüş, tehditlere karşı alınabilecek önlemler üzerine durmuştur. Göçoğlu (2018) Türkiye’nin Siber Güvenlik Politikalarının Kamu Politikası Analizi Çerçevesinden Değerlendirilmesi ismiyle yapmış olduğu doktora tezi çalışmasında; Türkiye’nin siber güvenlik politikalarını tanımlayan 28 belge üzerinde nitel çalışma yapmıştır. Tezde ele aldığı bir örnek olay ve beş ülke üzerinden kamu politikası ile siber güvenlik arasındaki ilişkiyi belirlemeye çalışmıştır. ‘Türkiye’ de kritik alt yapıların korunmasına yönelik bir algının yeni yeni oluşmaya başladığı sonucuna vardığı çalışmasında; ABD, Çin, Rusya, İran, Kuzey Kore, İsrail ve Almanya gibi ülkelerin siber güvenlik politikalarına ilişkin sonuçları değerlendirmiş ve Almanya’nın siber güvenliği sistematik olarak kurumsal çerçevede en iyi gerçekleştiren ülke olduğunu vurgulamıştır.

Hekim ve Başbüyük’ün (2013) Uluslararası Güvenlik ve Terörizm Dergisinde yayınlanan makalesinde Türkiye’nin siber güvenlik politikaları ele alınmıştır. Ülke olarak doğru politikalar ve stratejiler geliştirmedeğimiz takdirde risklerinde artacağı vurgulanmıştır. Siber güvenlik tehditleri denilince akla sadece internet güvenliği değil, tüm iletişim alt yapısı güvenliği gelmesi gerektiği belirtilmiştir. Siber güvenlik tedbirleri alınırken mali yük ile fayda, güvenlik ile demokrasi dengelerinin gözetilmesi gerektiği belirtilmiştir. Türkiye’deki siber suç istatistiklerine

yer verdikleri makalelerinde siber suçlar ayrı ayrı değerlendirilmiştir. Bunlar içerisinde en az maliyetle en etkili yöntem olan sosyal mühendislik olayına ayrı bir parantez açılmıştır. Bu saldırıların maliyetinin oldukça fazla olduğunun belirtildiği çalışmada sosyal mühendislik gibi insanı hedef alan saldırılarda insanların bilinçlendirilmesinin ve eğitilmesinin şart olduğu belirtilmiştir. Bu amaçla kamu kuruluşların koordineli bir şekilde çalışması gerektiği, bu iş birliğinin gerekli durumlarda özel sektörle de kurulmasının önemi üzerine durulmuştur.

Henkoğlu ve Tahiroğlu'nun (2015) 5. ve 6. sınıfa giden 165 öğrenci ile yapmış olduğu çalışmada öğrencilere 10 tane açık uçlu soru sorulmuştur. Bu sorularla öğrencilerin bilgiye ulaşmada interneti nasıl kullandıkları, bilgiye ulaşmada öncelik verdikleri kaynaklar ve kaynak göstermedeki farkındalıkları araştırılmıştır. Sonuçlara göre; ortaokul öğrencilerinin bilgiye ulaşırken kaynak olarak ilk önce interneti tercih ettikleri belirtilmiştir. Bilgi kaynağı olarak ilk interneti tercih etme nedenlerine bakıldığında ise, bilgiye ulaşmada hem kolay olduğu hem de diğer kaynaklara göre daha hızlı olduğu vurgulanmıştır. Fakat bazı öğrencilerin internetteki bilginin doğruluğunu teyit etmek amacı ile farklı kaynaklardan da karşılaştırma yöntemini izlediği görülmektedir. Yine araştırma sonuçlarına göre bilgi kaynağı olarak öğrencilerin interneti kullanma nedenlerinden bir tanesi de basılı ortamdaki bilgilerin belli bir süre sonra güncelliğini kaybetmesidir. Bu sonuçlara göre; öğrencilere küçük yaşlardan itibaren araştırma yapma becerisi ve bilgi okuryazarlığı konusunda derslerin verilmesi gerektiği önerilerinde bulunulmuştur. Ayrıca bu yaş gruplarına hitap eden öğretmenlerin de bilgi okuryazarlık eğitimleri almaları gerektiği vurgulanmıştır.

Yapılan alan yazın taraması neticesinde bazı kavramların iç içe geçmiş olduğu gözlenmiştir. Özellikle Siber Güvenlik, Bilgi Güvenliği, Bilişim Güvenliği, Dijital Veri Güvenliği, İnternet Güvenliği gibi anahtar kelimeler kullanılarak yapılan çalışmaların benzer amaç, sonuç veya önerileri olduğu dikkat çekmektedir. Yılmaz'ın (2015) Anadolu Üniversitesi Bilgisayar ve Öğretim Teknolojileri Anabilim Dalında (BÖTE) karma yöntem ile yapmış olduğu doktora tezinde öğretmenlerin dijital veri güvenliği farkındalığı farklı değişkenler açısından incelenmiştir. Araştırma kapsamında öğretmenlerin dijital vatandaşlık farkındalıkları geliştirdikleri ölçek ile tespit edilmeye çalışılmıştır. Araştırmanın nitel boyutu için yapılan görüşmelerde; öğretmenlerin ve eğitim fakültesindeki öğretim üyelerinin dijital veri güvenliği farkındalığı hakkındaki görüşleri tespit edilmeye çalışılmıştır. Öğretmenlerin ve öğretim üyelerinin kişisel bilgisayarını veya teknolojik cihazını korumak için veya güvenliği sağlamak için; genelde güncel virüs programları kullandıkları, internet sitelerin SSL (Secure Sockets Layer - Güvenli Giriş Katmanı) sertifikalı olup olmadığı, adres çubuğunda yazan adreslerin doğru olup olmadığı, tarayıcı geçmişini silme, ağır güvenliğinden emin olma, güvenli olmayan e-postayı açmama gibi güvenlik önlemleri aldıkları görülmüştür. Araştırmanın nicel boyutunda toplanan verilere göre; öğretmenlerin günlük

bilgisayar ve internet kullanımı 4 saatin altındadır. Ayrıca öğretmenlere uygulana Dijital Veri Güvenliği Farkındalığı (DVGF) ölçeği sonuçlarına göre; kadınların ve erkeklerin DVGF arasında anlamlı bir fark tespit edilmiştir. Branş bazında yapılan analizlerde anlamlı bir fark görülemedi. Yine mesleki deneyim, öğrenim kademesi ve öğrenim durumuna göre fark bulunamazken; günlük bilgisayar kullanımı, günlük internet kullanımı ve kişisel teknolojik cihazı olma durumuna göre farklılaştığı görülmüştür. Sonuç olarak dijital veri güvenliğinin tamamen sağlanması için toplum genelinde dijital veri güvenliği eğitimleri verilmesi gerektiği, küçük yaş kademelerinden itibaren okullarda bu alanda eğitimler verilmesi gerektiği üzerinde durmuştur.

Gökmen(2015) Sakarya, Siirt, Amasya ve Erzincan Üniversitesi'nde öğrenim gören 375 Bilgisayar ve Öğretim Teknolojileri Eğitimi bölümünde öğrenim gören öğretmen adayının bilişim güvenliği eğitimi verebilme yeterliliklerini ölçtüğü çalışmada; bu bölümdeki öğretmen adaylarının bilişim güvenliği yeterliliklerinin, cinsiyete ve öğrenim gördüğü üniversiteye göre değiştiği sonucuna varmıştır. Ayrıca öğretmen adaylarının bilişim güvenliği bilgilerinin düşük olduğu, bilişim güvenliği konusunda eğitim verebilme konusunda yeterli olmadığı sonucuna ulaşmıştır. Bu yeterliliğe sahip olunması için Bilgisayar ve Öğretim Teknolojileri Eğitimi lisans programında bu konuya yönelik zorunlu derslerin olması gerektiği vurgusu yapılmıştır.

Mart'ın (2012) BÖTE alanında bilgi güvenliği farkındalığını ölçmek amacı ile yapmış olduğu çalışmasının örneklemini Türkiye'de yaşayan farklı meslek gruplarından 501 kişi oluşturmuştur. Çalışmada veriler geliştirilen "Bilişim Kültüründe Bilgi Güvenliği Anketi" ile toplanmıştır. Araştırmaya katılanların bilgi güvenliği farkındalıkları ile teknoloji kullanımlarının; yaş, bilgisayar ve internet kullanım süreleri, cinsiyet, eğitim seviyeleri ve mesleklerine göre farklılaşım farklılaşmadı tespit edilmeye çalışılmıştır. Araştırma sonuçlarına göre katılımcıların teknoloji kullanımları ile yaş bilgisayar kullanımı ve internet kullanım süresine göre anlamlı farklılık görülürken; cinsiyet eğitim seviyesi ve meslek çeşitlerine göre anlamlı farka rastlanamamıştır. Katılımcıların bilgi güvenliği farkındalıkları ile yaş, cinsiyet, mesleklerine göre anlamlı farklılık tespit edilirken; eğitim durumlarına ve internet ve bilgisayar kullanım oranlarına göre anlamlı bir fark bulunamamıştır. Genel anlamda çalışma sonuçlarına bakarak yaptığı değerlendirmede; bireylerin bilgi güvenliği düzeylerinin istenilen seviyede olmadığı, bilgisayar ve bilgi güvenliğine yönelik farkındalık eğitimlerinin yetersiz olduğu belirtilmiştir.

Çakır (2012) öğretmen adaylarının sosyal ağlardaki siber güvenlik farkındalıklarını incelediği çalışmada; Sınıf, Fen Bilgisi, BÖTE, Türkçe, PDR, Matematik, Okul Öncesi, Sosyal Bilgiler öğretmenliği bölümlerinden 3. ve 4. sınıf toplam 909 öğretmen adayından veri toplanmıştır. Araştırma sonuçlarına göre katılımcıların güvenlik farkındalıkları cinsiyete göre erkeklerin lehine olacak şekilde farklılaşmaktadır. Ayrıca katılımcılar şifre oluşturma ve gizli sorunun cevabını gizli tutma konusunda yüksek düzey farkındalık düzeyine sahiptir. Ayrıca araştırmada katılımcıların

sosyal ağ hesapları oluştururken güvenlik politikalarını ve kullanım şartlarını okuma konusunda düşük farkındalığa sahip oldukları belirtilmiştir. Öğretmen adaylarının güvenlik tehditlerinin üstesinden gelmesi konusundaki farkındalıkları orta düzeyde olduğu, bu seviyenin geliştirilmesinin gerekliliği belirtilmiştir. Bu bağlamda bilişim teknolojileri branşına ayrı parantez açılmış, öğretim elemanlarına ve öğretmenlere büyük sorumluluk düştüğü vurgulanmıştır. Ayrıca bilişim teknolojileri dersi müfredatına bu alana yönelik yeni eklemelerin yapılması gerektiği vurgulanmıştır.

Tekerek (2013) Kahramanmaraş'ta ilk ve ortaöğretim düzeyinde öğrenim gören 2449 öğrenciden oluşan örnekleme yapmış olduğu çalışmada; kendi geliştirmiş olduğu "Bilgi Güvenliği Farkındalığı" ölçeği ile öğrencilerin bilgisayar alışkanlıklarını ve bilgi güvenliği farkındalıklarını ölçmeyi amaçlamıştır. Araştırma sonucuna göre; kız öğrencilerin bilgi güvenliği farkındalıkları erkek öğrencilere göre daha yüksek çıkmıştır. Ayrıca orta öğretim düzeyindeki öğrencilerin farkındalıkları ilköğretim düzeyine göre yüksek çıkmıştır. Yaşadıkları yerleşim bölgesine göre ise şehir merkezinde yaşayanların bilgi güvenliği farkındalıklarının daha yüksek olduğu görülmektedir. Araştırmasında ABD ulusal bilgi güvenliği raporuna yer verdiği bölümde, öğretmenlerin çok azının öğrencileri temel internet kullanımı ve bilgi güvenliği konusunda bilgilendirdiği vurgulanmıştır. Ayrıca Türk eğitim sisteminde bilgi ve iletişim teknolojileri ders saatlerinin az olduğu belirtilmiş, buradan yola çıkarak öğrencilere bilgi güvenliği farkındalığı eğitimlerinin daha fazla verilmesi gerekliliği vurgulanmıştır. Ayrıca daha düşük kademelerden itibaren bilgi güvenliği farkındalığı eğitimlerinin verilmesinin önemi üzerinde durulmuştur. Vardal (2009) "Yüksek Öğretimlerde Bilgi Güvenliği" adıyla yapmış olduğu çalışmada, Bilgi Güvenliği Yönetim Sistemi adında bir model önerisinde bulunmuş ve modelin pilot uygulamasını yapmıştır. Araştırmasında bilgi güvenliğinin sağlanması için en zayıf halka olan insan üzerinde duran araştırmacı, bilgi güvenliği için sadece teknolojik alt yapıların yeterli olmadığı, insan eğitimlerinin şart olduğu vurgusu yapmıştır.

Güldüren (2015) "Yükseköğretimde Öğretim Elemanlarının Bilgi Güvenliği Farkındalıklarını Değerlendirilmesi" adıyla yapmış olduğu çalışmasında; öğretim elemanlarının bilgi güvenliği farkındalıklarını geliştirmek amacı ile bir web sitesi tasarlanmış, sitenin bilgi güvenliği kazandırmadaki etkisi incelenmiştir. 65 katılımcı(31 deney 34 kontrol grubu) ile 12 hafta boyunca yapılan çalışma sonucunda, verilen eğitimin bilgi güvenliği farkındalığını artırmada etkisini incelemek için deney ve kontrol grubuna ön test ve son test uygulanmıştır. "Bilgi güvenliği farkındalığı" adındaki site üzerinden eğitimler alan deney grubunun son test puanının kontrol grubuna göre daha yüksek olduğu gözlenmiştir. Ayrıca bilgi güvenliği farkındalıklarının cinsiyet, bilgisayar kullanım süresi, unvan gibi değişkenlere göre farklılaşmadığı gözlenmiştir. Bilgi güvenliğinde yaşanan olayların temelinde insan olduğu vurgusu yapılan çalışmada zayıf halka

olan insana verilmesi gereken eğitimler üzerinde durulmuştur. Bu eğitimlerin yaşam boyu devam etmesi gerektiği, eğiticinin ortamda bulunmadığı durumlarda bu eğitimlerin uzaktan da verilebileceği vurgulanmıştır. Yine Güldüren ve Keser (2016) ortaöğretim öğrencilerinin bilgi güvenliği farkındalıklarını ölçmek için geliştirdikleri ölçek çalışması kapsamında 607 öğrenciye ulaşılmıştır. Elde edilen veriler hem ölçeğin geçerlilik ve güvenilirliğini tespit için kullanılmış hem de bazı değişkenlere göre analizler yapılmıştır. Bu analiz sonuçlarına göre; bilgi güvenliği farkındalığının erkek öğrencilerin lehine olacak şekilde farklılaştığı görülmüştür. Ayrıca liseye yeni başlamış ve üst sınıflardaki öğrencilerin bilgi güvenliği farkındalıklarının tespit edilmesi, bilgi güvenliği farkındalık seviyeleri düşük öğrencilere eğitimler verilmesi gerektiği vurgusu yapılmıştır.

Eminağaoğlu ve Gökşen (2009) dünyada ve Türkiye’den almış olduğu istatistiksel bilgilerden yararlanarak bilgi güvenliğinin sağlanmasında yapılan ortak yanlışlara dikkat çekmiş, uzun ve kısa vadede çözüm önerileri sunmuş, bilgi güvenliğinin sağlanması için en önemli etken olan insana yatırım yapılmasının gereğini vurgulamıştır. Bu amaçla bilgi güvenliği farkındalığı eğitimlerinin gerekliliği belirtilmiştir. Ayrıca sanıldığı gibi bilgi güvenliğinin sadece bilgisayar ve teknoloji güvenliği olmadığını önemi vurgulanmıştır. Genelde bilgi güvenliği denilince akla gelen kurumların bankacılık ve finans sektörleri olduğu, fakat bilgi güvenliğinin genele yayılması gerektiği belirtilmiştir. Genele yayılmanın da insanları bilgi güvenliği konusunda bilinçlendirme ile sağlanacağı vurgulanmıştır. Sonuç olarak; kurumlarda bilişim teknolojilerinden sorumlu personelden başlanarak gerekli eğitimlerin verilmesi, yöneticilerin sürece katılması, ülke olarak yasal zeminlerin oluşturulması gibi çözüm önerileri de sunulmuştur. Çetin (2014) ise kişilerin bilgi güvenliği algılarını ölçtüğü çalışmasında geliştirmiş olduğu “Kişisel Veri Güvenliği” anketini kullanarak veri toplamıştır. Değerlendirmeye alınması uygun görülen 501 kullanıcıdan topladığı veri sonuçlarına göre katılımcıların büyük bir bölümünün bilgi güvenliğine önem verdiği görülürken, yarısından fazlasının güncel tehlikelerden haberinin olmadığı saptanmıştır. Katılımcıların kişisel bilgisayarlarında anti virüs programı kullanırken cep telefonu ve tabletlerinde virüs programı kullanmaya ihtiyaç duymadığı da görülmüştür. Ayrıca olası bilgi güvenliği tehlikesinde nereye haber vereceği konusunda bilgisi olmayan katılımcıların oranı da bir hayli yüksek çıkmıştır. Erkek katılımcıların bilgisayar güvenliği farkındalıkları ise kadınlar göre daha yüksek çıkmıştır. Çalışmanın diğer alan yazındaki çalışmalarla kesişen bir önemli sonucu da kullanıcıların bilgi güvenliği konusunda eğitime ihtiyaçları olması ve buna istekli olmalarıdır. Çolak (2019) tarafından üniversite öğrencilerinin dijital güvenlik öz yeterliliklerini ve çevrim içi risk alma eğilimlerini araştırdığı çalışmada toplam 1601 katılımcıdan veri toplamıştır. Araştırma kapsamında öncelikle ölçek geliştirmiş, sonrasında geliştirilen ölçek ile Eskişehir ili devlet üniversitelerinden veri toplanmıştır. Araştırma sonuçlarına göre üniversite

öğrencilerinin dijital öz yeterlilikleri yüksek çıkmışken, çevrim içi risk alma eğilimleri düşük çıkmıştır. Ayrıca üniversite öğrencilerinin dijital öz yeterlilikleri ve çevrim içi risk alan eğilimleri cinsiyet, internet kullanım süresi, yaş gibi değişkenlere göre incelenmiştir. Sonuçlara göre hem öz yeterliliklerin hem de çevrim içi risk alma eğilimlerinin cinsiyete göre ve internet kullanım süresine göre farklılaştığı görülmüştür. Seferoğlu ve Yiğit (2019) üniversite öğrencilerinin siber güvenlik davranışlarını kişilik özellikleri ve cinsiyet, sınıf düzeyi, bölüm, bilişim güvenliği eğitimi alma durumu ve haftalık internet kullanım süresi değişkenlerine göre incelemiştir. Araştırmanın çalışma grubunu 2017-2018 eğitim-öğretim yılı bahar döneminde Türkiye'nin farklı üniversitelerinde ön lisans ve lisans düzeylerinde öğrenim gören 420 öğrenci oluşturmaktadır. Betimsel tarama modeli kullanılarak elde edilen verilerin sonuçlarına göre bilgisayar ile doğrudan ilişkili olmayan lojistik, PDR ve okul öncesi öğretmenliği programı öğrencilerinin siber güvenlik davranışları istenen düzeyde değildir. Ulaşılan bulgulardan ilki öğrencilerin siber güvenlik davranışları ile ilgili düzeylerinin yeterli denebilecek düzeyde olduğu yönündedir. Ulaşılan bulgular tüm ölçekten alınan genel siber güvenlik davranış puanlarının cinsiyete göre farklılaşmadığını göstermiştir. Siber güvenlik farkındalıkları 3. ve 4. sınıfta daha yüksektir. Siber güvenlik farkındalıkları bölüme göre, internet kullanım süresine göre farklılaşmaktadır.

Üniversitelerin internet sitelerine girerek yapmış olduğumuz tarama neticesinde; Türkiye'de siber güvenlik üzerine 3 tanesi lisans düzeyinde olmak üzere 15 üniversitede ders verilmektedir. Bu derslerin tamamı da mühendislik fakültelerindedir. Bazı eğitim fakültelerinde Dijital Vatandaşlık üzerine ise sadece Sosyal Bilgiler Öğretmenliği bölümünde ders verilmektedir. Türkiye'de 32'si devlet 4'ü özel olmak üzere toplam 36 üniversitede sosyal bilgiler öğretmenliği bölümü bulunmaktadır. Bu bölüme sahip üniversitelerin neredeyse tamamında ise vatandaşlık kavramının alt basamağı olarak dijital vatandaşlığa değinilmektedir. Direkt olarak "Dijital Vatandaşlık Eğitimi" adı ile açılan bir ders sadece Anadolu Üniversitesi Sosyal Bilgiler Öğretmenliği programında bulunmaktadır. Henüz eğitim fakültelerinde siber güvenlik üzerine bir dersin verilmiyor olması ve dijital vatandaşlık üzerine derslerin yok denecek kadar az olması, yetişen öğretmen adaylarının siber güvenlik ve dijital vatandaşlık farkındalıklarının ne düzeyde olduğu sorusunu beraberinde getirmektedir. Hem siber güvenlik hem de dijital vatandaşlık eğitimlerine üniversitelerde bu kadar az yer veriliyor olması bizim araştırmamızın araştırma problemini ve önemini destekler niteliktedir.

Alan yazında DV ile ilgili yapılan çalışmalar özetleyecek olur isek; dijital vatandaşlığın 21.yy becerilerinden olduğu, internet tutumu, bilgisayar öz yeterliliği ve teknoloji kullanımı arasında pozitif bir ilişki olduğu belirtilmiştir. Ayrıca DV düzeyi yüksek olan bireylerin daha az çevrim içi mağduriyet yaşadığı vurgulanmıştır. Erken yaşlarda verilecek DV eğitimlerinin çevrim içi ortamlarda yaşanacak mağduriyeti azaltacağı belirtilmiştir. Yine alan yazında vurgulanan diğer

bir husus ise öğretmenlere veya öğretmen adaylarına verilmesi gereken DV farkındalığı eğitimleridir. Verilecek bu eğitimler sayesinde toplumda daha fazla kitleye ulaşılabileceği düşünülmektedir. SBGF ile ilgili yapılan çalışmalar özetleyecek olursak; hem yabancı hem de yerli alan yazında SBGF farkındalığının oluşturulmasında insan faktörü üzerinde durulmuştur. Yaşanan birçok zafiyetin insan kaynaklı olduğu, bu zafiyetin hem işletmeleri hem de şahısları büyük maddi kayıplara uğrattığı vurgulanmıştır. Özellikle erken yaşlarda verilecek eğitimlerin SBGF'ni arttıracığı belirtilmiş, yine öğretmen veya öğretmen adaylarının SBGF'nin artırılmasının toplumun birçok kesimine dokunması adına önemli olduğu belirtilmiştir. Ayrıca 21. yy ile birlikte siber güvenlik alanında dünya genelinde büyük sermayelere sahip yeni bir sektörlerin oluştuğuna değinilmiştir. Yapmış olduğumuz alan yazın taramalarında da görüldüğü üzere, siber güvenlik ve dijital vatandaşlık hakkında farkındalık oluşturulması için insanların eğitilmesi ihtiyaçtır. Bu farkındalığı sağlamak adına gelecek hayatında toplumun büyük bir kesimine dokunacak öğretmen adaylarının siber güvenlik dijital vatandaşlık farkındalıklarının oluşturulması daha önceliklidir.

3.YÖNTEM

Araştırmada öğretmen adaylarının Siber Bilgi Güvenliği Farkındalıkları ile Dijital Vatandaşlık seviyelerinin çeşitli değişkenler açısından belirlenmesi ve iki değişken arasındaki ilişki durumunun tespit edilmesi amaçlanmıştır. Bu amaç doğrultusunda alan yazın taramaları yapılmış, uzman görüşleri alınmış ve kullanılacak ölçekler şekillenmiştir. Yöntem bölümünde araştırma yöntemi, örneklem ve evreni, verilerin analizi, veri toplama araçları ve veri toplama süreci ile ilgili alt başlıklara yer verilmiştir.

3.1. Araştırma Modeli

Öğretmen adaylarının siber bilgi güvenliği farkındalığını ve dijital vatandaşlık düzeylerini belirleyip, aralarında ilişki olup olmadığını belirlemek için yapılan bu araştırmada tarama modeli içerisinde yer alan ilişkisel tarama modeli kullanılmıştır. Tarama modeli; diğer araştırmalara göre çok daha büyük örneklem kapsayan, her hangi bir konuda katılımcıların; görüşlerini, ilgisini, yeteneğini vb. özelliklerini belirlemede kullanılan araştırma modelidir (Fraenkel, Walle ve Hyun, 2012). Mevcut durumun tespiti olarak da kullanılan tarama modeli, problemin ne durumda olduğunu görmemizi sağlar. Ayrıca tarama araştırmalarında amaç büyük kitlelerin özelliklerini betimlemektir (Büyüköztürk, Çakmak, Akgün, Karadeniz ve Demirel, 2016). Karasar'ın (2012) tanımıyla tarama modeli "Geçmişte ya da halen var olan bir durumu var olduğu şekliyle betimlemeye yarayan yaklaşımdır". İlişkisel tarama modeli ise; iki veya daha fazla değişkenin birbirini etkileme derecesini belirlemek için yapılan araştırma modelidir (Karasar, 1991, s.77). Bu araştırmada da öğretmen adaylarının Siber Güvenlik Farkındalıkları ve Dijital Vatandaşlık Düzeylerinin ne durumda olduğu tespit edilmiştir. Ayrıca araştırmada dijital vatandaşlık düzeyi ile siber bilgi güvenliği farkındalığı arasındaki ilişki çeşitli değişkenlere göre incelendiğinden tarama modellerinden ilişkisel tarama modeli kullanılmıştır.

3.2. Araştırmanın Evren ve Örneklemi

Evren; araştırma sonucu cevaplanması beklenen sorular için ihtiyaç duyulan verilerin elde edildiği canlı ya da cansız varlıklardan oluşan büyük gruplardır (Büyüköztürk ve diğerleri, 2016). Örneklem ise; "özellikleri hakkında bilgi toplamak için çalışılan evrenden seçilen onun sınırlı bir parçası" olarak tanımlanmaktadır (Büyüköztürk ve diğerleri, 2016, s.81). Evrenden çalışmanın amacına uygun birim seçme ve bu süreçteki yapılan tüm işlemlere de örnekleme denilmektedir (Yıldız, 2016). Seçkisiz olmayan örneklemede birim seçilirken örneklem için seçilme olasılıkları eşit değildir. Uygun (convenience) örneklemede ise seçkisiz olmayan örnekleme içinde yer alan örnekleme türüdür. Bu örneklemede; zaman, para, iş gücü gibi kısıtlı imkânlar yüzünden

örneklem daha kolay ulaşılabilir ve uygulanabilir birimlerden örneklem seçilir (Büyüköztürk, 2016). Araştırmada gerek maddi imkanlar gerek ise kısıtlı zaman nedeni ile örneklem kolay ulaşılabilir birimden seçilmiştir. Bu nedenle araştırmanın örneklem türü “uygun örneklem” olarak belirlenmiştir. Bu araştırmanın örneklemini Akdeniz Bölgesinde yer alan bir devlet üniversitesinin eğitim fakültesinde öğrenim gören öğretmen adayları oluşturmuştur. Araştırmanın evrenini Türkiye’nin Akdeniz Bölgesi’nde bulunan devlet üniversitelerinin eğitim fakültelerinde lisans eğitimi gören öğretmen adayları oluşturmaktadır. Araştırmanın ulaşılabilir evreni ise araştırma yapılan devlet üniversitesi Eğitim Fakültesi’nde lisans eğitimi gören öğretmen adayları olarak belirlenmiştir. Araştırmanın yapıldığı üniversitesinin resmi internet sitesinden alınan verilere göre, eğitim fakültesinde örgün öğretime kayıtlı 1432’si kadın 770’i erkek 2202 öğretmen adayı bulunmaktadır. Bu sayı araştırmanın ulaşılabilir evrenini oluşturmaktadır. Katılımcılara ulaşmak için üniversitenin Eğitim Fakültesi’nin resmi internet sitesinde yer alan ders programlarından öğretmen adaylarının ders saatleri ve derse giren akademisyenler belirlenmiştir. Daha sonra derse giren akademisyenlerin her biri ile görüşülerek ölçek uygulanması konusunda izinler alınmıştır. Ders hocasının uygun olmadığı veya sayının az olduğu durumlarda başka ders hocası ile görüşülerek maksimum katılımcı sayısına ulaşılmaya çalışılmıştır.

Tablo 3.1

Araştırmaya katılan öğretmen adaylarının bölümlere sayıları ve yüzdeleri.

Bölüm	Sayı	Yüzde(%)
Böte	42	59.14
Fen	174	74.04
Matematik	150	58.13
Sınıf	176	56.95
Okul Öncesi	158	44.25
PDR	196	57.14
Türkçe	134	45.27
Yabancı Dil	125	37.53
Total	1155	52.45

Tablo 3.1’ de bölümlere göre araştırmaya katılan öğretmen adayı sayıları ve yüzdeleri verilmiştir. Araştırmaya verinin toplanacağı üniversitenin Eğitim Fakültesinde kayıtlı 2202 öğretmen adayına ulaşmak amacı ile başlanmışken toplamda 1209 öğretmen adayına ulaşılmıştır. Fakat veri girişleri sırasında 54 adet ölçek eksik doldurulması nedeni ile değerlendirilmeye alınmamış, 1155 kişi ile analizlere devam edilmiştir. Veri toplama sürecinde üniversitenin Eğitim Fakültesinin 8 farklı bölümünden toplam 1155 öğretmen adayına ulaşılmıştır. Katılımcı sayısı en az olan bölümün BÖTE, en fazla olduğu bölümün PDR olduğu görülmektedir. Yüzde dağılımları

incelendiğinde ise en düşük katılım yüzdesinin Yabancı Dil Öğretmenliği (İngilizce Öğretmenliği) bölümünde, en yüksek katılımcı yüzdesini ise Fen Bilimleri Öğretmenliği bölümünde olduğu görülmektedir. BÖTE bölümündeki katılımcı sayısının diğer bölümlerden düşük olmasının sebebi YÖK'ün son iki yılda söz konusu üniversitedeki BÖTE bölümüne kontenjan vermemesidir.

Tablo 3.2

Araştırmaya katılan öğretmen adaylarının cinsiyete göre sayıları

Kadın	Yüzde(%)	Erkek	Yüzde(%)
809	70.04	346	29.96

Tablo 3.2'ye göre araştırmaya katılan kadın öğretmen adayı 809'iken (%70,04) erkek öğretmen adayı sayısı 346'dır (%29,6). Bu verilere bakılarak kadın öğretmen adayı sayısının erkek öğretmen adayı sayısının iki katından fazla olduğunu söylemek mümkündür.

Tablo 3.3

Sınıf kademelerine göre Eğitim Fakültesine kayıtlı öğretmen adayı ve değerlendirmeye alınan öğretmen adayı sayıları.

Sınıf Kademesi	Kayıtlı Olan	Araştırmaya Katılan	Yüzde(%)
1.Sınıf	546	319	58.42
2.Sınıf	539	286	53.06
3.Sınıf	539	366	67.90
4.Sınıf	578	284	49.13
Toplam	2202	1155	52.45

Tablo 3.3'e bakıldığında araştırmaya katılan öğretmen adaylarının 319'u 1.sınıf, 286'sı 2.Sınıf, 366'sı 3.sınıf ve 284'ü 4.sınıftır. Toplam katılımcı sayısına bakıldığında örneklemin %52,45'ine ulaşıldığı görülmektedir.

Tablo 3.4

Araştırmaya Katılan Öğretmen Adayların Teknolojik Alete Sahip Olma Durumları

Sahip Olduğu Teknolojik Aletler	Kişi Sayısı	Toplam Kişi Sayısı
Bilgisayar+ Tablet+ Akıllı Telefon	152	
Bilgisayar+ Akıllı Telefon	444	
Tablet+ Akıllı Telefon	110	
Akıllı Telefon	1140	
Bilgisayar	607	
Tablet	265	1155
Sadece Akıllı Telefonu Olan	434	
Sadece Bilgisayarı Olan	10	
Sadece Tableti Olan	2	

Tablo 3.4' te öğretmen adaylarının teknolojik aletlere sahip olma durumları gösterilmiştir. Bu verilere; bilgisayar, telefon ve tableti olan, sadece bilgisayar ve akıllı telefonu olan, tablet ve akıllı telefonu olan, akıllı telefonu olan, bilgisayarlı olan, tableti olan, sadece akıllı telefonu olan, sadece bilgisayarlı olan ve sadece tableti olan öğretmen aday sayıları verilmiştir.

Tablo 3.5
Araştırmaya Katılan Öğretmen Adayların Teknoloji Kullanım(GTK) ve Günlük Sosyal Medya(GSK) Kullanım Sürelerine Göre Sayıları

Süre	Teknoloji Kullanıcı Sayısı	Sosyal Medya Kullanıcı Sayısı
1 saatten az	39	223
1-3 saat	463	587
4-6 saat	509	280
7 saat ve üzeri	144	65
Toplam	1155	1155

Tablo 3.5' te araştırmaya katılan öğretmen adaylarının GTK süresi ve GSK süresine göre sayıları verilmiştir. Teknoloji kullanımından kasıttın sadece bilgisayar, akıllı telefon ve tablet kullanımı olarak anlaşılmadığı görülmektedir. Bazı süre zarflarında sosyal medya kullanıcı sayısının teknoloji kullanıcı sayısından fazla olmasının sebebi bu olabilir.

3.3. Veri Toplama Araçları

Çalışma kapsamında SBGF ve DV düzeylerini tespit etmek için öncelikle alan yazında bu konuda geliştirilmiş olan ölçme araçları irdelenmiştir. İnceleme sonucunda alan yazında bu iki yapıyı ele alan farklı ölçme araçlarının geliştirildiği görülmüştür. Bu ölçme araçları içerdiği maddeler bazında ele alınmış ve Yılmaz (2015) tarafından geliştirilen "Siber Bilgi Güvenlik Farkındalığı Ölçeği" ile İşman ve Güngören (2014) tarafından geliştirilen "Dijital Vatandaşlık Ölçeği"nin bu çalışmanın kapsamına uygun olduğu belirlenmiştir. Veri toplama aracı; iki ölçek ve kişisel bilgi formu olmak üzere 3 bölümden oluşmaktadır(EK.2, EK.3,EK.4).

- A. *Siber Bilgi Güvenliği Farkındalığı Ölçeği*: Veri toplama sürecinin ilk bölümünde Yılmaz (2015) tarafından geliştirilen 32 maddelik ölçek kullanılmıştır. Yapılan alan yazın taramasında siber bilgi güvenliği farkındalığını ölçmeye yönelik birden çok ölçek tespit edilmesine rağmen uzman görüşü ve madde madde yapılan analizler neticesinde bu ölçeğin kullanılması uygun bulunmuştur. Ölçekteki ifadeler beşli Likert tipinde "Kesinlikle Katılıyorum", "Katılıyorum", "Kararsızım", "Katılmıyorum", "Kesinlikle Katılmıyorum" biçimindedir. "Kesinlikle Katılmıyorum" seçeneğinden başlamak üzere 1'den 5'e artan şekilde puanlanmıştır. Yapmış olduğumuz analizde tek

faktörlü yapıya sahip ölçek maddelerinin Cronbach Alfa (α) iç tutarlılık katsayısı .935 olarak bulunmuştur. Aynı ölçek için Yılmaz (2015) bu değeri .945 olarak bulmuştur.

- B. *Dijital Vatandaşlık Ölçeği*: Kullanılacak ölçeğe karar verilirken alan yazında kullanılmaya uygun olan ölçekler tespit edilmiş, ölçeklerin geçerlilik ve güvenilirlik puanları incelenmiş, uzman görüşleri alınmıştır. Sonuç olarak İşman ve Güldüren (2014) tarafından geliştirilen 33 maddelik “Dijital vatandaşlık Ölçeği” kullanılmasına karar verilmiştir. Dijital vatandaşlık düzeyini tespit etmeye yönelik geliştirilmiş bu ölçek için Cronbach Alpha değeri .850 bulunmuştur. Ölçeğin 9 Alt faktörü incelendiğine Cronbach Alpha; dijital okuryazarlık boyutunda .78, dijital hukuk boyutunda .84, dijital hak ve sorumluluklar boyutunda .80, dijital iletişim boyutunda .79, dijital güvenlik boyutunda .85, dijital ticaret boyutunda .84, dijital erişim boyutunda .90; dijital etik boyutunda .70 ve dijital sağlık boyutunda .70 olarak bulunmuştur. Bizim yapmış olduğumuz analizler neticesinde dijital vatandaşlık ölçeğinin Cronbach Alpha değeri .881 bulunmuştur.
- C. *Kişisel Bilgi Formu*: Veri toplama aracının son bölümünde yer almaktadır. Bu bölümde öğretmen adaylarının Cinsiyet, Üniversite, Bölüm, Sınıf kademesi, Günlük Toplam Akıllı Telefon-Tablet-Bilgisayar Kullanım Saati, Sosyal Medya Kullanım Saati, Tablet-Bilgisayar- Akıllı Telefon Sahibi olup olmama durumunu belirlemek amacı ile sorulan 7 maddeden oluşmaktadır. Öğretmen adaylarının SBGF ve DV düzeylerini farklı değişkenlere göre incelemek için bu bilgilere ihtiyaç duyulmuştur.

3.4 Veri Toplama Süreci

SBGF, DV ölçeği ve Kişisel Bilgi formundan oluşan veri toplama aracının uygulanması sürecinde devlet üniversitesinin idari birimlerinden gerekli izinler alınmıştır (EK-1). Veri toplama aracı verinin toplandığı üniversitenin Eğitim Fakültesinde bulunan; BÖTE, Fen Bilgisi Öğretmenliği, İlköğretim Matematik Öğretmenliği, Sınıf Öğretmenliği, Okul Öncesi Öğretmenliği, Psikolojik Danışmanlık ve Rehberlik, Türkçe Öğretmenliği ve İngilizce Öğretmenliği bölümlerinin 1. 2. 3. ve 4. sınıf kademelerinden toplam 1209 öğretmen adayına 2019-2020 eğitim öğretim yılının Ekim-Kasım aylarında uygulanmıştır. Verilerin toplanma sürecinde ilgili bölümlerin ders programları üniversitenin sitesinden temin edilerek ders saatleri ve derse giren akademisyenler tespit edilmiştir. İlgili her ders hocası ile bizzat veya tez danışmanı aracılığı ile görüşülerek ölçeğin uygulanma tarihi ile ilgili randevular alınmıştır. Ölçekler tek bir kâğıda arkalı önlü şekilde basılmış olup, iki ölçek aynı anda uygulanmıştır. Uygulama için randevu alınan saatlerde ilgili dersliğe gidilerek ölçekler bizzat araştırmacı tarafından dağıtılmıştır. Araştırmacı öncelikle

öğrencilere ölçek ve amacı hakkında bilgi vermiş, öğretmen adaylarının ölçeği gerçek görüşlerini yansıtacak şekilde doldurmaları konusunda açıklamada bulunmuştur. Ölçeklerin ikisi için toplamda yaklaşık 15 dakika verilmiştir. Ölçeklerin doldurulması esnasında iki ölçek olduğu hatırlatılmış, arka sayfaların boş bırakılması önlenmeye çalışılmıştır.

3.5 Verilerin Analizi

Verilerin analizi için SPSS 20 programı kullanılmıştır. Veriler SPSS 20 programına girilirken ölçek maddelerine verilen cevaplar; Kesinlikle Katılmıyorum "1", Katılmıyorum "2", Kısmen Katılıyorum "3", Katılıyorum "4", Kesinlikle Katılıyorum "5" olarak belirlenmiştir. Ayrıca cinsiyet değişkeninde Kadın "1", Erkek "2" sınıf kademeleri "1","2","3","4" şeklinde belirlenmiştir. Günlük Teknoloji Kullanım Saati (GTK) ve Günlük Sosyal Medya Kullanım Saati (GSK) için: 1 saatten az "1", 1-3 saat "2", 4-6 saat "3", 7 saat üzeri "4" olarak; Tablet, Bilgisayar ve Akıllı telefonu sahip olma durumu "1", olmama durumu "0" olarak belirlenmiştir. Verilerin girişleri sırasında 54 adet kullanıcın ölçeği; arka sayfanın boş bırakılması, çok fazla boş bırakma ve birden çok seçenek işaretleme gibi nedenlerle dikkate alınmamıştır. Analizler toplamda 1155 öğretmen adayı üzerinden gerçekleştirilmiştir. Sağlıklı toplanan veri oranı %95.51 olarak tespit edilmiştir.

Betimsel analiz, analiz sürecinin ilk aşamasında kullanılan; ortalama, mod, medyan, standart sapma gibi ölçülmesinin mümkün olduğu değerlerin ve katılımcıların yanıtlarının genel şablonun çıkarıldığı analiz tekniğidir (Bayrak, 2017). Bu araştırmada öncelikle betimsel analiz yapılmış, daha sonra ise çıkarımsal analiz olarak t-testi ve tek yönlü Varyans Analizi (ANOVA) gerçekleştirilmiştir. T-testi iki gruptan elde edilen ortalamaların birbirinden farklı olup olmadığını tespit etmek için kullanılan yöntemdir (Büyüköztürk, 2016). Ortalamalar arasında fark olup olmadığını araştırmak, iki veya daha fazla grubun birbirinden farklı olup olmadığını tespit etmek için kullanılan analiz yöntemi ANOVA'dır (Akyıldız, 2009). Öğretmen adaylarının SBGF ve DV düzeylerinin cinsiyete göre farklılaşıp farklılaşmadıklarını tespit etmek için T-testi analizi uygulanmıştır. Ardından birden fazla grup olması dolayısı ile farklılaşmaların tespiti için ANOVA analizleri gerçekleştirilmiştir. Öğretmen adaylarının; öğrenim gördükleri bölümlerin SBGF ve DV düzeylerine etkisini incelemek, sınıf kademelerinin SBGF ve DV düzeyleri ile ilişki durumunu incelemek, GTK sürelerinin SBGF ve DV düzeyleri ile ilişki durumunu, GSK sürelerinin SBGF ve DV düzeyleri ile ilişki durumunu incelemek için ANOVA gerçekleştirilmiştir. Gruplar arası fark tespit edildiğinde, tespit edilen farkın hangi gruptan kaynaklı olduğunu ortaya çıkaran istatistik yöntemi post-hoc olarak bilinmektedir (Köklü ve diğerleri, 2007). Analizlerde gruplar arası farklılaşma tespit edilmiş, bu farklılaşmanın kaynağına tespit etmek için ise post-hoc testine bakılmıştır. Son olarak DV ile SBGF arasında ilişki olup olmadığını tespit etmek için korelasyon analizi gerçekleştirilmiştir.

3.6 Geçerlilik ve Güvenirlilik

Bağımlı değişkenlerde meydana gelen değişimlerin, bağımsız değişkenlerce açıklanabilme derecesine iç geçerlilik denilmektedir. Elde edilen sonuçların evreni temsil edebilme derecesine de dış geçerlilik denilmektedir (Büyüköztürk ve diğerleri, 2016). Araştırmada iç geçerliliği ve dış geçerliliği tehdit edebilecek faktörler dikkate alınmıştır. Bu kapsamda geçerliliğin sağlanması için örneklem seçiminde zaman, maliyet, ulaşılabilirlik göz önünde tutulmuştur. Veri toplama esnasında verinin toplandığı ortamın benzer olmasına özen gösterilmiştir. Verilerin tamamı sınıf ortamında toplanmıştır. Verilerin büyük bölümü araştırmacı tarafından bizzat toplanmıştır. Bizzat uygulanan ölçeklerde ölçek hakkında tüm açıklamalar yapılmıştır. Bazı durumlarda ölçek, danışman veya veri toplanan gruba dersi olan akademisyen tarafından uygulanmıştır. Bu durumlarda ölçek uygulayıcısı detaylı şekilde bilgilendirilmiştir. Ölçeğin uygulanması sırasında tesadüfi, sistematik veya sabit hataların yapılmaması için gerekli önlemler alınmıştır. Güvenirlilik Büyüköztürk ve diğerleri (2016) tarafından; ölçekten elde edilen puanların tesadüfi hatadan arındırılması ve aynı ölçme aracının farklı uygulamalarda benzer sonuçlar vermesi olarak tanımlanmıştır. Ölçeğin uygulanması esnasında tesadüfi hatanın en aza indirilmesi adına ölçeğin gönüllülük esasına göre doldurulması gerektiği vurgulanmıştır. Kendini yorgun veya hazır hissetmeyenlerden ölçeği doldurmaması istenmiştir. Ölçeğin uygulandığı ortamın fiziki şartlarının da veri toplamaya uygun olduğundan emin olunmuştur. Verilerin analizi yapılırken hangi analizlerin yapılması gerektiği konusunda alan yazın taraması yapılmış, uzman görüşü alınmıştır. Ayrıca verilerin normal dağılıp dağılmadığı tespit edilmiş, varyansların homojen olup olmadığı test edilmiştir.

4.BULGULAR

Bu bölümde öğretmen adaylarının Siber Bilgi Güvenliği Farkındalıkları, Dijital Vatandaşlık Düzeyleri ve Dijital Vatandaşlık Alt Boyutlarının; cinsiyet, bölüm, sınıf kademesi, günlük teknoloji kullanım oranı, günlük sosyal medya kullanım oranı gibi değişkenlere göre analizleri gerçekleştirilmiştir. “Öğretmen adaylarının SBGF ve DV düzeyleri cinsiyete göre farklılaşıyor mu?” sorusunu cevaplamak adına t- testi yapılmıştır. “Öğretmen adaylarının SBGF ve DV düzeylerinin; bölüm, Sınıf düzeyi, GTK, GSK sürelerine göre farklılaşıyor mu ?” sorusunu cevaplamak için ise ANOVA testi yapılmıştır. Hangi bölümler arasında fark olduğunu tespit için de Post Hoc analizlerinden yararlanılmıştır.

Analizlere devam edilmeden önce normallik ve homojenlik dağılımları test edilmiş varsayımların sağlandığı görülmüştür. Homojenlik test edilirken siber bilgi güvenliği farkındalığı ve bölümler arası levenenin anlamlı olduğu görülmüştür. Fakat Field (2013); levene anlamlı çıksa da karşılaştırılan değişkenlere ait en büyük standart sapmanın en küçük standart sapmaya oranının 4 veya altında çıkması durumunda varsayımın sağlanmadığı durumunun göz ardı edilebileceğini belirtmiştir. Yapmış olduğumuz hesaplamada bu oranın 1.58 olduğu görülmüş, varsayımın sağlandığı kabul edilmiştir.

4.1. Öğretmen Adaylarının Siber Bilgi Güvenliği Farkındalığı ve Dijital Vatandaşlık Düzeyleri

Tablo 4.1
Öğretmen Adaylarının Siber Bilgi Güvenliği Farkındalığı ve Dijital Vatandaşlık Düzeylerinin Ortalama, Standart Sapma Değerleri

Ölçek	N	SD	M
Siber Bilgi Güvenliği Farkındalığı	1155	,640	3,704
Dijital Vatandaşlık Düzeyi	1155	,482	3,717

Tablo 4.1' de yer alan veriler incelendiğinde öğretmen adaylarının siber bilgi güvenliği ortalaması(M=3.70) ve dijital vatandaşlık ortalamasının(M=3.71) birbirine çok yakın olduğu görülmektedir.

4.1.1. Öğretmen Adaylarının Siber Bilgi Güvenliği Farkındalıklarının ve Dijital Vatandaşlık Düzeylerinin Cinsiyete Göre İncelenmesi

Tablo 4.2.

Siber Bilgi Güvenliği Farkındalığı ve Dijital Vatandaşlık Seviyesinin Cinsiyete Göre Karşılaştırılması

Bağımlı Değişken	Grup	N	M	SD	t	df	p	Ortalamalar Farkı
Siber Bilgi Güvenliği Farkındalığı	Kadın	809	3.6627	.63422	-3.369	1153	.001	-.13797
	Erkek	346	3.8007	.64524				
Dijital Vatandaşlık	Kadın	809	3.7052	.47753	-1.288	1153	.198	-.03989
	Erkek	346	3.7451	.49222				

Tablo 4,2'de kadın ve erkeklerin siber bilgi güvenliği farkındalığı ölçeği ve dijital vatandaşlık ölçeğinden aldıkları puanlarını karşılaştırmak için bağımsız örneklem t testi sonuçları verilmiştir. Öğretmen adaylarına uygulanan SBGF ölçeği sonucuna göre kadınların ($M = 3.66$, $SD = .63$) ve erkeklerin ($M = 3.80$, $SD = .65$) **siber bilgi güvenliği farkındalığı** puanları arasında istatistiksel olarak anlamlı bir fark bulunmuştur ($t(1153) = -3,369$, $p < .05$, $Cohen's d = .02$). Bu sonuçlara göre erkeklerin siber bilgi güvenliği farkındalığının kadınlardan daha yüksek olduğunu söylemek mümkündür. Öğretmen adaylarının **dijital vatandaşlık** seviyelerinin cinsiyete göre farklılaşıp farklılaşmadığını tespit etmek için gerçekleştirilen t testi sonuçlarına göre kadınların ($M = 3.70$, $SD = .47$) ve erkeklerin ($M = 3.74$, $SD = .49$) puanları arasında istatistiksel olarak anlamlı bir fark bulunamamıştır ($p > .05$). Bu sonuç ise cinsiyetin dijital vatandaşlık üzerinde etkisi yoktur şeklinde yorumlanabilir.

4.1.2. Öğretmen Adaylarının Dijital Vatandaşlık Alt Boyutlarının Cinsiyet Değişkenine Göre İncelenmesi

Tablo 4.3'te öğretmen adaylarının cinsiyetlerine göre Dijital vatandaşlığın 9 alt boyutu olan; Dijital Okuryazarlık, Dijital Yasa, Dijital Hak Sorumluluk, Dijital İletişim, Dijital Güvenlik, Dijital Ticaret, Dijital Erişim, Dijital Etik, Dijital Sağlık durumlarına yönelik istatistiksel sonuçları verilmiştir.

Tablo 4.3

Dijital Vatandaşlığın 9 alt boyutunun cinsiyete göre karşılaştırılması

Bağımlı Değişken	Grup	N	M	SD	t	df	p	Ortalamalar Farkı
Dijital Okuryazarlık	Kadın	809	3.3937	.74408	-5.127	1153	.000	-.24503
	Erkek	346	3.6387	.74386				
Dijital Yasa	Kadın	809	4.2580	.81005	3.730	1153	.000	.19156
	Erkek	346	4.0665	.77431				
Dijital Hak Sorumluluk	Kadın	809	3.9886	.72479	1.235	1153	.217	.05793
	Erkek	346	3.9306	.74325				
Dijital İletişim	Kadın	809	3.7719	.81536	-.310	1153	.757	-.01635
	Erkek	346	3.7883	.83589				
Dijital Güvenlik	Kadın	809	3.4021	.79832	-1.936	1153	.053	-.09978
	Erkek	346	3.5019	.81145				
Dijital Ticaret	Kadın	809	3.6362	1.00803	-.893	1153	.372	-.05747
	Erkek	346	3.6936	.98781				
Dijital Erişim	Kadın	809	3.7808	.79983	-4.670	1153	.000	-.24521
	Erkek	346	4.0260	.85708				
Dijital Etik	Kadın	809	3.9827	.74608	2.917	1153	.004	.13780
	Erkek	346	3.8449	.71019				
Dijital Sağlık	Kadın	809	3.1438	.88148	.088	1153	.930	.00507
	Erkek	346	3.1387	.92836				

Tablo 4.3'teki veriler incelendiğinde; edilen ortalamalar 3.13 ile 4.26 arasında değişmektedir. Erkeklerde ($M=4.066$) ve kadınlarda ($M=4.258$) en yüksek ortama dijital yasa değişkeninde olduğu görülmüştür. Hem kadınların hem de erkeklerin ortalamalarının aynı değişkende en yüksek ortalamaya sahip olması bu değişkende farkındalıklarının yüksek olduğunu göstermektedir.

Yapılan t testin sonucunda; kadınların ($M = 3.39$, $SD = .74$) ve erkeklerin ($M = 3.63$, $SD = .74$) **dijital okuryazarlık** puanları arasında erkeklerin lehine olacak şekilde istatistiksel olarak anlamlı bir fark olduğu görülmüştür ($t(1153) = -5.128$, $p < .05$, $Cohen's d = .32$). Ortalamalara bakılarak erkeklerin dijital okuryazarlık seviyelerinin kadınlardan daha fazla olduğu söylenebilir. Yine bir başka alt boyut olan **dijital yasa** düzeyi puanlarını kıyaslamak için t testi yapılmış, sonuç olarak kadınların ($M = 4.25$, $SD = .81$) ve erkeklerin ($M = 4.06$, $SD = .77$) puanları arasında anlamlı bir fark bulunmuştur ($t(1153) = 3.730$, $p < .05$, $Cohen's d = .24$). Bu farka göre, kadınların dijital yasa boyutundaki farkındalık seviyelerinin erkeklerinkinden daha yüksek olduğunu söylemek mümkündür.

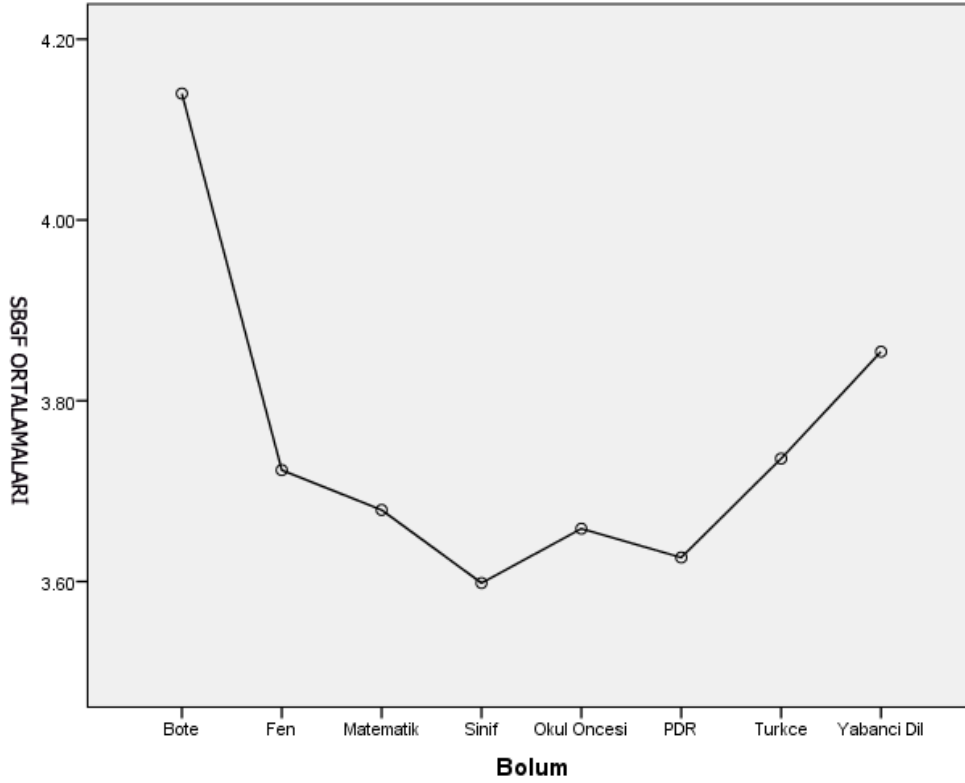
Kadınlar ve erkeklerin **dijital erişim** düzeyi puanlarını kıyaslamak adına t testi yapılmış, sonuç olarak kadınların ($M = 3,78$, $SD = .79$ ve erkeklerin ($M = 4,02$, $SD = .85$) dijital erişim puanları istatistiksel olarak anlamlı bir fark olduğu görülmüştür. ($t_{(1153)} = 3,7808$, $p < .05$). Bu sonucun erkeklerin lehine olduğunu söylemek mümkündür. Bu sonuca benzer kadınlar ve erkeklerin **dijital etik** düzeyi puanlarını kıyaslamak için yapılan testin sonuçları da göstermektedir ki kadınların ($M = 3,98$, $SD = .74$ ve erkeklerin ($M = 3,84$, $SD = .71$) puanları arasında kadınların lehine olacak şekilde istatistiksel olarak anlamlı bir fark vardır. ($t_{(1153)} = 3,8449$, $p < .05$).

Öğretmen adaylarının **dijital hak ve sorumluluk** düzeyi puanlarını cinsiyete göre karşılaştırdığımız ölçek sonucuna göre kadınların ($M = 3,98$, $SD = .72$) ve erkeklerin ($M = 3,93$, $SD = .74$) puanlarının istatistiksel olarak farklılaşmadığı tespit edilememiştir. ($p > .05$). Kadınlar ve erkeklerin **dijital iletişim** düzeyi puanlarını karşılaştırmak adına yapılan t testinde kadınların ($M = 3,77$, $SD = .81$) ve erkeklerin ($M = 3,78$, $SD = .83$) puanları arasında istatistiksel olarak anlamlı bir fark bulunamamıştır. ($p > .05$). Cinsiyete göre **dijital güvenlik** düzeyi puanlarını kıyaslamak için yapılan testi sonuçları göstermektedir ki; kadınların ($M = 3,40$, $SD = .79$) ve erkeklerin ($M = 3,50$, $SD = .81$) puanları arasında istatistiksel olarak anlamlı bir fark yoktur. ($p > .05$). Cinsiyete göre **dijital ticaret** düzeyi puanları karşılaştırıldığında kadın ($M = 3,63$, $SD = 1,00$ ve erkekler ($M = 3,69$, $SD = .98$) arasında istatistiksel olarak anlamlı bir fark olmadığı görülmüştür. ($p > .05$). Aynı şekilde kadınlar ve erkeklerin **dijital sağlık** düzeyi puanlarını kıyaslamak için yapılan testin sonucuna göre kadınların ($M = 3,14$, $SD = .88$ ve erkeklerin ($M = 3,13$, $SD = .92$) puanları arasında istatistiksel olarak anlamlı bir fark bulunamamıştır ($p > .05$).

4.2. Bağımlı Değişkenlerin Bölümlere Göre Karşılaştırılması Tek yönlü Varyans analizi

4.2.1. Siber Bilgi Güvenliği Farkındalığı Değişkeninin Bölümlere göre karşılaştırılması

Şekil 4.1' deki Siber Bilgi Güvenliği Farkındalığının bölümlere göre ortalamalarını gösteren grafiğe bakıldığında en yüksek ortalamanın BÖTE bölümünde olduğu görülürken, Fen, Matematik, Sınıf, Okul öncesi, PDR ve Türkçe bölümlerinin ortalamalarının birbirine yakın olduğu görülmektedir. BÖTE' den sonra en yüksek ortalamaya sahip olan bölümün İngilizce öğretmenliği olduğu görülürken, bölümler arasında en düşük ortalama da sınıf öğretmenliğine aittir.



Şekil 4.1. Bölümlere Göre Siber Bilgi Güvenliği Farkındalık Ortalamalarının Grafiği

Tablo 4.4

Siber Bilgi Güvenliği Farkındalığının Bölümlere göre kişi sayısı, ortalama ve standart sapmaları

Bağımlı Değişken	Bölüm(J)	N	M	Standart Sapma
Siber Güvenlik Farkındalığı	BÖTE	42	4.1399	.44991
	Fen	174	3.7232	.57305
	Matematik	150	3.6792	.58641
	Sınıf	176	3.5984	.61736
	Okul Öncesi	158	3.6584	.65721
	PDR	196	3.6266	.63338
	Türkçe	134	3.7360	.71458
	Yabancı Dil	125	3.8543	.70539
	Toplam	1155	3.7040	.64039

Tablo 4.4'te de bölümlere göre öğretmen adayları sayıları, bölümlerin siber bilgi güvenliği farkındalığı ölçeğinden aldığı ortalama puanlar ve bölümlerin standart sapmalarına yer verilmiştir. Bölümlerin ortalama puanları incelendiğinde en yüksek ortalamaya sahip bölümün BÖTE(N=42, M=4.1399), en düşük ortalamaya sahip bölümün ise sınıf öğretmenliği(N=176, M=3.5984) olduğu görülmüştür.

Tablo 4.5
Siber Bilgi Güvenliği Farkındalığının Bölümlere Karşılaştırılması

	Varyans Kaynağı	Kareler Toplamı	sd	Kareler Ortalaması	F	p	Eta Kare
SBGF	Gruplar Arası	14.562	7	2.080	5.202	.000*	.031
	Gruplar İçi	458.697	1147	.400			
	Toplam	473.260	1154				

(*p<.05 BÖTE=1, Fen=2, Matematik=3, Sınıf=4, Okul Öncesi=5, PDR=6, Türkçe=7, Yabancı Dil=8)

Öğretmen adaylarının öğrenim gördükleri bölümlerin siber bilgi güvenliği farkındalığı etkisini görme amacıyla tek faktörlü varyans analizi yürütülmüş, analiz sonucunda ulaşılan sonuçlar Tablo 4.5 'te sunulmuş ve bölümler arasında anlamlı bir fark bulunmuştur ($F(7,1147) = 5.202, p < .05, \eta^2 = .031$). Gruplar arasındaki farklılıkların büyüklüğü hakkında bilgi vermesi amacı ile etki büyüklüğü hesaplanmış, küçük düzeyde bir etki büyüklüğü tespit edilmiştir. Cohen (1988)' e göre etki büyüklüğü .01 küçük etki, .06 orta düzey etki, .14 büyük etki olarak hesaplamıştır. Anova sonucu tespit edilen farklılaşmaların hangi bölümler arasında olduğunu gösteren Post-Hoc sonuçları ise Tablo 4.6'dan Tablo 4.13'e kadar verilmiştir.

Tablo 4.6
BÖTE bölümünün diğer bölümlere göre Siber Bilgi Güvenliği Farkındalığı farkı- Post Hoc

Bağımlı Değişken	(I)Bölüm	(J)Bölüm	Ortalamaların Farkı	p
Siber Güvenlik Farkındalığı	BÖTE	Fen	.41664*	.003*
		Matematik	.46071*	.001*
		Sınıf	.54151*	.000*
		Okul Öncesi	.48146*	.000*
		PDR	.51329*	.000*
		Türkçe	.40387*	.008*
		Yabancı Dil	.28563	.183

Bölümler arası farkları detaylı incelemek amacıyla yürütülen Post-Hoc analiz sonuçlarına göre; **BÖTE** (M = 4.14, SD = .45) ile Fen Bilgisi(M = 3.72, SD = .57), Matematik(M = 3.68, SD = .59), Sınıf(M = 3.60, SD = .62), Okul Öncesi(M = 3.66, SD = .66), PDR(M = 3.63, SD = .63) ve Türkçe öğretmenliği(M = 3.74, SD = .71) bölümleri öğretmen adayları puanları arasında anlamlı bir farka işaret ederken, **BÖTE** ile Yabancı Dil(M = 3.85, SD = .70) öğretmen adayları puanları arasında ise anlamlı bir fark tespit edilememiştir. BÖTE öğretmen adaylarının SBGF Yabancı Dil Öğretmenliği bölümü öğretmen adayları haricinde diğer bölümlerde okuyan öğretmen adaylarından yüksek olduğu belirlenmiştir.

Tablo 4.7

Fen Bilgisi Öğretmenliği bölümünün diğer bölümlere göre Siber Bilgi Güvenliği Farkındalığı farkı-Post Hoc

Bağımlı Değişken	(I)Bölüm	(J)Bölüm	Ortalamaların Farkı	p
Siber Güvenlik Farkındalığı	Fen	BÖTE	-.41664*	.003*
		Matematik	.04407	.999
		Sınıf	.12487	.588
		Okul Öncesi	.06481	.983
		PDR	.09665	.825
		Türkçe	-.01277	1.000
		Yabancı Dil	-.13101	.643

Tablo 4.7 incelendiğinde; **Fen Bilgisi**(M =3.72, SD =.57), ile BÖTE (M =4.13 , SD =.44)bölümü öğretmen adayları puanları arasında anlamlı bir fark olduğu tespit edilmişken, **Fen** ile Matematik(M =3.67 , SD =.58), Sınıf(M =3.59 , SD =.61), Okul Öncesi(M = 3.65, SD =.65), PDR(M =3.62 , SD =.63) ve Türkçe(M =3.73 , SD =.71), Yabancı Dil(M =3.85 , SD =.70) öğretmen adayları puanları arasında anlamlı bir fark tespit edilememiştir.

Tablo 4.8

Matematik öğretmenliği bölümünün diğer bölümlere göre Siber Bilgi Güvenliği Farkındalığı farkı-Post Hoc

Bağımlı Değişken	(I)Bölüm	(J)Bölüm	Ortalamaların Farkı	p
Siber Güvenlik Farkındalığı	Matematik	BÖTE	-.46071*	.001*
		Fen	-.04407	.999
		Sınıf	.08080	.945
		Okul Öncesi	.02074	1.000
		PDR	.05257	.995
		Türkçe	-.05684	.995
		Yabancı Dil	-.17508	.302

Tablo 4.8'deki veriler incelendiğinde **Matematik** (M =3.67, SD =.58) ile BÖTE(M =4.13 , SD =.44) bölümü öğretmen adayları puanları arasında anlamlı bir fark varken, **Matematik** ile Fen(M =3.72 , SD =.57), Sınıf(M =3.59 , SD =.61), Okul Öncesi(M =3.65 , SD =.65), PDR(M =3.62 , SD =.63) ve Türkçe(M =3.73 , SD =.71), Yabancı Dil(M =3.85 , SD =.70) öğretmen adayları puanları arasında anlamlı bir fark yoktur.

Tablo 4.9

Sınıf öğretmenliği bölümünün diğer bölümlere göre Siber Bilgi Güvenliği Farkındalığı farkı- Post Hoc

Bağımlı Değişken	(I)Bölüm	(J)Bölüm	Ortalamaların Farkı	p
Siber Güvenlik Farkındalığı	Sınıf	Böte	-.54151*	.000*
		Fen	-.12487	.588
		Matematik	-.08080	.945
		Okul Öncesi	-.06006	.989
		PDR	-.02823	1.000
		Türkçe	-.13764	.552
		Yabancı Dil	-.25588*	.013*

Tablo 4.9'daki farklılaşmalara göre **Sınıf**(M =3.59, SD =.61) ile BÖTE(M =4.13, SD =.44), Yabancı Dil(M =3.85, SD =.70), bölümü öğretmen adayları puanları arasında istatistiksel olarak anlamlı bir fark olduğu dikkat çekerken, **Sınıf** ile Okul Öncesi(M =3.65, SD =.65), Fen Bilgisi(M =3.72, SD =.57), PDR(M =3.62, SD =.63), Matematik(M =3.67, SD =.58), ve Türkçe(M =3.73, SD =.71) öğretmenliği bölümü öğretmen adayları puanları arasında anlamlı bir farka ulaşamamıştır. Diğer ifade ile sınıf öğretmenliği bölümü öğretmen adaylarının siber bilgi güvenliği farkındalıkları BÖTE ve Yabancı dil bölümü öğretmen adaylarından daha düşüktür.

Tablo 4.10

Okul öncesi öğretmenliği bölümün diğer bölümlere göre Siber Bilgi Güvenliği Farkındalığı farkı- Post Hoc

Bağımlı Değişken	(I)Bölüm	(J)Bölüm	Ortalamaların Farkı	p
Siber Güvenlik Farkındalığı	Okul Öncesi	Böte	-.48146*	.000*
		Fen	-.06481	.983
		Matematik	-.02074	1.000
		Sınıf	.06006	.989
		PDR	.03183	1.000
		Türkçe	-.07758	.967
		Yabancı Dil	-.19582	.162

Tablo 4.10'a göre **Okul Öncesi**(M =3.65, SD =.65) ile BÖTE(M =4.13, SD =.44) bölümü öğretmen adayları puanları arasında anlamlı bir fark vardır. Fakat **Okul Öncesi** ile Matematik(M =3.67, SD =.58), Fen(M =3.72, SD =.57), Sınıf(M =3.59, SD =.61), PDR(M =3.62, SD =.63) ve Türkçe(M =3.73, SD =.71), Yabancı Dil(M =3.85, SD =.70) öğretmen adayları puanları arasında anlamlı bir fark yoktur.

Tablo 4.11

PDR bölümünün diğer bölümlere göre Siber Bilgi Güvenliği Farkındalığı farkı- Post Hoc

Bağımlı Değişken	(I)Bölüm	(J)Bölüm	Ortalamaların Farkı	p
Siber Güvenlik Farkındalığı	PDR	Böte	-.51329*	.000*
		Fen	-.09665	.825
		Matematik	-.05257	.995
		Sınıf	.02823	1.000
		Okul Öncesi	-.03183	1.000
		Türkçe	-.10941	.784
		Yabancı Dil	-.22766*	.036*

Tablo 4.11'deki post Hoc verileri incelendiğinde **PDR** bölümü (M =3.62, SD =.63) ile BÖTE(M =4.13, SD =.44), Yabancı Dil(M =3.85, SD =.70), bölümü öğretmen adayları puanları arasında anlamlı bir farka işaret ederken, **PDR** ile Fen Bilgisi(M =.72, SD =.57), Okul Öncesi(M =3.65, SD =.65), Matematik(M =3.67, SD =.58), ve Türkçe(M =3.73, SD =.71), Sınıf öğretmeni(M =3.59, SD =.61) adayları puanları arasında anlamlı farkın olmadığı gözlenmiştir. Sonuç olarak, PDR bölümü öğretmen adaylarının siber bilgi güvenliği farkındalıkları BÖTE ve Yabancı Dil öğretmenliği öğretmen adaylarından daha düşüktür.

Tablo 4.12

Türkçe Öğretmenliği bölümünün diğer bölümlere göre Siber Bilgi Güvenliği Farkındalığı farkı- Post Hoc

Bağımlı Değişken	(I)Bölüm	(J)Bölüm	Ortalamaların Farkı	p
Siber Güvenlik Farkındalığı	Türkçe	Böte	-.40387*	.008
		Fen	.01277	1.000
		Matematik	.05684	.995
		Sınıf	.13764	.552
		Okul Öncesi	.07758	.967
		PDR	.10941	.784
		Yabancı Dil	-.11824	.806

Tablo 4.12'deki verilerde de görüldüğü gibi **Türkçe**(M =3.73, SD =.71) ile BÖTE(M =4.13, SD =.44), bölümü öğretmen adayları puanları arasında anlamlı bir fark vardır. Buna karşın **Türkçe** ile Matematik(M =3.67, SD =.58), Fen Bilgisi(M =.72, SD =.57), Sınıf öğretmeni(M =3.59, SD =.61), **PDR** (M =3.62, SD =.63), Okul Öncesi(M =3.65, SD =.65),Yabancı Dil Öğretmenliği(M =3.85, SD =.70) bölümü öğretmen adayları puanları arasında anlamlı bir fark olmadığı tespit edilmiştir.

Tablo 4.13

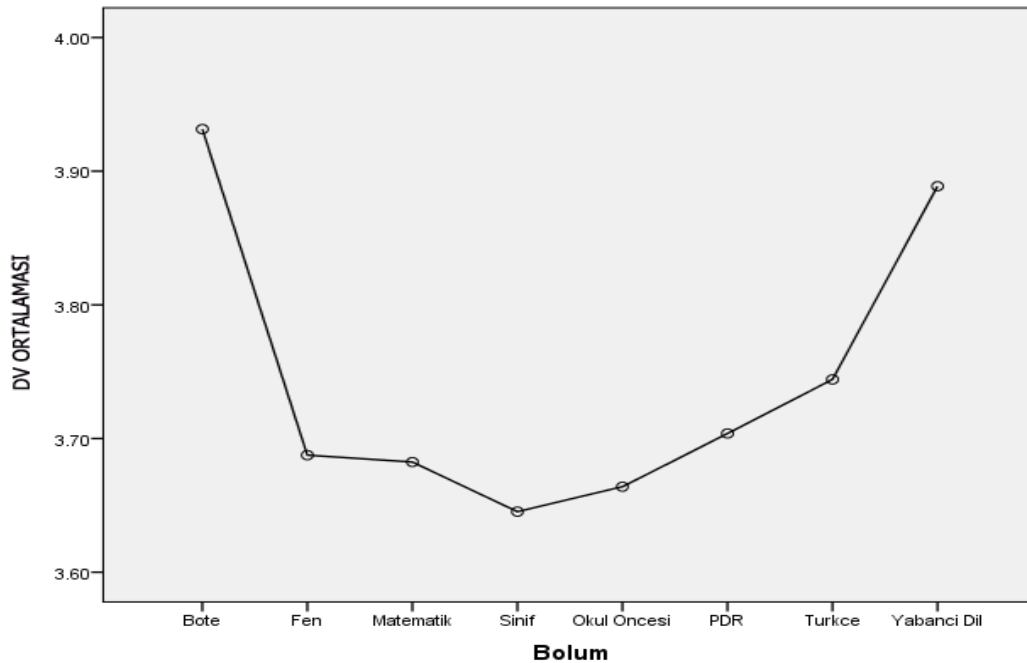
Yabancı Dil Öğretmenliği bölümün diğer bölümlere göre Siber Bilgi Güvenliği Farkındalığı farkı-Post Hoc

Bağımlı Değişken	(I)Bölüm	(J)Bölüm	Ortalamaların Farkı	p
Siber Güvenlik Farkındalığı	Yabancı Dil	Böte	-.28563	.183
		Fen	.13101	.643
		Matematik	.17508	.302
		Sınıf	.25588*	.013*
		Okul Öncesi	.19582	.162
		PDR	.22766*	.036*
		Türkçe	.11824	.806

Tablo 4.13'deki verilerden yola çıkarak **Yabancı Dil**(M =3.85, SD =.70) ile sınıf öğretmeni(M =3.59, SD =.61), PDR (M =3.62, SD =.63) bölümü öğretmen adayları puanları arasında anlamlı bir fark olduğu görülmüştür. Fakat **Yabancı Dil** ile BÖTE(M =4.13, SD =.44), Fen(M =.72, SD =.57), Okul Öncesi(M =3.65, SD =.65), Matematik(M =3.67, SD =.58), ve Türkçe(M =3.73, SD =.71), öğretmen adayları puanları arasında anlamlı bir fark olduğu söylenemez.

4.2.2. Dijital Vatandaşlık Düzeyinin Bölümlere Göre Karşılaştırılması

Şekil 4.2' de öğretmen adaylarının dijital vatandaşlık düzeylerinin bölümlere göre ortalamaları gösterilmiştir. Grafik incelendiğinde en yüksek ortalamaya sahip bölümlerin BÖTE ve İngilizce olduğu görülmektedir.



Şekil 4.2. Bölümlere Göre Dijital Vatandaşlık Düzeyi Ortalamalarının Grafiği

Tablo 4.14

Dijital Vatandaşlık Düzeylerinin bölümlere göre kişi sayısı, ortalama ve standart sapmaları.

Bağımlı Değişken	Bölüm(J)	N	Mean	Std. Deviation
Dijital Vatandaşlık	BÖTE	42	3.9315	.42186
	Fen	174	3.6876	.44811
	Matematik	150	3.6824	.45416
	Sınıf	176	3.6453	.48575
	Okul Öncesi	158	3.6640	.51146
	PDR	196	3.7038	.43941
	Türkçe	134	3.7442	.51117
	Yabancı Dil	125	3.8887	.51794
	Toplam	1155	3.7172	.48211

Tablo 4.14' te bölümlerde yer alan öğretmen sayıları, bölümlerin dijital vatandaşlık ölçeğinden aldığı ortalamalar ve standart sapma değerleri görülmektedir. Dijital vatandaşlık ölçeği ortalamalarına bakıldığında en yüksek ortalamanın BÖTE bölümüne ait olduğu görülmektedir(N=42, M=3.9315). Yine en düşük ortalamanın ise Sınıf öğretmenliğinde olduğu görülmektedir. (N=176, M=3.6453). Dikkat edildiğinde bu sonucun siber bilgi güvenliği farkındalığı ile paralel olduğu göze çarpmaktadır.

Tablo 4.15

Dijital Vatandaşlık Düzeylerinin bölümlere göre karşılaştırılması

	Varyans Kaynağı	Kareler Toplamı	sd	Kareler Ortalaması	F	p	Eta Kare
Dijital Vatandaşlık	Gruplar Arası	7.430	7	1.061	4.668	.000*	.028
	Gruplar İçi	260.798	1147	.227			
	Toplam	268.228	1154				

(*p<.05 BÖTE=1, Fen=2, Matematik=3, Sınıf=4, Okul Öncesi=5, PDR=6, Türkçe=7, Yabancı Dil=8)

Tablo 4.15'te öğretmen adaylarının öğrenime devam ettikleri bölümlerin dijital vatandaşlık düzeyleri olan etkisini tespit etmek için gerçekleştirilen tek yönlü varyans analizi sonuçları yer almaktadır. Bu sonuçlara göre öğretmen adaylarının öğrenime devam ettikleri bölümler ile dijital vatandaşlık seviyeleri arasında anlamlı bir fark tespit edilmiştir($F(7,1147) = 4.668, p < .05, \eta^2 = .028$). Bu ilişkinin hangi bölümler arasında olduğunu tespit etmek amacı ile Post Hoc testi yürütülmüş, sonuçlar Tablo 4.3.13' ten Tablo 4.3.20' ye kadar verilmiştir.

Tablo 4.16

BÖTE bölümünün diğer bölümlere göre Dijital Vatandaşlık Düzeyi farkı- Post Hoc

Bağımlı Değişken	(I) Bölüm	(J)Bölüm	Ortalamaların Farkı	p
Dijital Vatandaşlık	BÖTE	Fen	.24389	.060
		Matematik	.24903	.057
		Sınıf	.28614*	.012*
		Okul Öncesi	.26748*	.028*
		PDR	.22769	.094
		Türkçe	.18722	.340
		Yabancı Dil	.04273	1.000

Tablo 4.16'da **BÖTE** (M =3.93, SD =.42) ile Sınıf (M =3.64, SD =.48) ve Okul Öncesi (M =3.66, SD =.51) öğretmenliği bölümlerinde öğrenim gören öğretmen adaylarının puanları arasında anlamlı bir fark tespit edilmiştir ve bu fark BÖTE bölümü lehinedir. Buna karşılık **BÖTE** ile Matematik (M =3.68, SD =.45), Fen Bilgisi (M =3.68, SD =.44), PDR (M =3.70, SD =.43) ve Yabancı Dil (M =3.88, SD =.51) ve Türkçe (M =3.74, SD =.51) öğretmenliği bölümlerinde öğrenimlerine devam etmekte olan öğretmen adayları puanları incelendiğinde anlamlı farka ulaşılamamıştır.

Tablo 4.17

Fen Bilgisi Öğretmenliği bölümünün diğer bölümlere göre Dijital Vatandaşlık Düzeyi farkı- Post Hoc

Bağımlı Değişken	(I) Bölüm	(J)Bölüm	Ortalamaların Farkı	p
Dijital Vatandaşlık	Fen	Böte	-.24389	.060
		Matematik	.00514	1.000
		Sınıf	.04225	.991
		Okul Öncesi	.02358	1.000
		PDR	-.01621	1.000
		Türkçe	-.05667	.969
		Yabancı Dil	-.20116*	.008*

Tablo 4.17'de **Fen Bilgisi** (M =3.68, SD =.44) ile Yabancı Dil (M =3.88, SD =.51) öğretmenliği bölümü öğretmen adayları puanları incelendiğinde, puanlar arasında anlamlı bir fark olduğu görülmüştür. Fakat **Fen Bilgisi** ile BÖTE (M =3.93, SD =.42), Matematik (M =3.68, SD =.45), PDR (M =3.70, SD =.43) Sınıf (M =3.64, SD =.48), Türkçe (M =3.74, SD =.51) ve Okul Öncesi (M =3.66, SD =.51) öğretmenliği bölümü öğretmen adayları puanları arasında anlamlı bir fark tespit edilememiştir. En büyük farklılaşmanın ise Fen Bilgisi ile Yabancı Dil öğretmenliği bölümleri arasında olduğu görülmüştür.

Tablo 4.18

Matematik Öğretmenliği bölümünün diğer bölümlere göre Dijital Vatandaşlık Düzeyi farkı - Post Hoc

Bağımlı Değişken	(I) Bölüm	(J) Bölüm	Ortalamaların Farkı	p
Dijital Vatandaşlık	Matematik	Böte	-.24903	.057
		Fen	-.00514	1.000
		Sınıf	.03711	.997
		Okul Öncesi	.01844	1.000
		PDR	-.02135	1.000
		Türkçe	-.06181	.959
		Yabancı Dil	-.20630*	.009*

Tablo 4.18'de **Matematik**(M =3.68, SD =.45) ile **Yabancı Dil**(M =3.88, SD =.51) bölümü öğretmen adayları puanları incelendiğinde aralarında anlamlı bir fark olduğu görülmektedir. Buna karşılık **Matematik ile** BÖTE(M =3.93, SD =.42), PDR (M =3.70, SD =.43), Sınıf(M =3.64, SD =.48), Türkçe(M =3.74, SD =.51), Okul Öncesi(M =3.66, SD =.51), Fen(M =3.68, SD =.44) öğretmen adayları dijital vatandaşlık puanları arasında anlamlı bir fark tespit edilememiştir.

Tablo 4.19

Okul Öncesi Öğretmenliği bölümünün diğer bölümlere göre Dijital Vatandaşlık Düzeyi farkı - Post Hoc

Bağımlı Değişken	(I) Bölüm	(J) Bölüm	Ortalamaların Farkı	p
Dijital Vatandaşlık	Okul Öncesi	Böte	-.26748*	.028*
		Fen	-.02358	1.000
		Matematik	-.01844	1.000
		Sınıf	.01866	1.000
		PDR	-.03979	.994
		Türkçe	-.08025	.842
		Yabancı Dil	-.22475*	.002*

Tablo 4.19'da **Okul Öncesi Öğretmenliği** (M =3.66, SD =.51) bölümü ile BÖTE (M =3.93, SD =.42) ve **Yabancı Dil Öğretmenliği** (M =3.88, SD =.51) bölümlerinde öğrenim gören öğretmen adayları arasında anlamlı bir fark tespit edilmiştir. Ama **Okul Öncesi** ile **Matematik** (M =3.68, SD =.45), **PDR** (M =3.70, SD =.43) **Türkçe** (M =3.74, SD =.51), **Sınıf** (M =3.64, SD =.48) ve **Fen Bilgisi** (M =3.68, SD =.44) öğretmen adaylarının ölçekten aldığı puanlar incelendiğinde anlamlı bir fark saptanamamıştır.

Tablo 4.20

Sınıf Öğretmenliği bölümünün diğer bölümlere göre Dijital Vatandaşlık Düzeyi farkı - Post Hoc

Bağımlı Değişken	(I) Bölüm	(J)Bölüm	Ortalamaların Farkı	p
Dijital Vatandaşlık	Sınıf	Böte	-.28614*	.012
		Fen	-.04225	.991
		Matematik	-.03711	.997
		Okul Öncesi	-.01866	1.000
		PDR	-.05846	.937
		Türkçe	-.09892	.614
		Yabancı Dil	-.24341*	.000

Tablo 4.20’de **Sınıf Öğretmenliği** (M =3.64, SD =.48) ile BÖTE (M =3.93, SD =.42) ve Yabancı Dil (M =3.88, SD =.51) öğretmenliği bölümleri öğretmen adayları puanları arasında anlamlı bir farka olduğu söylenebilir. Fakat **Sınıf** ile Matematik (M =3.68, SD =.45), PDR (M =3.70, SD =.43), Türkçe (M =3.74, SD =.51), Okul Öncesi (M =3.66, SD =.51) ve Fen Bilgisi (M =3.68, SD =.44) öğretmen adayları puanları arasında anlamlı bir fark söz konusu değildir.

Tablo 4.21

PDR bölümünün diğer bölümlere göre Dijital Vatandaşlık Düzeyi farkı- Post Hoc

Bağımlı Değişken	(I) Bölüm	(J)Bölüm	Ortalamaların Farkı	p
Dijital Vatandaşlık	PDR	Böte	-.22769	.094
		Fen	.01621	1.000
		Matematik	.02135	1.000
		Sınıf	.05846	.937
		Okul Öncesi	.03979	.994
		Türkçe	-.04046	.995
		Yabancı Dil	-.18495*	.017*

Tablo 4.21’de Öğretmen adaylarının okudukları bölümün dijital vatandaşlık seviyelerine etkisini tespit etmek amacı ile yürütülen Post Hoc testi sonucu **PDR** (M =3.70, SD =.43) ile Yabancı Dil (M =3.88, SD =.51) öğretmenliği bölümündeki öğretmen adayları puanları arasında anlamlı bir fark tespit edilmiştir. **PDR** ile BÖTE (M =3.93, SD =.42), Sınıf (M =3.64, SD =.48), Türkçe (M =3.74, SD =.51), Okul Öncesi (M =3.66, SD =.51), Fen Bilgisi (M =3.68, SD =.44) ve Matematik (M =3.68, SD =.45) öğretmenliği bölümleri öğretmen adayları puanları arasında anlamlı bir fark bulunamamıştır. Burada da yabancı dilin birçok bölümle de olduğu gibi en fazla farklılaşma gösteren bölüm olduğu görülmektedir.

Tablo 4.22

Türkçe Öğretmenliği bölümünün diğer bölümlere göre Dijital Vatandaşlık Düzeyi farkı - Post Hoc

Bağımlı Değişken	(I) Bölüm	(J) Bölüm	Ortalamaların Farkı	p
Dijital Vatandaşlık	Türkçe	Böte	-.18722	.340
		Fen	.05667	.969
		Matematik	.06181	.959
		Sınıf	.09892	.614
		Okul Öncesi	.08025	.842
		PDR	.04046	.995
		Yabancı Dil	-.14449	.225

Tablo 4.22'deki sonuçlar incelendiğinde **Türkçe** (M =3.64, SD =.48) ile BÖTE (M =3.93, SD =.42), Sınıf (M =3.74, SD =.51), Okul Öncesi (M =3.66, SD =.51), Fen Bilgisi (M =3.68, SD =.44), Matematik (M =3.68, SD =.45), Yabancı Dil (M =3.88, SD =.51) ve PDR (M =3.70, SD =.43) bölümlerindeki öğretmen adayları puanları arasında anlamlı bir farkın olmadığı görülmüştür. Bu sonuçlara göre Türkçe öğretmenliğinde öğrenim gören öğretmen adayları ile diğer bölümlerdeki öğretmen adaylarının Dijital Vatandaşlık Düzey puanları arasında anlamlı bir fark yoktur.

Tablo 4.23

Yabancı Dil Öğretmenliği bölümünün diğer bölümlere göre Dijital Vatandaşlık Düzeyi farkı - Post Hoc

Bağımlı Değişken	(I) Bölüm	(J) Bölüm	Ortalamaların Farkı	p
Dijital Vatandaşlık	Yabancı Dil	Böte	-.04273	1.000
		Fen	.20116*	.008*
		Matematik	.20630*	.009*
		Sınıf	.24341*	.000*
		Okul Öncesi	.22475*	.002*
		PDR	.18495*	.017*
		Türkçe	.14449	.225

Tablo 4.23 incelendiğinde, **Yabancı Dil** (M =3.88, SD =.51) ile Sınıf (M =3.64, SD =.48), Okul Öncesi (M =3.66, SD =.51), Fen Bilgisi (M =3.68, SD =.44), Matematik (M =3.68, SD =.45), PDR (M =3.70, SD =.43) bölümlerindeki öğretmen adayları puanları arasında anlamlı bir fark olduğu görülmüştür. **Yabancı Dil Öğretmenliği** bölümünde öğrenim gören öğretmen adayları ile sadece BÖTE (M =3.93, SD =.42) ve Türkçe (M =3.74, SD =.51) öğretmen adayları puanları arasında anlamlı bir fark tespit edilememiştir.

4.2.2.1. Dijital Okuryazarlık Düzeylerinin Bölümlere Göre Karşılaştırılması

Bu bölümde dijital okuryazarlık düzeyinin bölümlere göre karşılaştırılması yapılmış, anlamlı fark olup olmadığı tespit edilmeye çalışılmıştır.

Tablo 4.24

Dijital Okur Yazarlık Düzeylerinin; Bölümlere Göre Kişi Sayısı, Ortalama ve Standart Sapmaları

Bağımlı Değişken	Bölüm(J)	N	M	Standart Sapma
Dijital Okur Yazarlık	BÖTE	42	3.8651	.69086
	Fen	174	3.5287	.69182
	Matematik	150	3.4433	.73219
	Sınıf	176	3.2945	.74679
	Okul Öncesi	158	3.3882	.84198
	PDR	196	3.3427	.66242
	Türkçe	134	3.4963	.76019
	Yabancı Dil	125	3.7827	.75141
	Toplam	1155	3.4671	.75212

Tablo 4.24'te öğretmen adaylarının bölümlere göre sayıları, bölümlerin dijital okuryazarlık alt boyutundan aldığı ortalama puanlar ve bölümlerin standart sapmaları gösterilmiştir. Tablodaki veriler incelendiğinde bağımlı değişkene ait en yüksek ortalamaya sahip bölümün BÖTE olduğu görülmektedir. En düşük ortalamasının ise sınıf öğretmenliği bölümünde olduğu görülmektedir.

Tablo 4.25

Dijital Okur Yazarlık Alt Boyutunun Bölümlere Göre Karşılaştırılması

	Varyans Kaynağı	Kareler Toplamı	sd	Kareler Ortalaması	F	p	Eta Kare
Dijital Okur Yazarlık	Gruplar Arası	29.220	7	4.174	7.678	.000*	.045
	Gruplar İçi	623.585	1147	.544			
	Toplam	652.805	1154				

(* $p < .05$ BÖTE=1, Fen=2, Matematik=3, Sınıf=4, Okul Öncesi=5, PDR=6, Türkçe=7, Yabancı Dil=8)

Tablo 4.25'te öğretmen adaylarının öğrenim gördükleri bölümlerin dijital okuryazarlık düzeylerine etkisini tespit etmek amacıyla yürütülen tek faktörlü varyans analizi yer almaktadır. Elde edilen bulgulara göre bölümler arasında anlamlı bir fark olduğu görülmüştür ($F(7,1147) = 7.678, p < .05, n^2 = .045$). Tablodaki veriler kullanılarak hesaplanan etki büyüklüğün orta düzeyde olduğu görülmektedir. Ayrıca tespit edilen anlamlı farklılığın hangi bölümler arasında olduğunu görmek için yürütülen Post Hoc test sonuçları Tablo 4.26'dan Tablo 4.33'e kadar verilmiştir.

Tablo 4.26

BÖTE Bölümünün Diğer Bölümlere Göre Dijital Okur Yazarlık Düzeyi- Post Hoc

Bağımlı Değişken	(I)Bölüm	(J)Bölüm	Ortalamaların Farkı	p
Dijital Okuryazarlık	BÖTE	Fen	.33634	.138
		Matematik	.42175*	.024*
		Sınıf	.57057*	.000*
		Okul Öncesi	.47689*	.005*
		PDR	.52239*	.001*
		Türkçe	.36881	.089
		Yabancı Dil	.08241	.999

Tablo 4.26'da BÖTE bölümü öğretmen adayları dijital okuryazarlık düzeyinin hangi bölümler ile anlamlı farklılaştığını göstermek için yapılmış Post Hoc test sonuçlarını göstermektedir. Bu sonuçlara göre **BÖTE** (M=3,90, SD=.69) ile Matematik (M=3,44, SD=.73), Sınıf (M=3,23, SD=.75), Okul Öncesi (M=3,39, SD=.84) ve PDR (M=3,34, SD=.66) bölümleri öğretmen adayları puanları arasında anlamlı bir fark tespit edilmiştir. Fakat **BÖTE** ile Yabancı Dil (M=3,78, SD=.75), Fen Bilgisi (M=3,52, SD=.69) ve Türkçe (M=3,90, SD=.69) öğretmenliği bölümlerindeki öğretmen adayları puanları arasında anlamlı bir görülememiştir.

Tablo 4.27

Fen Bilgisi Öğretmenliği Bölümünün Diğer Bölümlere Göre Dijital Okur Yazarlık Düzeyi - Post Hoc

Bağımlı Değişken	(I)Bölüm	(J)Bölüm	Ortalamaların Farkı	p
Dijital Okuryazarlık	Fen	Böte	-.33634	.138
		Matematik	.08540	.968
		Sınıf	.23423	.060
		Okul Öncesi	.14055	.664
		PDR	.18605	.231
		Türkçe	.03247	1.000
		Yabancı Dil	-.25393	.066

Tablo 4.27'de 24'de yer alan post hoc tablosu incelendiğinde; **Fen Bilgisi** (M=3,90, SD=.69) ile BÖTE (M=3,90, SD=.69), Matematik (M=3,44, SD=.73), Sınıf (M=3,23, SD=.75), Okul Öncesi (M=3,39, SD=.84), PDR (M=3,34, SD=.66), Yabancı Dil (M=3,78, SD=.75) ve Türkçe (M=3,90, SD=.69) öğretmenliği bölümleri öğretmen adayları puanları arasında anlamlı fark tespit edilememiştir.

Tablo 4.28

Matematik Öğretmenliği Bölümünün Diğer Bölümlere Göre Dijital Okur Yazarlık Düzeyi - Post Hoc

Bağımlı Değişken	(I)Bölüm	(J)Bölüm	Ortalamaların Farkı	p
Dijital Okuryazarlık	Matematik	Böte	-.42175*	.024*
		Fen	-.08540	.968
		Sınıf	.14883	.609
		Okul Öncesi	.05515	.998
		PDR	.10065	.914
		Türkçe	-.05294	.999
		Yabancı Dil	-.33933*	.004*

Tablo 4.28' de yer alan veriler incelendiğinde; **Matematik** (M=3,44, SD=.73) ile BÖTE (M=3,90, SD=.69) ve Yabancı Dil (M=3,78, SD=.75) öğretmenliği bölümlerinde öğrenim gören öğretmen adaylarının dijital okuryazarlık puanları arasında anlamlı fark olduğu görülmüştür. Fakat **Matematik** ile Sınıf (M=3,23, SD=.75), Okul Öncesi (M=3,39, SD=.84), PDR (M=3,34, SD=.66), Fen Bilgisi (M=3,52, SD=.69) ve Türkçe (M=3,90, SD=.69) öğretmenliği öğretmen adayları puanları arasında anlamlı fark olmadığı görülmüştür. Yine aynı tablodaki veriler incelendiğinde en büyük anlamlı farkın matematik ile yabancı dil öğretmenliği bölümleri arasında olduğu görülmektedir.

Tablo 4.29

Sınıf Öğretmenliği Bölümünün Diğer Bölümlere Göre Dijital Okur Yazarlık Düzeyi- Post Hoc

Bağımlı Değişken	(I)Bölüm	(J)Bölüm	Ortalamaların Farkı	p
Dijital Okuryazarlık	Sınıf	Böte	-.57057*	.000*
		Fen	-.23423	.060
		Matematik	-.14883	.609
		Okul Öncesi	-.09368	.943
		PDR	-.04818	.998
		Türkçe	-.20176	.249
		Yabancı Dil	-.48816*	.000*

Tablo 4.29'da yer alan veriler incelendiğinde; **Sınıf** (M=3,23, SD=.75) ile BÖTE (M=3,90, SD=.69) ve Yabancı Dil (M=3,78, SD=.75) öğretmenliği bölümündeki öğretmen adaylarının dijital okuryazarlık puanları arasında anlamlı bir fark olduğu görülmüştür. Buna karşılık; **Sınıf** (M=3,23, SD=.75) ile Fen Bilgisi (M=3,90, SD=.69), Matematik (M=3,44, SD=.73), Okul Öncesi (M=3,39, SD=.84), PDR (M=3,34, SD=.66) ve Türkçe (M=3,90, SD=.69) öğretmenliği öğretmen adaylarının dijital okuryazarlık puanları arasında anlamlı bir fark olmadığı görülmüştür.

Tablo 4.30

Okul Öncesi Öğretmenliği Bölümünün Diğer Bölümlere Göre Dijital Okur Yazarlık Düzeyi - Post Hoc

Bağımlı Değişken	(I)Bölüm	(J)Bölüm	Ortalamaların Farkı	p
Dijital Okuryazarlık	Okul Öncesi	Böte	-.47689*	.005*
		Fen	-.14055	.664
		Matematik	-.05515	.998
		Sınıf	.09368	.943
		PDR	.04550	.999
		Türkçe	-.10808	.917
		Yabancı Dil	-.39448*	.000*

Tablo 4.30' da yer alan Post Hoc tablosu verilerine bakıldığında; **Okul Öncesi** (M=3,39, SD=.84) bölümündeki öğretmen adaylarının dijital okuryazarlık puanları ile Yabancı Dil (M=3,78, SD=.75) ve BÖTE (M=3,90, SD=.69) bölümlerindeki öğretmen adaylarının puanları arasında anlamlı fark olduğu görülmüştür. Fakat **Okul Öncesi** (M=3,39, SD=.84) ile Matematik (M=3,44, SD=.73), Sınıf (M=3,23, SD=.75), PDR (M=3,34, SD=.66), Türkçe (M=3,90, SD=.69) ve Fen Bilgisi (M=3,90, SD=.69) öğretmenliği bölümü öğretmen adayları puanları arasında anlamlı fark tespit edilememiştir.

Tablo 4.31

PDR Bölümünün Diğer Bölümlere Göre Dijital Okur Yazarlık Düzeyi- Post Hoc

Bağımlı Değişken	(I)Bölüm	(J)Bölüm	Ortalamaların Farkı	p
Dijital Okuryazarlık	PDR	Böte	-.52239*	.001
		Fen	-.18605	.231
		Matematik	-.10065	.914
		Sınıf	.04818	.998
		Okul Öncesi	-.04550	.999
		Türkçe	-.15358	.580
		Yabancı Dil	-.43998*	.000

Tablo 4.31'de ki sonuçlara bakıldığında; **PDR** (M=3,34, SD=.66) bölümündeki öğrenimine devam eden öğretmen adaylarının dijital okuryazarlık puanları ile Yabancı Dil Öğretmenliği (M=3,78, SD=.75) ve BÖTE (M=3,90, SD=.69) bölümlerindeki öğretmen adaylarının puanları arasında anlamlı fark tespit edilmiştir. Fakat **PDR** (M=3,34, SD=.66) ile Matematik (M=3,44, SD=.73), Sınıf (M=3,23, SD=.75), Okul Öncesi (M=3,39, SD=.84), Türkçe (M=3,90, SD=.69) ve Fen Bilgisi (M=3,90, SD=.69) öğretmen adaylarının dijital okuryazarlık puanları arasında anlamlı fark tespit edilememiştir. Yine birçok bölümde olduğu gibi en büyük anlamlı farkın ise yabancı dil öğretmenliği ile olduğu görülmektedir.

Tablo 4.32

Türkçe Öğretmenliği Bölümünün Diğer Bölümlere Göre Dijital Okur Yazarlık Düzeyi - Post Hoc

Bağımlı Değişken	(I)Bölüm	(J)Bölüm	Ortalamaların Farkı	p
Dijital Okuryazarlık	Türkçe	Böte	-.36881	.089
		Fen	-.03247	1.000
		Matematik	.05294	.999
		Sınıf	.20176	.249
		Okul Öncesi	.10808	.917
		PDR	.15358	.580
		Yabancı Dil	-.28640*	.039

Tablo 4.32’de **Türkçe** (M=3,90, SD=.69) bölümü öğretmen adaylarının puanları ile Yabancı Dil Öğretmenliği (M=3,78, SD=.75) bölümlerindeki öğretmen adaylarının puanları arasında anlamlı fark tespit edilmiştir. Fakat **Türkçe** (M=3,90, SD=.69) ile BÖTE (M=3,90, SD=.69), PDR (M=3,34, SD=.66), Matematik (M=3,44, SD=.73), Sınıf (M=3,23, SD=.75), Okul Öncesi (M=3,39, SD=.84) ve Fen Bilgisi (M=3,90, SD=.69) öğretmenliği bölümlerindeki öğretmen adayları puanları arasında anlamlı fark tespit edilememiştir.

Tablo 4.33

Yabancı Dil bölümünün Diğer Bölümlere Göre Dijital Okur Yazarlık Düzeyi- Post Hoc

Bağımlı Değişken	(I)Bölüm	(J)Bölüm	Ortalamaların Farkı	p
Dijital Okuryazarlık	Yabancı Dil	Böte	-.08241	.999
		Fen	.25393	.066
		Matematik	.33933*	.004*
		Sınıf	.48816*	.000*
		Okul Öncesi	.39448*	.000*
		PDR	.43998*	.000*
		Türkçe	.28640*	.039*

Tablo 4.33’deki Post Hoc tablosuna göre **Yabancı Dil** (M=3,78, SD=.75) ile PDR (M=3,34, SD=.66), Matematik (M=3,44, SD=.73), Sınıf (M=3,23, SD=.75), Okul Öncesi (M=3,39, SD=.84) ve Türkçe (M=3,90, SD=.69) öğretmenliği bölümlerindeki öğretmen adaylarının dijital okuryazarlık puanları ile anlamlı bir fark olduğu gözlenmiştir. Fakat **Yabancı Dil** (M=3,78, SD=.75) ile BÖTE (M=3,90, SD=.69) ve Fen Bilgisi (M=3,90, SD=.69) öğretmenliği bölümlerindeki öğretmen adayları puanları arasında anlamlı gözlenememiştir.

4.2.2.2. Dijital Yasa Düzeylerinin Bölümlere Göre Karşılaştırılması

Bu bölümde dijital yasa düzeyinin bölümlere göre karşılaştırması yapılmış olup, bölümlere göre anlamlı farklılaşma farklılaşmadığı tespit edilmiştir.

Tablo 4.34

Dijital Yasa Düzeylerinin Bölümlere göre kişi sayısı, ortalama ve standart sapmaları

Bağımlı Değişken	Bölüm(J)	N	M	Standart Sapma
Dijital Yasa	BÖTE	42	4.3155	.68756
	Fen	174	4.1149	.81603
	Matematik	150	4.1967	.73650
	Sınıf	176	4.1463	.83425
	Okul Öncesi	158	4.2627	.85109
	PDR	196	4.2015	.67857
	Türkçe	134	4.2257	.83276
	Yabancı Dil	125	4.2560	.93996
	Toplam	1155	4.2006	.80399

Tablo 4.34'deki veriler incelendiğinde dijital yasa puanındaki en yüksek ortalamanın BÖTE bölümüne ait olduğu görülmektedir. En düşük ortalamanın ise Fen Bilgisi Öğretmenliği bölümünde olduğu görülmektedir. Yine tabloya göre ortalamaların birbirine yakın olduğunu da söylemek mümkündür.

Tablo 4.35

Dijital Yasa Alt Boyutunun Bölümlere Karşılaştırılması

	Varyans Kaynağı	Kareler Toplamı	sd	Kareler Ortalaması	F	p
Dijital Yasa	Gruplar Arası	3.429	7	.490	.757	.624
	Gruplar İçi	742.508	1147	.647		
	Toplam	745.937	1154			

(*p<.05 BÖTE=1, Fen=2, Matematik=3, Sınıf=4, Okul Öncesi=5, PDR=6, Türkçe=7, Yabancı Dil=8)

Tablo 4.35'de öğretmen adaylarının öğrenim gördükleri bölümlerin dijital yasa farkındalık düzeylerine etkisini incelemek amacıyla gerçekleştirilen tek faktörlü varyans analizinin sonucu yer almaktadır. Bu sonuçlara göre bölümler arasında dijital yasa puanları yönünden anlamlı bir fark yoktur ($F(7,1147) = .757, p > .05$).

4.2.2.3. Dijital Hak ve Sorumluluklar Düzeylerinin Bölümlere Göre Karşılaştırılması

Bu bölümde dijital hak ve sorumluluk düzeylerinin bölümlere göre karşılaştırılmasına yer verilmiştir.

Tablo 4.36

Dijital Hak ve Sorumluluk Düzeylerinin Bölümlere göre kişi sayısı, ortalama ve standart sapmaları

Bağımlı Değişken	Bölüm(J)	N	M	Standart Sapma
Dijital Hak ve Sorumluluk	BÖTE	42	4.2143	.59102
	Fen	174	3.8937	.70109
	Matematik	150	3.8817	.70037
	Sınıf	176	3.9276	.69494
	Okul Öncesi	158	3.9320	.80684
	PDR	196	3.9579	.69740
	Türkçe	134	4.1007	.79715
	Yabancı Dil	125	4.0980	.73910
	Toplam	1155	3.9712	.73053

Tablo 4.36'daki veriler incelendiğinde dijital yasa puanındaki en yüksek ortalamanın BÖTE bölümüne ait olduğu görülmektedir. En düşük ortalamanın ise Fen bölümünde olduğu görülmektedir. Yine tabloya göre ortalamaların birbirine yakın olduğunu da söylemek mümkündür. Fakat bu Farklılaşmanın hangi bölümler arasında olduğunu tespit etmek için Post Hoc tablosuna bakıldığında $p < .05$ durumunu sağlayan değere rastlanamamıştır.

Tablo 4.37

Dijital Hak ve Sorumluluk Alt Boyutunun Bölümlere Göre Karşılaştırılması

	Varyans Kaynağı	Kareler Toplamı	sd	Kareler Ortalaması	F	p	Eta Kare
Dijital Okur Hak ve Sorumluluk	Gruplar Arası	9.602	7	1.372	2.595	.012*	.016
	Gruplar İçi	606.254	1147	.529			
	Toplam	615.855	1154				

(* $p < .05$ BÖTE=1, Fen=2, Matematik=3, Sınıf=4, Okul Öncesi=5, PDR=6, Türkçe=7, Yabancı Dil=8)

Tablo 4.3'de öğretmen adaylarının öğrenim gördükleri bölümlerin hak ve sorumluluk farkındalık düzeylerine etkisini araştırmak için yapılan Anova sonuçlar yer almaktadır. Bu sonuçlar incelendiğinde bölümler arasında anlamlı bir fark olduğu görülmektedir. ($F(7,1147) = 2.595, p < .05, \eta^2 = .016$).

4.2.2.4. Dijital İletişim Alt Boyutunun Bölümlere Göre Karşılaştırılması

Bu bölümde dijital iletişim alt boyutunun bölümlere göre karşılaştırması yapılmıştır. Analiz sonuçları tablolar halinde verilmiştir.

Tablo 4.38

Dijital İletişim Alt Boyutunun Bölümlere göre kişi sayısı, ortalama ve standart sapmaları

Bağımlı Değişken	Bölüm(J)	N	M	Standart Sapma
Dijital İletişim	BÖTE	42	4.2143	.59102
	Fen	174	3.8937	.70109
	Matematik	150	3.8817	.70037
	Sınıf	176	3.9276	.69494
	Okul Öncesi	158	3.9320	.80684
	PDR	196	3.9579	.69740
	Türkçe	134	4.1007	.79715
	Yabancı Dil	125	4.0980	.73910
	Toplam	1155	3.9712	.73053

Tablo 4.38'deki verilere bakıldığında dijital iletişim puanında en yüksek ortalamanın yine BÖTE (N=42, M=4.21) bölümüne ait olduğu görülmektedir. Matematik Öğretmenliği (N=150, M=3.88) bölümünün ortalamasının ise diğer bölümlere göre en düşük olduğunu söylemek de mümkündür. Hangi bölümler arasında anlamlı farkın olduğunu gösteren Post Hoc analiz sonuçları ise Tablo 4.40' da verilmiştir.

Tablo 4.39

Dijital iletişim Alt Boyutunun Bölümlere Karşılaştırılması

	Varyans Kaynağı	Kareler Toplamı	sd	Kareler Ortalaması	F	p	Eta Kare
Dijital İletişim	Gruplar Arası	15.097	7	2.157	3.241	.002*	.019
	Gruplar İçi	763.196	1147	.665			
	Toplam	778.293	1154				

(*p<.05 BÖTE=1, Fen=2, Matematik=3, Sınıf=4, Okul Öncesi=5, PDR=6, Türkçe=7, Yabancı Dil=8)

Tablo 4.39'da verilen tek faktörlü varyans analizi sonuçlarına göre öğretmen adaylarının öğrenim gördükleri bölümler ile dijital iletişim alt boyutu arasında anlamlı bir fark vardır. ($F(7,1147) = 3.241, p < .05, n^2=.020$).

Tablo 4.40

Dijital İletişim Altı Boyutunda Anlamlı Farklılaşma Olan Bölümler- Post Hoc

Bağımlı Değişken	(I)Bölüm	(J)Bölüm	Ortalamaların Farkı	p
Dijital İletişim	Fen	BÖTE	-.31404	.329
		Matematik	-.09023	.975
		Sınıf	-.09184	.966
		Okul Öncesi	-.03759	1.000
		PDR	-.05511	.998
		Türkçe	-.13040	.862
		Yabancı Dil	-.38790*	.001*
	Sınıf	Böte	-.22220	.759
		Fen	.09184	.966
		Matematik	.00161	1.000
		Okul Öncesi	.05425	.999
		PDR	.03673	1.000
		Türkçe	-.03856	1.000
		Yabancı Dil	-.29606*	.041*
Dijital İletişim	Okul Öncesi	Böte	-.27645	.515
		Fen	.03759	1.000
		Matematik	-.05264	.999
		Sınıf	-.05425	.999
		PDR	-.01752	1.000
		Türkçe	-.09281	.979
		Yabancı Dil	-.35030*	.008*
	PDR	Böte	-.25893	.574
		Fen	.05511	.998
		Matematik	-.03512	1.000
		Sınıf	-.03673	1.000
		Okul Öncesi	.01752	1.000
		Türkçe	-.07529	.992
		Yabancı Dil	-.33279*	.009*
Yabancı Dil	Böte	.07386	1.000	
	Fen	.38790*	.001*	
	Matematik	.29767	.053	
	Sınıf	.29606*	.041*	
	Okul Öncesi	.35030*	.008*	
	PDR	.33279*	.009*	
	Türkçe	.25749	.180	

* $P < .05$ Türkçe(M=4,10, SD=.80) Yabancı Dil(M=4,10, SD=.74) BÖTE(M=4,21, SD=.59) PDR(M=3,96, SD=.68), Matematik(M=3,88, SD=.70), Sınıf(M=3,92, SD=.69), Okul Öncesi(M=3,93, SD=.81), Fen(M=3,89, SD=.70)

Analiz sonuçlarında; BÖTE, Matematik ve Türkçe öğretmenliği bölümünde okuyan öğretmen adaylarının dijital iletişim puanları ile diğer bölümlerdeki öğretmen adayları dijital iletişim puanları arasında anlamlı bir fark olmadığı tespit edilmiştir. Farklılaşma olan bölümler ise Tablo 4.40'de verilmiştir. Bu sonuçlara göre;

Fen Bilgisi ile Yabancı Dil öğretmenliği bölümü öğretmen adayları puanları arasında anlamlı bir farka işaret ederken, **Fen Bilgisi** ile BÖTE, Matematik, Sınıf, Okul Öncesi, PDR ve Türkçe öğretmenliği öğretmen adayları puanları arasında anlamlı bir fark yoktur.

Yine **Sınıf** ile Yabancı Dil öğretmenliği bölümleri öğretmen adayları puanları arasında anlamlı bir fark olduğu görülürken, **Sınıf** ile BÖTE, Fen Bilgisi, Okul Öncesi, PDR, Matematik ve Türkçe öğretmenliği bölümleri öğretmen adayları puanları arasında anlamlı bir fark olmadığı görülmektedir.

Okul Öncesi ile Yabancı Dil öğretmenliği bölümü öğretmen adayları puanları arasında anlamlı bir fark olduğu görülürken, **Okul Öncesi** ile BÖTE, Matematik, Fen Bilgisi, Sınıf, PDR ve Türkçe öğretmenliği bölümündeki öğretmen adayları puanları arasında anlamlı bir fark tespit edilememiştir.

Fen Bilgisi, sınıf, okulöncesi bölümlerinde olduğu gibi **PDR** ile Yabancı Dil bölümü öğretmen adayları puanları arasında istatistiksel olarak anlamlı bir fark tespit edilmişken, **PDR** ile BÖTE, Fen Bilgisi, Okul Öncesi, Matematik, Türkçe ve Sınıf Öğretmenliği bölümleri öğretmen adayları puanları arasında anlamlı bir fark tespit edilememiştir. Yapılan post hoc analiz sonuçlarına göre Yabancı dil öğretmenliği bölümünün dijital iletişim puanın BÖTE, Matematik, Türkçe bölümü dışındaki bölümler ile anlamlı farklılaştığı görülmektedir.

4.2.2.5. Dijital Güvenlik Düzeylerinin Bölümlere Göre Karşılaştırılması

Bu bölümde gerçekleştirilen analiz ile öğretmen adaylarının bölümleri ile dijital güvenlik düzeyi puanları karşılaştırılmıştır. Çıkan sonuçlar tablolar halinde verilmiştir.

Tablo 4.41

Dijital Güvenlik Alt Boyutunun Bölümlere göre kişi sayısı, ortalama ve standart sapmaları

Bağımlı Değişken	Bölüm(J)	N	M	Standart Sapma
Dijital Güvenlik	BÖTE	42	3.6111	.70966
	Fen	174	3.4387	.78424
	Matematik	150	3.4311	.67836
	Sınıf	176	3.2841	.88089
	Okul Öncesi	158	3.5274	.80182
	PDR	196	3.3656	.79139
	Türkçe	134	3.5423	.84927
	Yabancı Dil	125	3.4373	.82785
	Toplam	1155	3.4320	.80322

Tablo 4.41'deki betimsel istatistiki veriler incelendiğinde bölümlerin dijital güvenlik ortalamalarının 3.28 ile 3.61 arasında değiştiği görülmektedir. Yine tablodaki verilere bakılarak bölümlerin ortalamalarının genelde toplam ortalamaya yakın veya ortalamanın üstünde olduğunu söylemek mümkündür.

Tablo 4.42

Dijital Güvenlik Alt Boyutunun Bölümlere Karşılaştırılması

	Varyans Kaynağı	Kareler Toplamı	sd	Kareler Ortalaması	F	p	Eta Kare
Dijital Güvenlik	Gruplar Arası	9.141	7	1.306	2.037	.048*	.012
	Gruplar İçi	735.385	1147	.641			
	Toplam	744.526	1154				

(* $p < .05$ BÖTE=1, Fen=2, Matematik=3, Sınıf=4, Okul Öncesi=5, PDR=6, Türkçe=7, Yabancı Dil=8)

Tablo 4.42'deki veriler incelendiğinde öğretmen adaylarının öğrenim gördükleri bölümler ile dijital güvenlik alt boyutu arasında anlamlı bir fark olduğu görülmektedir. ($F(7,1147) = 2.037, p < .05, \eta^2 = .012$). Farklılaşmanın hangi bölümler arasında olduğunu gösteren veriler ise Tablo 4.3.40' ta gösterilmiştir. Fakat post hoc verileri incelendiğinde anlamlı düzeyde farklılaşma olan bölümler tespit edilememiştir. Bunun nedeni farklılaşmanın sınırda olması ve etki değerinin düşük olması olarak gösterilebilir.

Tablo 4.43

Dijital Güvenlik Altı Boyutunda Anlamlı Farklılaşma Olan Bölümler- Post Hoc

Bağımlı Değişken	(I)Bölüm	(J)Bölüm	Ortalamaların Farkı	p
Dijital Güvenlik	BÖTE	Fen	.17241	.916
		Matematik	.18000	.904
		Sınıf	.32702	.253
		Okul Öncesi	.08368	.999
		PDR	.24546	.618
		Türkçe	.06882	1.000
		Yabancı Dil	.17378	.927
	Fen	BÖTE	-.17241	.916
		Matematik	.00759	1.000
		Sınıf	.15461	.616
		Okul Öncesi	-.08873	.973
		PDR	.07305	.988
		Türkçe	-.10359	.951
		Yabancı Dil	.00136	1.000
	Matematik	BÖTE	-.18000	.904
		Fen	-.00759	1.000
		Sınıf	.14702	.718
		Okul Öncesi	-.09632	.966
		PDR	.06546	.995
		Türkçe	-.11118	.941
		Yabancı Dil	-.00622	1.000
	Sınıf	Böte	-.32702	.253
		Fen	-.15461	.616
		Matematik	-.14702	.718
		Okul Öncesi	-.24334	.103
		PDR	-.08156	.977
		Türkçe	-.25820	.093
		Yabancı Dil	-.15324	.728

Tablo 4.43

Dijital Güvenlik Altı Boyutunda Anlamlı Farklılaşma Olan Bölümler- Post Hoc(Devam)

Bağımlı Değişken	(I)Bölüm	(J)Bölüm	Ortalamaların Farkı	p
Dijital Güvenlik	Okul Öncesi	Böte	-.08368	.999
		Fen	.08873	.973
		Matematik	.09632	.966
		Sınıf	.24334	.103
		PDR	.16178	.558
		Türkçe	-.01486	1.000
		Yabancı Dil	.09009	.982
	PDR	Böte	-.24546	.618
		Fen	-.07305	.988
		Matematik	-.06546	.995
		Sınıf	.08156	.977
		Okul Öncesi	-.16178	.558
		Türkçe	-.17664	.504
		Yabancı Dil	-.07169	.994
	Türkçe	Böte	-.06882	1.000
		Fen	.10359	.951
		Matematik	.11118	.941
		Sınıf	.25820	.093
		Okul Öncesi	.01486	1.000
		PDR	.17664	.504
		Yabancı Dil	.10496	.966
Yabancı Dil	Böte	-.17378	.927	
	Fen	-.00136	1.000	
	Matematik	.00622	1.000	
	Sınıf	.15324	.728	
	Okul Öncesi	-.09009	.982	
	PDR	.07169	.994	
	Türkçe	-.10496	.966	

Türkçe(M=3,54 SD=.85) Yabancı Dil(M=3,44, SD=.83) BÖTE(M=3,61, SD=.71) PDR(M=3,36, SD=.79), Matematik(M=3,43, SD=.68), Sınıf(M=3,28, SD=.88), Okul Öncesi(M=3,53, SD=.80), Fen(M=3,43, SD=.78)

4.2.8. Dijital Ticaret Düzeylerinin Bölümlere Göre Karşılaştırılması

Tablo 4.44

Dijital Ticaret Boyutunun Bölümlere göre kişi sayısı, ortalama ve standart sapmaları

Bağımlı Değişken	Bölüm(J)	N	M	Standart Sapma
Dijital Ticaret	BÖTE	42	3.8333	.90542
	Fen	174	3.6590	.96233
	Matematik	150	3.5222	1.01914
	Sınıf	176	3.6212	.99354
	Okul Öncesi	158	3.5992	1.04584
	PDR	196	3.7925	.94162
	Türkçe	134	3.5149	1.06404
	Yabancı Dil	125	3.7867	1.01900
	Toplam	1155	3.6534	1.00193

Tablo 4.44'teki istatistiki veriler incelendiğinde Türkçe(N=134, M=3.51), Okulöncesi(N=158, M=3.60), ve Matematik(N=150, M=3.52) bölümlerinin puanlarının ortalamasının(N=1155, M=3.65) altında kaldığı görülmektedir. Buna karşın ortalamasının altında olan bölümlerin puanları da ortalama çok yakındır.

Tablo 4.45

Dijital Ticaret Alt Boyutunun Bölümlere Karşılaştırılması

	Varyans Kaynağı	Kareler Toplamı	sd	Kareler Ortalaması	F	p
Dijital Ticaret	Gruplar Arası	13.176	7	1.882	1.885	.069
	Gruplar İçi	1145.287	1147	.999		
	Toplam	1158.463	1154			

(*p<.05 BÖTE=1, Fen=2, Matematik=3, Sınıf=4, Okul Öncesi=5, PDR=6, Türkçe=7, Yabancı Dil=8)

Tablo 4.45'teki veriler incelendiğinde dijital ticaret değişkeninin öğretmen adaylarının öğrenim gördükleri bölüme göre farklılaşıp farklılaşmadığını tespit etmek için tek faktörlü varyans analizi yapılmıştır. Analiz sonucunda bölümler arasındaki farkın anlamlı olmadığı görülmüştür($F(7,1147) = 1.885, p > .05$).

4.2.2.7. Dijital Erişim Düzeylerinin Bölümlere Göre Karşılaştırılması

Bu bölümde öğretmen adaylarının öğrenim gördükleri bölümlerin dijital erişim düzeylerine etkisini incelemek amacıyla tek faktörlü varyans analizi yürütülmüştür.

Tablo 4.46

Dijital Erişim Boyutunun Bölümlere göre kişi sayısı, ortalama ve standart sapmaları

Bağımlı Değişken	Bölüm(J)	N	M	Standart Sapma
Dijital Erişim	BÖTE	42	3.6111	.70966
	Fen	174	3.4387	.78424
	Matematik	150	3.4311	.67836
	Sınıf	176	3.2841	.88089
	Okul Öncesi	158	3.5274	.80182
	PDR	196	3.3656	.79139
	Türkçe	134	3.5423	.84927
	Yabancı Dil	125	3.4373	.82785
	Toplam	1155	3.4320	.80322

Tablo 4.46'daki betimsel istatistiki veriler incelendiğinde bölümlerin dijital güvenlik ortalamalarının 3.28 ile 3.61 arasında değiştiği görülmektedir. Yine tablodaki verilere bakılarak bölümlerin ortalamalarının genelde toplam ortalamaya yakın veya ortalamanın üstünde olduğunu söylemek mümkündür.

Tablo 4.47

Dijital Erişim Alt Boyutunun Bölümlere Karşılaştırılması

	Varyans Kaynağı	Kareler Toplamı	sd	Kareler Ortalaması	F	p	Eta Kare
Dijital Erişim	Gruplar Arası	24.679	7	3.526	5.319	.000*	.035*
	Gruplar İçi	760.232	1147	.663			
	Toplam	784.911	1154				

(* $p < .05$ BÖTE=1, Fen=2, Matematik=3, Sınıf=4, Okul Öncesi=5, PDR=6, Türkçe=7, Yabancı Dil=8)

Tablo 4.47'deki veriler incelendiğinde öğretmen adaylarının öğrenim gördükleri bölümler ile dijital erişim alt boyutu arasında anlamlı bir fark olduğu görülmektedir. ($F(7,1147) = 5.319, p < d .05, n^2=.035$). Farklılaşmanın hangi bölümler arasında olduğunu gösteren veriler ise Tablo 4.58'de gösterilmiştir.

Tablo 4.48

Dijital Erişim Altı Boyutunda Anlamlı Farklılaşma Olan Bölümler- Post Hoc

Bağımlı Değişken	(I)Bölüm	(J)Bölüm	Ortalamaların Farkı	p	
Dijital Erişim	BÖTE	Fen	.44527*	.032*	
		Matematik	.50603*	.009*	
		Sınıf	.54969*	.002*	
		Okul Öncesi	.50412*	.009*	
		PDR	.53798*	.003*	
		Türkçe	.47572*	.022*	
		Yabancı Dil	.14159	.978	
	Fen	BÖTE		-.44527*	.032*
		Matematik		.06077	.998
		Sınıf		.10443	.932
		Okul Öncesi		.05885	.998
		PDR		.09272	.958
		Türkçe		.03045	1.000
		Yabancı Dil		-.30368*	.032*
Matematik	BÖTE		-.50603*	.009	
	Fen		-.06077	.998	
	Sınıf		.04366	1.000	
	Okul Öncesi		-.00191	1.000	
	PDR		.03195	1.000	
	Türkçe		-.03032	1.000	
	Yabancı Dil		-.36444*	.006*	
Sınıf	Böte		-.54969*	.002*	
	Fen		-.10443	.932	
	Matematik		-.04366	1.000	
	Okul Öncesi		-.04557	1.000	
	PDR		-.01171	1.000	
	Türkçe		-.07398	.994	
	Yabancı Dil		-.40811*	.001*	

Tablo 4.48

Dijital Erişim Altı Boyutunda Anlamlı Farklılaşma Olan Bölümler- Post Hoc(Devam)

Bağımlı Değişken	(I)Bölüm	(J)Bölüm	Ortalamaların Farkı	p
Dijital Erişim	Okul Öncesi	Böte	-.50412*	.009
		Fen	-.05885	.998
		Matematik	.00191	1.000
		Sınıf	.04557	1.000
		PDR	.03386	1.000
		Türkçe	-.02840	1.000
		Yabancı Dil	-.36253*	.005
	PDR	Böte	-.53798*	.003
		Fen	-.09272	.958
		Matematik	-.03195	1.000
		Sınıf	.01171	1.000
		Okul Öncesi	-.03386	1.000
		Türkçe	-.06227	.997
		Yabancı Dil	-.39639*	.001
Türkçe	Böte	-.47572*	.022	
	Fen	-.03045	1.000	
	Matematik	.03032	1.000	
	Sınıf	.07398	.994	
	Okul Öncesi	.02840	1.000	
	PDR	.06227	.997	
	Yabancı Dil	-.33413*	.022	
Dijital Erişim	Yabancı Dil	Böte	-.14159	.978
		Fen	.30368*	.032
		Matematik	.36444*	.006
		Sınıf	.40811*	.001
		Okul Öncesi	.36253*	.005
		PDR	.39639*	.001
		Türkçe	.33413*	.022

P<.05* Türkçe(M=3,54 SD=.84) Yabancı Dil(M=3,44, SD=.82) BÖTE(M=3,61, SD=.70) PDR(M=3,36, SD=.79), Matematik(M=3,43, SD=.67), Sınıf(M=3,28, SD=.88), Okul Öncesi(M=3,52, SD=.80), Fen(M=3,43, SD=.78)

Tablo 4.48' de hangi bölümler arasında farklılaşma olduğu gösterilmiştir. Bu tablodan da anlaşılacağı gibi **BÖTE** ile Matematik, Sınıf, Okul Öncesi, PDR, Fen Bilgisi ve Türkçe öğretmenliği bölümleri öğretmen adaylarının dijital erişim puanları arasında anlamlı bir farklılaşma görülmektedir. Fakat **BÖTE** ile Yabancı Dil öğretmenliği bölümü öğretmen adayları puanları arasında anlamlı bir farka ulaşamamıştır.

Fen Bilgisi ile BÖTE ve Yabancı Dil öğretmenliği bölümü öğretmen adayları dijital erişim puanları arasında anlamlı bir fark varken, **Fen Bilgisi** ile Matematik, Sınıf, Okul Öncesi, PDR ve Türkçe öğretmenliği bölümleri öğretmen adayları puanları arasında anlamlı bir fark yoktur.

Yine post hoc analizi sonuçları **Matematik** ile BÖTE ve Yabancı Dil öğretmenliği bölümü öğretmen adayları dijital erişim puanları arasında anlamlı bir fark varken, **Matematik** ile Sınıf, Okul Öncesi, PDR, Fen Bilgisi ve Türkçe öğretmenliği bölümleri öğretmen adaylarının puanları arasında anlamlı bir fark yoktur.

Sınıf Öğretmenliği ile BÖTE ve Yabancı Dil öğretmenliği bölümü öğretmen adayları puanları arasında anlamlı bir fark gözlenmişken; **Sınıf** ile Fen Bilgisi, Okul Öncesi, PDR, Matematik ve Türkçe öğretmenliği bölümleri öğretmen adayları puanları arasında anlamlı bir farka ulaşamamıştır. **Okul Öncesi** ile BÖTE ve Yabancı Dil öğretmenliği bölümü öğretmen adayları puanları arasında anlamlı bir fark olduğu görülürken, **Okul Öncesi** ile Matematik, Fen Bilgisi, Sınıf, PDR ve Türkçe öğretmen adayları puanları arasında anlamlı bir fark yoktur.

PDR ile BÖTE ve Yabancı Dil öğretmenliği bölümü öğretmen adayları puanları arasında anlamlı bir farkın olduğu görülürken, **PDR** ile Fen Bilgisi, Okul Öncesi, Matematik, Türkçe ve Sınıf öğretmenliği bölümü öğretmen adayları puanları arasında anlamlı bir fark yoktur.

Diğer bölümlerde olduğu gibi **Türkçe** ile BÖTE ve Yabancı Dil öğretmenliği bölümü öğretmen adayları puanları arasında anlamlı bir fark varken, **Türkçe** ile Fen Bilgisi, Okul Öncesi, Matematik ve Sınıf öğretmenliği bölümleri öğretmen adayları puanları arasında anlamlı bir fark yoktur.

Yabancı Dil ile Fen Bilgisi, Sınıf, PDR, Okul Öncesi, Türkçe ve Matematik öğretmenliği bölümü öğretmen adayları dijital erişim puanları arasında anlamlı bir fark tespit edilmiştir. Fakat **Yabancı Dil** ile BÖTE öğretmen adayları puanları arasında küçükte olsa bir fark olmasına rağmen bu fark anlamlı düzeyde değildir.

4.2.2.8. Dijital Etik Düzeylerinin Bölümlere Göre Karşılaştırılması

Bu bölümde öğretmen adaylarının öğrenim gördükleri bölüm ile dijital etik düzeylerini karşılaştırmak amacıyla yürütülen analiz sonuçlarına yer verilmiştir.

Tablo 4.49

Dijital Etik Alt Boyutunun Bölümlere göre kişi sayısı, ortalama ve standart sapmaları

Bağımlı Değişken	Bölüm(J)	N	M	Standart Sapma
Dijital Etik	BÖTE	42	4.0873	.70253
	Fen	174	3.8621	.72669
	Matematik	150	3.9933	.68702
	Sınıf	176	3.8883	.71679
	Okul Öncesi	158	3.7827	.82420
	PDR	196	4.0493	.66096
	Türkçe	134	3.9204	.71641
	Yabancı Dil	125	4.0693	.82880
	Toplam	1155	3.9414	.73791

Tablo 4.49'daki betimsel istatistik sonuçlarına göre dijital etik ortalaması en düşük olan bölüm Okul Öncesidir(N=158, M=3,78). Yine tablodaki verilere bakılarak Türkçe, Okul Öncesi, Sınıf, Fen bölümlerin puanlarının ortalamasının altında olduğu görülmektedir.

Tablo 4.50

Dijital Etik Alt Boyutunun Bölümlere Karşılaştırılması

	Varyans Kaynağı	Kareler Toplamı	sd	Kareler Ortalaması	F	p	Eta Kare
Dijital Etik	Gruplar Arası	11.258	7	1.608	2.989	.004*	.018
	Gruplar İçi	617.111	1147	.538			
	Toplam	628.369	1154				

(*p<.05 BÖTE=1, Fen=2, Matematik=3, Sınıf=4, Okul Öncesi=5, PDR=6, Türkçe=7, Yabancı Dil=8)

Tablo 4.50'daki veriler incelendiğinde öğretmen adaylarının öğrenim gördükleri bölümler ile dijital etik alt boyutu arasında anlamlı bir fark olduğu görülmektedir. ($F(7,1147) = 5.319, p < .05, n^2 = .018$). Farklılaşmanın hangi bölümler arasında olduğunu gösteren veriler ise Tablo 4.61' de gösterilmiştir.

Tablo 4.51

Dijital Etik Altı Boyutunda Anlamlı Farklılaşma Olan Bölümler- Post Hoc

Bağımlı Değişken	(I)Bölüm	(J)Bölüm	Ortalamaların Farkı	P	
Dijital Etik	BÖTE	Fen	.22523	.630	
		Matematik	.09397	.996	
		Sınıf	.19904	.762	
		Okul Öncesi	.30460	.246	
		PDR	.03798	1.000	
		Türkçe	.16690	.904	
		Yabancı Dil	.01797	1.000	
	Fen	BÖTE		-.22523	.630
		Matematik		-.13126	.747
		Sınıf		-.02619	1.000
		Okul Öncesi		.07937	.977
		PDR		-.18725	.218
		Türkçe		-.05833	.997
		Yabancı Dil		-.20726	.237
Matematik	BÖTE		-.09397	.996	
	Fen		.13126	.747	
	Sınıf		.10508	.903	
	Okul Öncesi		.21063	.188	
	PDR		-.05599	.997	
	Türkçe		.07294	.991	
	Yabancı Dil		-.07600	.990	
Sınıf	Böte		-.19904	.762	
	Fen		.02619	1.000	
	Matematik		-.10508	.903	
	Okul Öncesi		.10556	.894	
	PDR		-.16106	.406	
	Türkçe		-.03214	1.000	
	Yabancı Dil		-.18108	.409	
Okul Öncesi	Böte		-.30460	.246	
	Fen		-.07937	.977	
	Matematik		-.21063	.188	
	Sınıf		-.10556	.894	
	PDR		-.26662*	.016*	
	Türkçe		-.13770	.751	
	Yabancı Dil		-.28663*	.025*	

Tablo 4.51

Dijital Etik Altı Boyutunda Anlamlı Farklılaşma Olan Bölümler- Post Hoc(Devam)

Bağımlı Değişken	(I)Bölüm	(J)Bölüm	Ortalamaların Farkı	P
Dijital Etik	PDR	Böte	-.03798	1.000
		Fen	.18725	.218
		Matematik	.05599	.997
		Sınıf	.16106	.406
		Okul Öncesi	.26662*	.016*
		Türkçe	.12892	.769
		Yabancı Dil	-.02001	1.000
		Türkçe	Böte	-.16690
	Fen		.05833	.997
	Matematik		-.07294	.991
	Sınıf		.03214	1.000
	Okul Öncesi		.13770	.751
	PDR		-.12892	.769
	Yabancı Dil	Yabancı Dil	-.14894	.730
Böte		-.01797	1.000	
Fen		.20726	.237	
Matematik		.07600	.990	
Sınıf		.18108	.409	
Okul Öncesi		.28663*	.025*	
PDR		.02001	1.000	
Türkçe		.14894	.730	

Türkçe(M=3,92 SD=.71) Yabancı Dil(M=4,07, SD=.83) BÖTE(M=4,09, SD=.70) PDR(M=4,05, SD=.66), Matematik(M=3,99, SD=.68), Sınıf(M=3,88, SD=.71), Okul Öncesi(M=3,78, SD=.82), Fen(M=3,86, SD=.73)

Tablo 4.51' deki post hoc analiz sonuçları incelendiğinde **BÖTE** ile Matematik, Sınıf, Okul Öncesi, PDR, Fen Bilgisi, Türkçe ve Yabancı Dil öğretmen adayları puanları arasında anlamlı bir fark olmadığı görülmektedir.

Fen Bilgisi ile BÖTE, Yabancı Dil, Matematik, Sınıf, Okul Öncesi, PDR ve Türkçe öğretmen adayları puanları arasında anlamlı bir fark yoktur. **Matematik** ile BÖTE, Yabancı Dil, Sınıf, Okul Öncesi, PDR, Fen Bilgisi ve Türkçe öğretmen adayları puanları arasında anlamlı bir fark yoktur. **Sınıf Öğretmenliği** ile BÖTE, Yabancı Dil, Fen Bilgisi, Okul Öncesi, PDR, Matematik ve Türkçe öğretmen adayları puanları arasında anlamlı bir fark tespit edilememiştir. **Okul Öncesi** ile PDR ve Yabancı Dil öğretmenliği bölümü öğretmen adayları puanları arasında anlamlı bir fark bulunurken, **Okul Öncesi** ile Matematik, Fen Bilgisi, Sınıf, BÖTE ve Türkçe öğretmen adayları

puanları arasında anlamlı bir fark yoktur. **PDR** ile Okul Öncesi bölümü öğretmen adayları puanları arasında anlamlı bir fark varken, **PDR** ile BÖTE, Yabancı Dil, Fen Bilgisi, Matematik, Türkçe ve Sınıf öğretmenliği bölümleri öğretmen adayları puanları arasında anlamlı bir fark olmadığı görülmektedir. Yine **Türkçe** ile BÖTE, Yabancı Dil, Fen Bilgisi, Okul Öncesi, Matematik, Sınıf ve PDR öğretmen adayları puanları arasında anlamlı bir fark bulunamamıştır. **Yabancı Dil** ile Okul Öncesi öğretmenliği bölümü öğretmen adayları puanları arasında anlamlı bir fark tespit edilmişken, **Yabancı Dil** ile Fen Bilgisi, Sınıf, PDR, Okul Öncesi, Türkçe, Matematik ve BÖTE öğretmen adayları puanları arasında anlamlı bir fark tespiti yapılamamıştır.

4.2.2.9. Dijital Sağlık Düzeylerinin Bölümlere Göre Karşılaştırılması

Tablo 4.52

Dijital Sağlık Boyutunun Bölümlere göre kişi sayısı, ortalama ve standart sapmaları

Bağımlı Değişken	Bölüm(J)	N	M	Standart Sapma
Dijital Sağlık	BÖTE	42	3.0000	.84904
	Fen	174	3.1207	.85799
	Matematik	150	3.0956	.83128
	Sınıf	176	3.1856	.93518
	Okul Öncesi	158	2.9536	.85334
	PDR	196	3.2415	.90617
	Türkçe	134	3.2239	.95406
	Yabancı Dil	125	3.2107	.92509
	Toplam	1155	3.1423	.89538

Tablo 4.52’de farklı bölümlerdeki öğretmen adaylarının dijital sağlık alt boyutundaki puanlarının ortalaması sunulmaktadır.

Tablo 4.53

Dijital Sağlık Alt Boyutunun Bölümlere Karşılaştırılması

	Varyans Kaynağı	Kareler Toplamı	sd	Kareler Ortalaması	F	p
Dijital Sağlık	Gruplar Arası	10.621	7	1.517	1.903	.066
	Gruplar İçi	914.553	1147	.797		
	Toplam	925.174	1154			

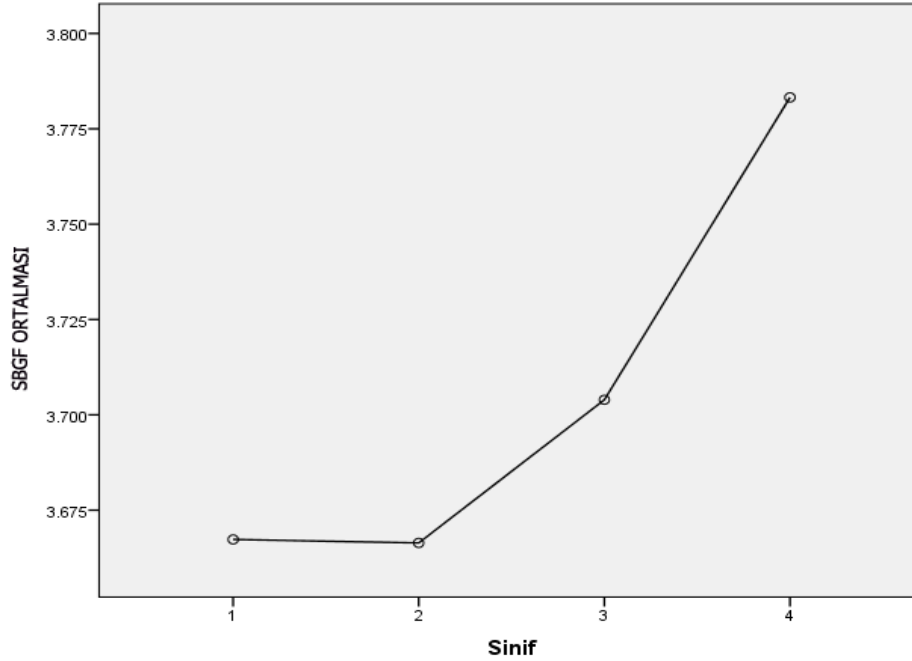
(*p<.05 BÖTE=1, Fen=2, Matematik=3, Sınıf=4, Okul Öncesi=5, PDR=6, Türkçe=7, Yabancı Dil=8)

Öğretmen adaylarının öğrenim gördükleri bölümlerin dijital sağlık farkındalık düzeylerine etkisini incelemek amacıyla tek faktörlü varyans analizi gerçekleştirilmiştir. Analiz sonuçlarına göre bölümler arasında dijital sağlık değişkenine göre anlamlı bir fark yoktur ($F(7,1147) = 1.903, p > .05$).

4.3. Bağımlı Değişkenlerin Sınıf Düzeylerine Göre Farkı - Tek Yönlü Varyans Analizi (ANOVA)

4.3.1. Siber Bilgi Güvenliği Farkındalığı Değişkeninin Sınıf Düzeyine Göre Karşılaştırılması

Şekil 4.3'teki grafikte sınıf düzeyine göre siber bilgi güvenliği farkındalıkları gösterilmiştir. Grafik incelendiğinde 1. ve 2. sınıf ' siber bilgi güvenliği farkındalığı puanlarının değişmediği söylemek mümkünken, 3. ve 4. sınıfta da arttığını söylemek mümkündür.



Şekil 4.3. Sınıf Düzeyine Göre Siber Bilgi Güvenliği Farkındalık Ortalamalarının Grafiği

Tablo 4.54

Siber Bilgi Güvenliği Farkındalığının Sınıf Düzeyine Göre Kişi Sayısı, Ortalama ve Standart Sapmaları

Bağımlı Değişken	Sınıf Düzeyi	N	M	Standart Sapma
Siber Güvenlik Farkındalığı	1	319	3.6673	.64410
	2	286	3.6664	.65669
	3	266	3.7039	.62677
	4	284	3.7832	.62828
	Toplam	1155	3.7040	.64039

Tablo 4.54' te öğretmen adaylarının sınıf Düzeyine göre kişi sayısı, ortalama ve standart sapma değerleri verilmiştir.

Tablo 4.55

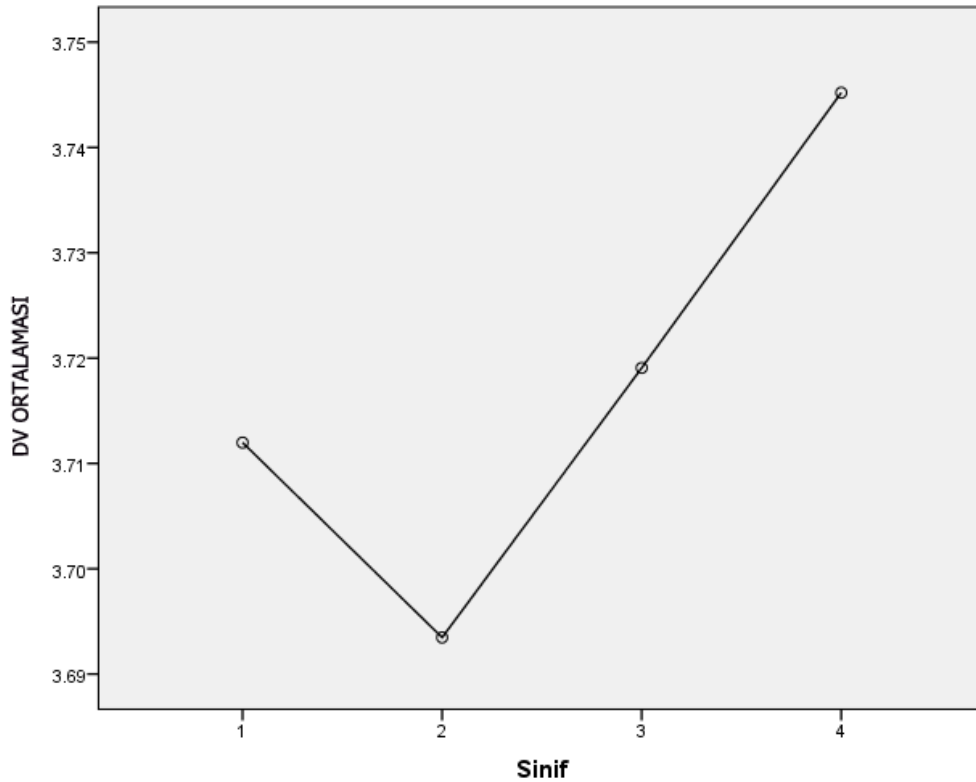
Siber Bilgi Güvenliği Farkındalığının Sınıf Düzeylerine Göre Karşılaştırılması

	Varyans Kaynağı	Kareler Toplamı	sd	Kareler Ortalaması	F	p
SBGF	Gruplar Arası	2.616	3	.872	2.133	.094
	Gruplar İçi	470.643	1151	.409		
	Toplam	473.260	1154			

Tablo 4.55'te öğretmen adaylarının öğrenim gördükleri Sınıf Düzeyinin siber bilgi güvenliği farkındalığına etkisini incelemek amacı ile yürütülen tek faktörlü varyans analizi sonuçları gösterilmektedir ($F(7,1147) = 2.133$). Sonuçlar incelendiğinde öğrenim gördükleri kademe ile siber güvenlik farkındalıkları arasında anlamlı bir fark olup olmadığını gösteren sig.(p) değeri .05' ten büyük çıkmıştır. Bu değer anlamlı farklılaşmanın olmadığını göstermektedir.

4.3.2. Dijital vatandaşlık düzeyinin Sınıf düzeyine göre farkı

Şekil 4.4' te yer alan grafikte öğretmen adaylarının Sınıf düzeyine göre dijital vatandaşlık seviyeleri verilmiştir. Grafik incelendiğinde dijital vatandaşlık ortalamalarının 2.sınıf ta en düşük seviyede olduğu, 3 ve 4. Sınıfta ise arttığı görülmüştür.



Şekil 4.4. Sınıf Düzeyine Göre Dijital Vatandaşlık Ortalamalarının Grafiği

Tablo 4.56

Dijital Vatandaşlık Seviyelerinin Sınıf Düzeyine Göre Kişi Sayısı, Ortalama ve Standart Sapmaları

Bağımlı Değişken	Sınıf Düzeyi	N	M	Standart Sapma
Dijital Vatandaşlık	1	319	3.7120	.51792
	2	286	3.6935	.48163
	3	266	3.7191	.46706
	4	284	3.7452	.45510
	Toplam	1155	3.7172	.48211

Tablo 4.56' daki veriler incelendiğinde öğretmen adayları dijital vatandaşlık düzeyi bakımından sadece 2. Sınıfta(N=319, M=3.71) ortalamanın altında kalmıştır. En yüksek ortalama ise 4.sınıfta(N=284, M=3,75) ulaşmışlardır.

Tablo 4.57

Dijital Vatandaşlık Seviyelerinin Sınıf Düzeylerine Göre Karşılaştırılması

	Varyans Kaynağı	Kareler Toplamı	sd	Kareler Ortalaması	F	p
Dijital Vatandaşlık	Gruplar Arası	.393	3	.131	.563	.639
	Gruplar İçi	267.835	1151	.233		
	Toplam	268.228	1154			

Öğretmen adaylarının öğrenim gördükleri Sınıf kademesinin dijital vatandaşlık düzeylerine etkisini tespit etmek amacı ile gerçekleştirilen analiz sonuçları Tablo 4.57'te verilmiştir. Analiz sonuçlarına göre öğretmen adaylarının buldukları sınıf kademesi ile dijital vatandaşlık düzeyleri arasında anlamlı bir fark bulunamamıştır ($F(3,1151) = .563, p > .05$).

4.3.2. 1.Dijital okuryazarlık alt boyutunu düzeyinin sınıf düzeyine göre farkı

Tablo 4.58

Dijital Okuryazarlık Seviyelerinin Sınıf Düzeyine Göre Kişi Sayısı, Ortalama ve Standart Sapmaları

Bağımlı Değişken	Sınıf Düzeyi	N	M	Standart Sapma
Dijital Okuryazarlık	1	319	3.3960	.72738
	2	286	3.4172	.74192
	3	266	3.4618	.77750
	4	284	3.6021	.75187
	Toplam	1155	3.4671	.75212

Tablo 4.58' deki veriler incelendiğinde öğretmen adayları dijital okuryazarlık düzeyinin Sınıf kademesi ile doğru orantılı olarak arttığı görülmektedir. Ayrıca ortalamalar 1. ve 2. Sınıfta toplam ortalamanın altında kalmışken 3. ve 4. Sınıfta ortalamanın üstüne çıkmıştır.

Tablo 4.59

Dijital Okuryazarlık Seviyelerinin Sınıf Düzeylerine Göre Karşılaştırılması

	Varyans Kaynağı	Kareler Toplamı	sd	Kareler Ortalaması	F	p	Eta Kare
Dijital Okuryazarlık	Gruplar Arası	7.506	3	2.502	4.463	.004*	.011
	Gruplar İçi	645.299	1151	.561			
	Toplam	652.805	1154				

Öğretmen adaylarının öğrenim gördükleri Sınıf kademesinin dijital okuryazarlık düzeyleri üzerine etkisini belirlemek için gerçekleştirilen analiz sonuçları Tablo 4.59'da verilmiştir. Bu analiz sonuçlarına göre öğrenim gördükleri Sınıf kademesi ile dijital okuryazarlık düzeyleri arasında anlamlı bir fark olduğu görülmektedir. ($F(3,1151) = 4.463, p < .05, n^2 = .011$). Anlamlı farklılaşmanın hangi Sınıf Düzeyinde olduğunu gösteren post hoc analiz sonuçları ise Tablo 4.60'te verilmiştir.

Tablo 4.60

Dijital Okuryazarlık Altı Boyutunda Anlamlı Farklılaşma Sınıf Düzeyi- Post Hoc

Bağımlı Değişken	(I) Sınıf Düzeyi	(J) Sınıf Düzeyi	Ortalamaların Farkı	p
Dijital Okuryazarlık	1	2	-.02122	.986
		3	-.06575	.715
		4	-.20608*	.004*
	2	1	.02122	.986
		3	-.04453	.898
		4	-.18486*	.017*
	3	1	.06575	.715
		2	.04453	.898
		4	-.14033	.125
	4	1	.20608*	.004
		2	.18486*	.017*
		3	.14033	.125

(1.sınıf(M=3.40,SD=73), 2.Sınıf(M=3.41,SD=74),3.Sınıf(M=3.46,SD=77),4.Sınıf(M=3.60,SD=75))

Tablo 4.60'de yer alan bölümler arası farkları detaylı incelemek amacıyla yürütülen Post-Hoc analiz sonuçları;

- 1.sınıf öğretmen adayları ile 4 öğretmen adayları puanları arasında anlamlı bir farka işaret ederken, 1. Sınıf ile 2. ve 3. Sınıf öğretmen adayları ile anlamlı fark yoktur.
- 2.Sınıf öğretmen adayları ile 4 öğretmen adayları puanları arasında anlamlı bir fark söz konusuyken, 2. Sınıf ile 1. Ve 3. Sınıf öğretmen adayları ile anlamlı fark yoktur.

- 3.Sınıf öğretmen adayları ile 1., 2. ve 4. Sınıf öğretmen adayları ile anlamlı fark yoktur.
- 4.Sınıf öğretmen adayları ile 1. ve 2.Sınıf öğretmen adayları puanları arasında anlamlı bir fark vardır. Fakat 4.Sınıf öğretmen adaylarının dijital okuryazarlık puanları ile 3. Sınıf öğretmen adaylarının dijital okuryazarlık puanları arasında anlamlı fark yoktur.

4.3.2.2. Dijital yasa düzeyinin Sınıf düzeyine göre farkı

Tablo 4.61

Dijital Yasa Seviyelerinin Sınıf Düzeyine Göre Kişi Sayısı, Ortalama ve Standart Sapmaları

Bağımlı Değişken	Sınıf Düzeyi	N	M	Standart Sapma
Dijital Yasa	1	319	4.2712	.85836
	2	286	4.1801	.85451
	3	266	4.1344	.77674
	4	284	4.2042	.70531
	Toplam	1155	4.2006	.80399

Tablo 4.61'deki veriler incelendiğinde öğretmen adayları dijital yasa düzeylerinin ortalaması 1. ve 4.sınıfta toplam ortalamadan üstüne çıkmıştır. Buna rağmen diğer Sınıf Düzeyindeki ortalamadan da toplam ortalamadan çok uzaklaşmadığı görülmektedir.

Tablo 4.62

Dijital Yasa Seviyelerinin Sınıf Düzeylerine Göre Karşılaştırılması

	Varyans Kaynağı	Kareler Toplamı	sd	Kareler Ortalaması	F	p
Dijital Yasa	Gruplar Arası	2.878	3	.959	1.486	.217
	Gruplar İçi	743.059	1151	.646		
	Toplam	745.937	1154			

Öğretmen adaylarının öğrenim gördükleri sınıf kademesinin dijital yasa düzeyleri üzerine etkisini olup olmadığını tespit etmek amacı ile tek tek faktörlü varyans analizi yapılmıştır. Elde edilen sonuçlara göre öğretmen adaylarının öğrenim gördükleri kademe ile dijital yasa düzeyleri arasında anlamlı bir fark bulunamamıştır ($F(3,1151) = 1.486, p > .05$).

4.3.2.3 Dijital hak ve sorumluluk düzeyinin Sınıf düzeyine göre farkı

Tablo 4.63

Dijital Hak ve Sorumluluk Seviyelerinin Sınıf Düzeyine Göre Kişi Sayısı, Ortalama ve Standart Sapmaları

Bağımlı Değişken	Sınıf Düzeyi	N	M	Standart Sapma
Dijital Hak ve Sorumluluk	1	319	3.9592	.77747
	2	286	3.9598	.76097
	3	266	3.9774	.74064
	4	284	3.9903	.63200
	Toplam	1155	3.9712	.73053

Tablo4.63 deki veriler incelendiğinde öğretmen adaylarının dijital hak ve sorumluluk düzeylerinin 1.sınıf, 2.Sınıf ve 3.sınıfta düzenli olarak arttığı gözlenirken 4.sınıfa gelindiğinde ortalamada bir düşüş olduğu gözlenmiştir.

Tablo 4.64

Dijital Hak ve Sorumluluk Seviyelerinin Sınıf Düzeylerine Göre Karşılaştırılması

	Varyans Kaynağı	Kareler Toplamı	sd	Kareler Ortalaması	F	p
Dijital Hak ve Sorumluluk	Gruplar Arası	.197	3	.066	.123	.947
	Gruplar İçi	615.658	1151	.535		
	Toplam	615.855	1154			

Tablo 4.64'te öğretmen adaylarının öğrenim gördükleri Sınıf kademesinin dijital hak ve sorumluluk düzeyleri üzerine etkisini incelemek amacıyla tek faktörlü varyans analizi gerçekleştirilmiştir. Analiz sonucunda öğrenim gördükleri kademe ve dijital hak ve sorumluluk düzeyleri arasında anlamlı bir fark olmadığı görülmüştür ($F(3,1151) = .123, p > .05$).

4.3.2.4. Dijital iletişim düzeyinin Sınıf düzeyine göre farkı

Tablo 4.65

Dijital İletişim Seviyelerinin Sınıf Düzeyine Göre Kişi Sayısı, Ortalama ve Standart Sapmaları

Bağımlı Değişken	Sınıf Düzeyi	N	M	Standart Sapma
Dijital İletişim	1	319	3.7704	.88265
	2	286	3.7369	.81437
	3	266	3.8242	.75354
	4	284	3.7799	.81937
	Toplam	1155	3.7768	.82124

Tablo4.65'deki veriler incelendiğinde öğretmen adaylarının dijital iletişim ortalamalarının 3.73 ile 3.82 aralığında değiştiği, toplam ortalamasının ise (N=1155) 3.77 olduğu tespit edilmiştir. Ayrıca öğretmen adaylarının en yüksek ortalamaya 3.sınıf kademesinde ulaştığı görülmektedir.

Tablo 4.66

Dijital İletişim Seviyelerinin Sınıf Düzeylerine Göre Karşılaştırılması						
	Varyans Kaynağı	Kareler Toplamı	sd	Kareler Ortalaması	F	p
Dijital Hak İletişim	Gruplar Arası	1.070	3	.357	.528	.663
	Gruplar İçi	777.223	1151	.675		
	Toplam	778.293	1154			

Tablo 4.66' da öğretmen adaylarının öğrenim gördükleri sınıf kademesinin dijital iletişim düzeyleri üzerine etkisini belirlemek amacıyla tek faktörlü varyans analizi yapılmıştır. Yapılan tek faktörlü varyans analizi sonucunda öğrenim gördükleri kademe ile dijital erişim düzeyleri arasında anlamlı bir farka ulaşılamamıştır ($F(3,1151) = .528, p > .05$).

4.3.2.5. Dijital güvenlik düzeyinin Sınıf düzeyine göre farkı

Tablo 4.67

Dijital Güvenlik Seviyelerinin Sınıf Düzeyine Göre Kişi Sayısı, Ortalama ve Standart Sapmaları				
Bağımlı Değişken	Sınıf Düzeyi	N	M	Standart Sapma
Dijital Güvenlik	1	319	3.4232	.85267
	2	286	3.4977	.77522
	3	266	3.3622	.75984
	4	284	3.4413	.81172
	Toplam	1155	3.4320	.80322

Tablo 4.67'deki veriler incelendiğinde öğretmen adaylarının dijital güvenlik ortalamalarının 3.36 ile 3.49 aralığında değiştiği tespit edilmiştir. Dijital güvenlik ortalamasının en düşük 3.Sınıf kademesinde olduğu da görülmektedir

Tablo 4.68

Dijital Güvenlik Seviyelerinin Sınıf Düzeylerine Göre Karşılaştırılması

	Varyans Kaynağı	Kareler Toplamı	sd	Kareler Ortalaması	F	p
Dijital Güvenlik	Gruplar Arası	1.070	2.580	.860	1.334	.262
	Gruplar İçi	777.223	741.946	.645		
	Toplam	778.293	744.526			

Tablo 4.68’de öğretmen adaylarının öğrenim gördükleri sınıf kademesinin dijital güvenlik düzeyleri üzerine etkisini incelemek amacıyla tek faktörlü varyans analizi yürütülmüştür. Analiz sonucunda öğrenim gördükleri kademe arasında anlamlı bir fark olmadığı tespiti yapılmıştır ($F(3,1151) = 1.334, p > .05$).

4.3.2.6. Dijital ticaret düzeyinin Sınıf düzeyine göre farkı

Tablo 4.69

Dijital Ticaret Seviyelerinin Sınıf Düzeyine Göre Kişi Sayısı, Ortalama ve Standart Sapmaları

Bağımlı Değişken	Sınıf Düzeyi	N	M	Standart Sapma
Dijital Ticaret	1	319	3.4232	.85267
	2	286	3.4977	.77522
	3	266	3.3622	.75984
	4	284	3.4413	.81172
	Toplam	1155	3.4320	.80322

Tablo 4.69’ da öğretmen adaylarının Sınıf Düzeyine göre kişi sayıları, ortalamaları ve standart sapmaları verilmiştir. Bu verilere bakıldığında öğretmen adaylarının dijital ticaret seviyelerinin toplam ortalamasının 3.43 olduğu görülmektedir (N=1155).

Tablo 4.70

Dijital Ticaret Seviyelerinin Sınıf Düzeylerine Göre Karşılaştırılması

	Varyans Kaynağı	Kareler Toplamı	sd	Kareler Ortalaması	F	p
Dijital Ticaret	Gruplar Arası	4.051	2.580	1.350	1.346	.258
	Gruplar İçi	1154.412	741.946	1.003		
	Toplam	1158.463	744.526			

Tablo 4.70’de gerçekleştirilen tek yönlü faktörlü varyans analizi ile öğretmen adaylarının buldukları sınıf kademesi ile dijital ticaret düzeyleri arasında anlamlı bir fark olup olmadığı

tespit edilmeye çalışılmıştır. Analiz sonucunda öğrenim gördükleri kademe arasında anlamlı bir fark bulunamamıştır ($F(3,1151) = 1.346, p > .05$).

4.3.2.7. Dijital erişim düzeyinin Sınıf düzeyine göre farkı

Tablo 4.71

Dijital Erişim Seviyelerinin Sınıf Düzeyine Göre Kişi Sayısı, Ortalama ve Standart Sapmaları

Bağımlı Değişken	Sınıf Düzeyi	N	M	Standart Sapma
Dijital Erişim	1	319	3.7858	.89358
	2	286	3.7925	.83846
	3	266	3.9298	.76840
	4	284	3.9225	.77218
	Toplam	1155	3.8543	.82472

Tablo 4.71'deki veriler incelendiğinde öğretmen adaylarının dijital erişim düzeylerinin Sınıf kademesi arttıkça arttığı görülmektedir. Yine tablodaki verilere bakılarak dijital erişim seviyelerinin sadece 1. Sınıf(N=319, M=3.78) ve 2.sınıfta(N=286, M=3.79) toplam ortalamanın altında kaldığı söylenebilir.

Tablo 4.72

Dijital Erişim Seviyelerinin Sınıf Düzeylerine Göre Karşılaştırılması

	Varyans Kaynağı	Kareler Toplamı	sd	Kareler Ortalaması	F	p	Eta Kare
Dijital Erişim	Gruplar Arası	5.428	1.809	.860	2.672	.046*	.007
	Gruplar İçi	779.483	.677	.645			
	Toplam	784.911					

Tablo 4.72'de öğretmen adaylarının öğrenim gördükleri Sınıf kademesinin dijital erişim düzeyleri üzerine etkisini incelemek amacıyla tek faktörlü varyans analizi yürütülmüştür. Analiz sonucunda öğrenim gördükleri kademe arasında anlamlı bir fark olduğu görülmektedir. ($F(3,1151) = 2.672, p > .05, \eta^2 = .007$). Hangi kademeler arasında fark olduğunu gösteren post-hoc sonuçları Tablo 4.83' te gösterilmiştir.

Tablo 4.73

Dijital Erişim Altı Boyutunda Anlamlı Farklılaşma Sınıf Düzeyi- Post Hoc

Bağımlı Değişken	(I) Sınıf Düzeyi	(J) Sınıf Düzeyi	Ortalamaların Farkı	p
Dijital Erişim	1	2	-.00675	1.000
		3	-.14404	.151
		4	-.13675	.175
	2	1	.00675	1.000
		3	-.13728	.205
		4	-.12999	.235
	3	1	.14404	.151
		2	.13728	.205
		4	.00729	1.000
	4	1	.13675	.175
		2	.12999	.235
		3	-.00729	1.000

(1.Sınıf(M=3.78,SD=.89), 2.Sınıf(M=3.79,SD=.83),3.sınıf(M=3.93,SD=.76),4.Sınıf(M=3.92,SD=.77))

Bölümler arası farkları detaylı incelemek amacıyla yürütülen Post-Hoc analiz sonuçlarına bakıldığında ise Sınıf Düzeyi arasında anlamlı bir farka rastlanmamıştır.

4.3.2.8 Dijital etik düzeyinin Sınıf düzeyine göre farkı

Tablo 4.74

Dijital Etik Seviyelerinin Sınıf Düzeyine Göre Kişi Sayısı, Ortalama ve Standart Sapmaları

Bağımlı Değişken	Sınıf Düzeyi	N	M	Standart Sapma
Dijital Etik	1	319	3.9739	.79899
	2	286	3.8869	.73776
	3	266	3.9449	.74752
	4	284	3.9566	.65364
	Toplam	1155	3.9414	.73791

Tablo 4.74'e bakıldığında toplam ortalamasının(N=1155) 3.94 olduğu görülmektedir. Ayrıca dijital etik düzeyleri 1.Sınıf ve 4.sınıfta ortalamasının üstüne çıkmıştır

Tablo 4.75

Dijital Etik Seviyelerinin Sınıf Düzeylerine Göre Karşılaştırılması

	Varyans Kaynağı	Kareler Toplamı	sd	Kareler Ortalaması	F	p
Dijital Etik	Gruplar Arası	1.253	1.809	.418	.767	.513
	Gruplar İçi	627.116	.677	.545		
	Toplam	628.369				

Tablo 4.75'te dijital etik düzeyi ile sınıf kademesi arasında anlamlı bir fark olup olmadığını tespit etmek için yapılan tek faktörlü varyans analizi sonucuna göre öğretmen adaylarını buldukları sınıf kademesi ile dijital etik düzeyleri arasında anlamlı bir fark yoktur ($F(3,1151) = .767, p > .05$).

4.3.2.9. Dijital sağlık düzeyinin sınıf düzeyine göre farkı

Tablo 4.76

Dijital Sağlık Seviyelerinin Sınıf Düzeyine Göre Kişi Sayısı, Ortalama ve Standart Sapmaları

Bağımlı Değişken	Sınıf Düzeyi	N	M	Standart Sapma
Dijital Sağlık	1	319	3.1108	.90127
	2	286	3.1807	.92591
	3	266	3.1867	.91655
	4	284	3.0974	.83662
	Toplam	1155	3.1423	.89538

Tablo 4.76'ya bakıldığında toplam ortalamasının(N=1155) 3.14 olduğu görülmektedir. Ayrıca dijital sağlık ortalamalarının 4.Sınıf ve 1.sınıfta ortalamasının altında olduğu tespit edilmiştir.

Tablo 4.77

Dijital Sağlık Seviyelerinin Sınıf Düzeylerine Göre Karşılaştırılması

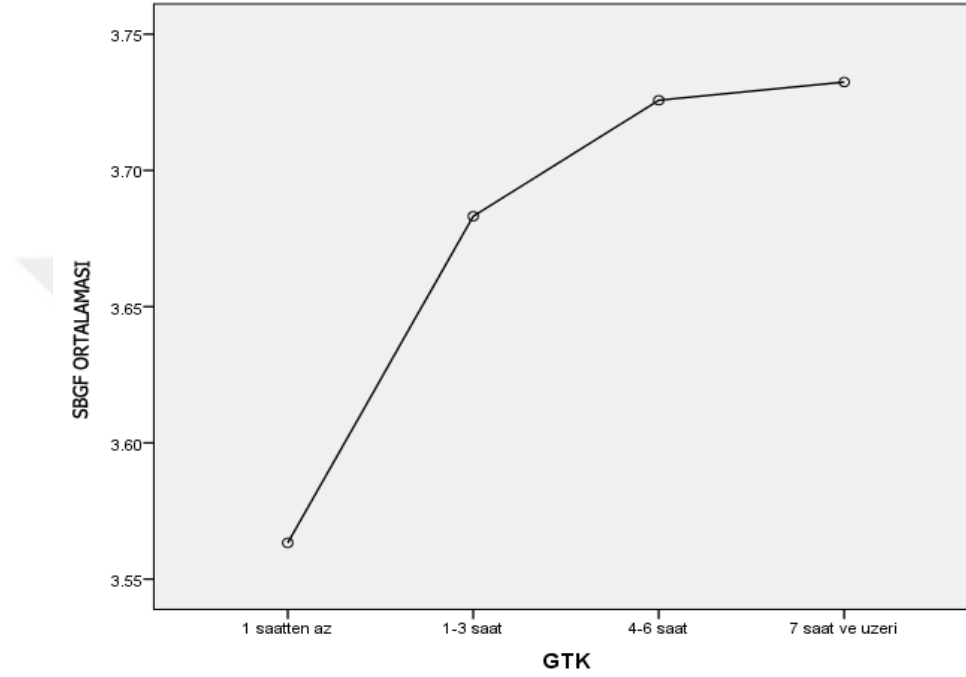
	Varyans Kaynağı	Kareler Toplamı	sd	Kareler Ortalaması	F	p
Dijital Sağlık	Gruplar Arası	1.835	1.809	.612	.762	.515
	Gruplar İçi	923.339	.677	.802		
	Toplam	925.174				

Tablo 4.77'de Dijital sağlık düzeyi ile sınıf kademesi arasındaki farkın anlamlı olup olmadığını tespit etmek için yapılan tek faktörlü varyans analizi sonucuna göre, öğretmen adaylarını buldukları sınıf kademesi ile dijital sağlık düzeyleri arasında anlamlı bir fark yoktur ($F(3,1151) = .767, p > .05$).

4.4 Değişkenlerin Günlük Toplam Teknoloji Kullanımına Göre Karşılaştırılması - Tek Yönlü Varyans Analizi (ANOVA)

4.4.1. Siber bilgi güvenliği farkındalığının günlük toplam teknoloji kullanımına göre karşılaştırılması

Şekil 4.5'te yer alan grafiğe göre öğretmen adaylarının Siber Bilgi Güvenliği Farkındalığı puanlarının GTK süreleri ile doğru orantılı olarak arttığını söylemek mümkündür.



Şekil 4.5. GTK Süresine Göre Siber Bilgi Güvenliği Farkındalık Ortalamalarının Grafiği

Tablo 4.78

Siber Bilgi Güvenlik Farkındalığının Günlük Teknoloji Kullanımı Süresine Göre; Kişi Sayısı, Ortalama ve Standart Sapmaları

Bağımlı Değişken	GTK Süresi(J)	N	M	Standart Sapma
SBGF	1 saatten az	39	3.5633	.60100
	1-3 saat	463	3.6832	.66779
	4-6 saat	509	3.7257	.62314
	7 saat ve üzeri	144	3.7324	.61971
	Toplam	1155	3.7040	.64039

Tablo 4.78' teki günlük teknoloji kullanımı oranları incelendiğinde yığılmanın 1-3 saat ve 4-6 saat aralığında olduğu görülmektedir. 1 saatten az kullanan kişi sayısı ise oldukça azdır.

Tablo 4.79

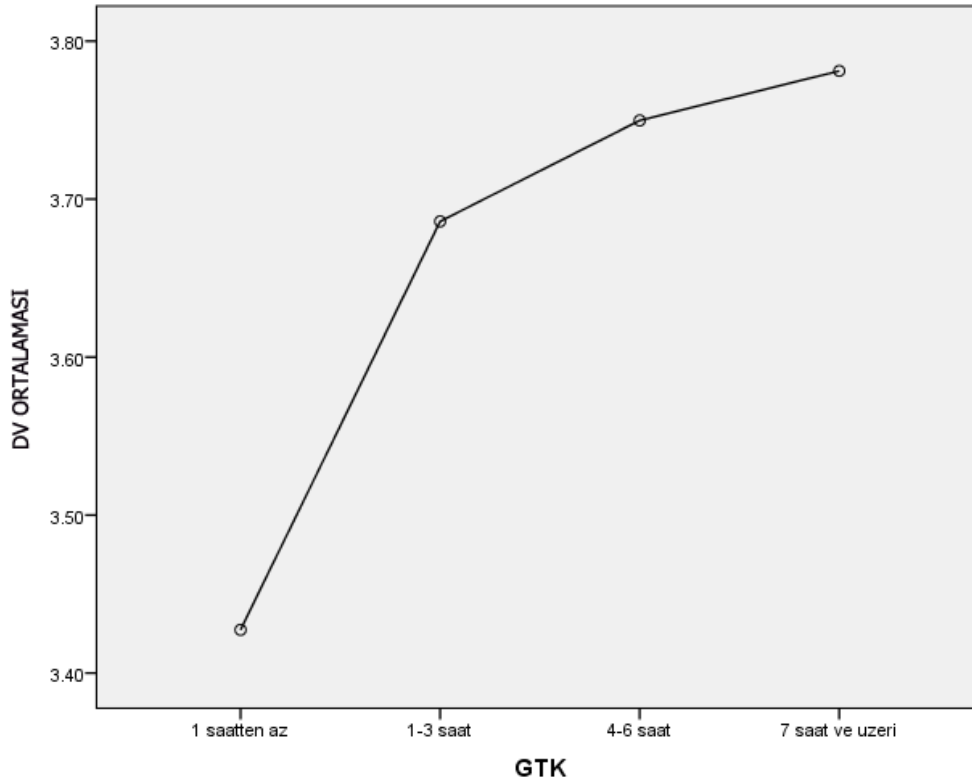
Siber Bilgi Güvenlik Farkındalığının Günlük Teknoloji Kullanımına Karşılaştırılması

	Varyans Kaynağı	Kareler Toplamı	sd	Kareler Ortalaması	F	p
SBGF	Gruplar Arası	1.330	7	.443	1.081	.356
	Gruplar İçi	471.930	1147	.410		
	Toplam	473.260	1154			

Tablo 4.79' da öğretmen adaylarının günlük toplam teknoloji kullanımının siber bilgi güvenliği farkındalığı üzerine etkisini incelemek amacıyla gerçekleştirilen tek faktörlü varyans analizi sonucunda öğrenim gördükleri kademe ile Siber Bilgi Güvenliği Farkındalığı arasında anlamlı bir fark bulunamamıştır ($F(3,1151) = 1.081, p > .05$).

4.4.2. Dijital vatandaşlık düzeyinin günlük toplam teknoloji kullanımına göre karşılaştırılması

Şekil 4.6' daki grafikte GTK süreleri ile dijital vatandaşlık düzeyleri ortalamalarına yer verilmiştir. Grafiğe göre öğretmen adaylarının GTK süresi arttıkça dijital vatandaşlık puanları da artmıştır.



Şekil 4.6. GTK Süresine Göre Dijital Vatandaşlık Düzeyi Ortalamalarının Grafiği

Tablo 4.80

Dijital Vatandaşlık Seviyelerinin Günlük Teknoloji Kullanımı Sürelerine Göre; Kişi Sayısı, Ortalama ve Standart Sapmaları

Bağımlı Değişken	GTK Süresi(J)	N	M	Standart Sapma
Dijital Vatandaşlık	1 saatten az	39	3.4274	.54059
	1-3 saat	463	3.6859	.48684
	4-6 saat	509	3.7498	.46827
	7 saat ve üzeri	144	3.7811	.46840
	Toplam	1155	3.7172	.48211

(* $p < .05$, 1saatten az($M=3.43$, $SD=.54$), 1-3 saat($M=3.69$, $SD=.48$), 4-6 saat($M=3.75$, $SD=.46$), 7 saat ve üzeri($M=3.78$, $SD=.47$))

Tablo 4.80'deki veriler incelendiğinde dijital vatandaşlık düzeyleri bakımından en yüksek ortalamayı 3.78 ile 7 saat ve üzeri GTK süresine sahip öğretmen adayları oluşturmaktadır. Yine bu verilere bakılarak GTK süreleri arttıkça dijital vatandaşlık ortalamalarının da arttığı söylenebilir

Tablo 4.81

Dijital Vatandaşlık Seviyelerinin Günlük Teknoloji Kullanımına Göre Karşılaştırılması

	Varyans Kaynağı	Kareler Toplamı	sd	Kareler Ortalaması	F	p	Eta Kare
Dijital Vatandaşlık	Gruplar Arası	4.859	3	1.620	7.078	.000	.018
	Gruplar İçi	263.369	1151	.229			
	Toplam	268.228	1154				

Gerçekleştirilen tek faktörlü varyans analizi ile öğretmen adaylarının günlük toplam teknoloji kullanımının dijital vatandaşlık düzeyleri üzerine etkisi incelenmiştir. Yapılan analiz sonucunda öğretmen adaylarının günlük teknoloji kullanım süreleri ile dijital vatandaşlık düzeyleri arasında anlamlı fark bulunmuştur. ($F(3,1151) = 7.078$, $p < .05^*$). GTK süreleri arasında anlamlı fark Tablo 4.81'de verilmişken, farklılaşmaların olduğu GTK süreleri gösteren post hoc veri analizi ise Tablo 4.82'de verilmiştir.

Tablo 4.82

Dijital Vatandaşlık Düzeyi Bakımından Anlamlı Farklılaşma Olan GTK Süreleri- Post Hoc

Bağımlı Değişken	GTK Süresi(I)	(J)GTK Süresi	Ortalamaların Farkı	p
Dijital Vatandaşlık	1 saatten az	1-3 saat	-.25856*	.007
		4-6 saat	-.32243*	.000
		7 saat ve üzeri	-.35379*	.000
	1-3 saat	1 saatten az	.25856*	.007
		4-6 saat	-.06387	.161
		7 saat ve üzeri	-.09524	.158
	4-6 saat	1 saatten az	.32243*	.000
		1-3 saat	.06387	.161
		7 saat ve üzeri	-.03137	.899
	7 saat ve üzeri	1 saatten az	.35379*	.000
		1-3 saat	.09524	.158
		4-6 saat	.03137	.899

(1.Sınıf(M=3.40,SD=73), 2.sınıf(M=3.41,SD=74),3.Sınıf(M=3.46,SD=77),4.Sınıf(M=3.60,SD=75))

Tablo 4.82' de GTK süreleri farklarını detaylı incelemek ve farklılaşmaların hangi bağımsız değişkenler arasında olduğunu tespit etmek amacı ile yürütülen Post-Hoc analiz sonuçları yer almaktadır. Bu sonuçlara göre;

- GTK süresi 1 saatten az olan öğretmen adayları ile 1-3 saat, 4-6 saat ve 7 saat üzeri GTK süresi olan öğretmen adayları puanları arasında anlamlı bir fark bulunmuştur.
- GTK süresi 1-3 saat olan öğretmen adayları ile 1 saatten az GTK süresi olan öğretmen adayları puanları arasında anlamlı bir fark bulunmuşken, GTK süresi 1-3 saat olan ile 4-6 saat ve 7 saat üzeri olan öğretmen adayları ile anlamlı bir fark olmadığı görülmüştür.
- GTK süresi 4-6 saat olan öğretmen adayları ile 1 saatten az GTK süresi olan öğretmen adayları puanları arasında anlamlı bir fark bulunmuşken, GTK süresi 4-6 saat olan ile 1-3 saat ve 7 saat üzeri olan öğretmen adayları ile anlamlı sayılabilecek bir fark tespit edilememiştir.
- GTK süresi 7 saat üzeri olan öğretmen adayları ile 1 saatten az GTK süresi olan öğretmen adayları puanları arasında anlamlı bir fark bulunmuşken, GTK süresi 7 saat üzeri olan ile 1-3 saat ve 4-6 saat olan öğretmen adayları ile anlamlı bir fark tespit edilememiştir.

4.4.2.1. Dijital okuryazarlık alt boyutunun günlük toplam teknoloji kullanımına göre karşılaştırılması

Tablo 4.83

Dijital Okuryazarlık Seviyelerinin Günlük Teknoloji Kullanımı Sürelerine Göre; Kişi Sayısı, Ortalama ve Standart Sapmaları

Bağımlı Değişken	GTK Süresi	N	M	Standart Sapma
Dijital Okuryazarlık	1 saatten az	39	3.2479	.75304
	1-3 saat	463	3.4226	.76460
	4-6 saat	509	3.4941	.74129
	7 saat ve üzeri	144	3.5741	.73480
	Toplam	1155	3.4671	.75212

Tablo 4.83'deki verilere göre GTK sürelerine göre Dijital okuryazarlık ortalamaları 3.24 ile 3.57 aralığındadır. Ayrıca ortalamanın GTK süresi arttıkça arttığı da görülmektedir.

Tablo 4.84

Dijital Okuryazarlık Düzeyinin Günlük Teknoloji Kullanımına Göre Karşılaştırılması

	Varyans Kaynağı	Kareler Toplamı	sd	Kareler Ortalaması	F	p	Eta Kare
Dijital Okuryazarlık	Gruplar Arası	4.810	3	1.603	2.848	.036*	.007
	Gruplar İçi	647.995	1151	.563			
	Toplam	652.805	1154				

Tablo 4.84 öğretmen adaylarının günlük toplam teknoloji kullanımının dijital okuryazarlık düzeyleri üzerine etkisini incelemek amacıyla yapılan tek faktörlü varyans analizi sonucunda öğretmen adaylarının GTK süreleri ile dijital okur yazarlık düzeyleri arasında istatistiksel olarak anlamlı bir fark bulunmuştur. ($F(3,1151) = 2.848, p < .05, n^2 = .007$).

Tablo 4.85

Dijital Okuryazarlık Düzeyi Bakımından Anlamlı Farklılaşma Olan GTK Süreleri- Post Hoc

Bağımlı Değişken	(I)GTK Süresi	(J)GTK Süresi	Ortalamaların Farkı	p
Dijital Okuryazarlık	1 saatten az	1-3 saat	-.17474	.502
		4-6 saat	-.24624	.198
		7 saat ve üzeri	-.32621	.076
	1-3 saat	1 saatten az	.17474	.502
		4-6 saat	-.07150	.448
		7 saat ve üzeri	-.15147	.149
	4-6 saat	1 saatten az	.24624	.198
		1-3 saat	.07150	.448
		7 saat ve üzeri	-.07997	.672
	7 saat ve üzeri	1 saatten az	.32621	.076
		1-3 saat	.15147	.149
		4-6 saat	.07997	.672

(*p<.05, 1saatten az(M=3.24, SD=.75) , 1-3 saat(M=3.42, SD=.76), 4-6 saat(M=3.49, SD=.74), 7 saat ve üzeri(M=3.57, SD=.73))

Tablo 4.85'te farklılaşmanın kaynağını tespit etmek için gerçekleştirilen Post-Hoc analiz sonuçlarına yer verilmiştir.

4.4.2.2. Dijital yasa alt boyutunun günlük toplam teknoloji kullanımına göre karşılaştırılması

Tablo 4.86

Dijital Yasa Seviyelerinin Günlük Teknoloji Kullanımı Sürelerine Göre Kişi Sayısı, Ortalama ve Standart Sapmaları

Bağımlı Değişken	GTK Süresi	N	M	Standart Sapma
Dijital Yasa	1 saatten az	39	3.8782	.86957
	1-3 saat	463	4.2138	.81195
	4-6 saat	509	4.2146	.79999
	7 saat ve üzeri	144	4.1962	.76309
	Toplam	1155	4.2006	.80399

Tablo 4.86'da yer alan veriler incelendiğinde dijital yasa puanı en yüksek olan aralığın 4-6 saat olduğu görülmektedir. Yine tablodaki verilere bakılarak puanların ortalamaya yakın olduğunu da söylemek mümkündür.

Tablo 4.87

Dijital Yasa Düzeyinin Günlük Teknoloji Kullanımına Göre Karşılaştırılması

	Varyans Kaynağı	Kareler Toplamı	sd	Kareler Ortalaması	F	p
Dijital Yasa	Gruplar Arası	4.238	3	1.413	2.192	.087
	Gruplar İçi	741.699	1151	.644		
	Toplam	745.937	1154			

Tablo 4.87’de öğretmen adaylarının GTK’nın dijital yasa farkındalığı üzerine etkisini incelemek amacıyla tek faktörlü varyans analizi yürütülmüştür. Analiz sonucunda GTK süreleri ile dijital yasa düzeyleri arasında istatistiksel olarak anlamlı bir fark olmadığı tespit edilmiştir. ($F(3,1151) = 2.192, p > .05$).

4.4.2.3. Dijital hak ve sorumluluk alt boyutunun günlük toplam teknoloji kullanımına göre karşılaştırılması

Tablo 4.88

Dijital Hak ve Sorumluluk Seviyelerinin Günlük Teknoloji Kullanımı Sürelerine Göre Kişi Sayısı, Ortalama ve Standart Sapmaları

Bağımlı Değişken	GTK Süresi	N	M	Standart Sapma
Dijital Hak ve Sorumluluk	1 saatten az	39	3.7179	.87955
	1-3 saat	463	3.9471	.73112
	4-6 saat	509	3.9980	.70134
	7 saat ve üzeri	144	4.0226	.77601
	Toplam	1155	3.9712	.73053

Tablo 4.88’deki verilere göre GTK süresi arttıkça dijital hak ve sorumluluk düzeyi puanları artmıştır. Yine tablodaki verilere bakılarak ortalamaların 3.71 ile 4.02 arasında olduğu görülmektedir.

Tablo 4.89

Dijital Hak ve Sorumluluk Düzeyinin Günlük Teknoloji Kullanımına Göre Karşılaştırılması

		Varyans	Kareler	sd	Kareler	F	p
		Kaynağı	Toplamı		Ortalaması		
Dijital Hak ve Sorumluluk	Gruplar Arası		3.517	3	1.172		
	Gruplar İçi		612.338	1151	.532	2.204	.086
	Toplam		615.855	1154			

Tablo 4.89 öğretmen adaylarının günlük toplam teknoloji kullanımının dijital hak ve sorumluluk düzeyleri üzerine etkisini incelemek amacıyla tek faktörlü varyans analizi yürütülmüştür. Analiz sonucunda öğretmen adaylarının GTK süreleri ile dijital hak ve sorumluluk düzeyleri arasında istatistiksel olarak anlamlı bir fark olmadığı görülmüştür ($F(3,1151) = 2.204, p > .05$).

4.4.2.4. Dijital iletişim alt boyutunun günlük toplam teknoloji kullanımına göre karşılaştırılması

Tablo 4.90

Dijital İletişim Seviyelerinin Günlük Teknoloji Kullanımı Sürelerine Göre; Kişi Sayısı, Ortalama ve Standart Sapmaları

Bağımlı Değişken	GTK Süresi	N	M	Standart Sapma
Dijital İletişim	1 saatten az	39	3.1154	.85233
	1-3 saat	463	3.6825	.80003
	4-6 saat	509	3.8571	.80450
	7 saat ve üzeri	144	3.9757	.81952
	Toplam	1155	3.7768	.82124

Tablo 4.90'deki betimsel istatistik sonuçlara göre öğretmen adaylarının dijital erişim düzeyi ortalamaları GTK süreleri arttıkça artmıştır. .

Tablo 4.91

Dijital İletişim Düzeyinin Günlük Teknoloji Kullanımına Göre Karşılaştırılması

	Varyans Kaynağı	Kareler Toplamı	sd	Kareler Ortalaması	F	p	Eta Kare
Dijital İletişim	Gruplar Arası	30.154	3	10.051	15.464	.000*	.039
	Gruplar İçi	748.139	1151	.650			
	Toplam	778.293	1154				

Tablo 4.91’de gerçekleştirilen tek faktörlü varyans analizi ile öğretmen adaylarının günlük toplam teknoloji kullanımının dijital iletişim düzeyleri üzerine etkisi incelenmiştir. Analiz sonucunda GTK süresi ile dijital iletişim düzeyleri arasında istatistiksel olarak anlamlı bir fark olduğu görülmüştür ($F(3,1151) = 15.464, p < .05, \eta^2 = .039$). Farklılaşmayı gösteren istatistiksel sonuçlar Tablo 4.92’de gösterilmiştir.

Tablo 4.92

Dijital İletişim Düzeyi Bakımından Anlamlı Farklılaşma Olan GTK Süreleri- Post Hoc

Bağımlı Değişken	(I) GTK Süresi	(J) GTK Süresi	Ortalamaların Farkı	p
Dijital İletişim	1 saatten az	1-3 saat	-.56712*	.000
		4-6 saat	-.74169*	.000
		7 saat ve üzeri	-.86031*	.000
	1-3 saat	1 saatten az	.56712*	.000
		4-6 saat	-.17457*	.004
		7 saat ve üzeri	-.29319*	.001
	4-6 saat	1 saatten az	.74169*	.000
		1-3 saat	.17457*	.004
		7 saat ve üzeri	-.11862	.403
	7 saat ve üzeri	1 saatten az	.86031*	.000
		1-3 saat	.29319*	.001
		4-6 saat	.11862	.403

(* $p < .05$, 1saatten az($M=3.11, SD=.85$), 1-3 saat($M=3.68, SD=.80$), 4-6 saat($M=3.85, SD=.80$), 7 saat ve üzeri($M=3.97, SD=.81$))

Tablo 4.92’de yer post hoc analiz sonuçlarına göre;

- GTK süresi 1 saatten az olan öğretmen adayları ile 1-3 saat, 4-6 saat ve 7 saat üzeri GTK süresi olan öğretmen adayları puanları arasında anlamlı bir fark bulunmuştur.
- GTK süresi 1-3 saat olan öğretmen adayları ile 1 saatten az, 4-6 saat ve 7 saat üzeri GTK süresi olan öğretmen adayları puanları arasında anlamlı bir fark olduğu görülmüştür.

- GTK süresi 4-6 saat olan öğretmen adayları ile 1 saatten az ve 1-3 saat GTK süresi olan öğretmen adayları puanları arasında anlamlı bir fark tespit edilmişken, GTK süresi 4-6 saat olan ile 7 saat üzeri olan öğretmen adayları ile istatistiksel olarak anlamlı bir fark bulunamamıştır.
- GTK süresi 7 saat üzeri olan öğretmen adayları ile 1 saatten az ve 1-3 saat GTK süresi olan öğretmen adayları puanları arasında anlamlı bir fark olduğu görülürken, GTK süresi 7 saat üzeri olan ile 4-6 saat olan öğretmen adayları ile istatistiksel olarak anlamlı bir fark olmadığı görülmüştür.

4.4.2.5. Dijital güvelik alt boyutunun günlük toplam teknoloji kullanımına göre karşılaştırılması

Tablo 4.93

Dijital Güvenlik Seviyelerinin Günlük Teknoloji Kullanımı Sürelerine Göre; Kişi Sayısı, Ortalama ve Standart Sapmaları

Bağımlı Değişken	GTK Süresi	N	M	Standart Sapma
Dijital Güvenlik	1 saatten az	39	3.1538	.96077
	1-3 saat	463	3.4132	.80856
	4-6 saat	509	3.4519	.78294
	7 saat ve üzeri	144	3.4977	.80209
	Toplam	1155	3.4320	.80322

Tablo 4.93'teki betimsel istatistiksel sonuçlar incelendiğinde dijital güvenlik ortalamalarının 3.15 ile 3.49 aralığında olduğu görülmektedir.

Tablo 4.94

Dijital Güvenlik Düzeyinin Günlük Teknoloji Kullanımına Göre Karşılaştırılması

	Varyans Kaynağı	Kareler Toplamı	sd	Kareler Ortalaması	F	p
Dijital Güvenlik	Gruplar Arası	4.002	3	1.334	2.074	.102
	Gruplar İçi	740.523	1151	.643		
	Toplam	744.526	1154			

Öğretmen adaylarının günlük toplam teknoloji kullanımının dijital güvenlik düzeyleri üzerine etkisini incelemek amacıyla tek faktörlü varyans analizi gerçekleştirilmiştir. Analiz sonucunda GTK süresi ile dijital güvenlik düzeyi arasında istatistiksel olarak anlamlı bir fark olmadığı görülmüştür ($F(3,1151) = 2.074, p < .05$).

4.4.2.6. Dijital ticaret alt boyutunun günlük toplam teknoloji kullanımına göre karşılaştırılması

Tablo 4.95

Dijital Ticaret Seviyelerinin Günlük Teknoloji Kullanımı Sürelerine Göre; Kişi Sayısı, Ortalama ve Standart Sapmaları

Bağımlı Değişken	GTK Süresi	N	M	Standart Sapma
Dijital Ticaret	1 saatten az	39	3.5897	.82880
	1-3 saat	463	3.5054	1.05154
	4-6 saat	509	3.7210	.95794
	7 saat ve üzeri	144	3.9074	.96597
	Toplam	1155	3.6534	1.00193

Tablo 4.95'teki betimsel istatistik sonuçlara göre öğretmen adaylarının dijital ticaret düzeyi ortalamaları 1 saatten az ve 1-3 saat aralığında toplam ortalamasının altında kalmıştır.

Tablo 4.96

Dijital Ticaret Düzeyinin Günlük Teknoloji Kullanımına Göre Karşılaştırılması

	Varyans Kaynağı	Kareler Toplamı	sd	Kareler Ortalaması	F	p	Eta Kare
Dijital Ticaret	Gruplar Arası	21.918	3	7.306	7.399	.000*	.019
	Gruplar İçi	1136.545	1151	.987			
	Toplam	1158.463	1154				

Tablo 4.96'da gerçekleştirilen tek faktörlü varyans analizi ile öğretmen adaylarının günlük toplam teknoloji kullanımının dijital ticaret düzeyleri üzerine etkisi incelenmiştir. Yapılan analiz sonuçlarına göre öğretmen adaylarının GTK süresi ile dijital ticaret düzeyleri arasında istatistiksel olarak anlamlı bir fark bulunmuştur ($F(3,1151) = 7.399, p < .05, n^2 = .019$). Farklılaşmanın olduğu GTK sürelerini detaylı incelemek için gerçekleştirilen post hoc analizi sonucu Tablo 4.97' te gösterilmiştir.

Tablo 4.97

Dijital Ticaret Düzeyi Bakımından Anlamlı Farklılaşma Olan GTK Süreleri- Post Hoc

Bağımlı Değişken	(I)GTK Süresi	(J) GTK Süresi	Ortalamaların Farkı	p
Dijital Ticaret	1 saatten az	1-3 saat	.08434	.957
		4-6 saat	-.13128	.857
		7 saat ve üzeri	-.31766	.288
	1-3 saat	1 saatten az	-.08434	.957
		4-6 saat	-.21562*	.004*
		7 saat ve üzeri	-.40201*	.000*
	4-6 saat	1 saatten az	.13128	.857
		1-3 saat	.21562*	.004*
		7 saat ve üzeri	-.18639	.193
	7 saat ve üzeri	1 saatten az	.31766	.288
		1-3 saat	.40201*	.000*
		4-6 saat	.18639	.193

(*p<.05, 1saatten az(M=3.59, SD=.83) , 1-3 saat(M=3.50, SD=1.00), 4-6 saat(M=3.72, SD=.95), 7 saat ve üzeri(M=3.90, SD=.97))

Tablo 4.97'de yer olan post hoca analiz sonuçları incelendiğinde;

- GTK süresi 1 saatten az olan öğretmen adayları ile 1-3 saat, 4-6 saat ve 7 saat üzeri GTK süresi olan öğretmen adayları puanları arasında anlamlı bir fark bulunamamıştır.
- GTK süresi 1-3 saat olan öğretmen adayları ile 4-6 saat ve 7 saat üzeri GTK süresi olan öğretmen adayları puanları arasında anlamlı bir fark bulunmuşken, GTK süresi 1-3 saat olan öğretmen adayları ile 1 saatten az olan öğretmen adayları puanları arasında istatistiksel olarak anlamlı bir fark bulunamamıştır.
- GTK süresi 4-6 saat olan öğretmen adayları ile 1-3 saat GTK süresi olan öğretmen adayları puanları arasında anlamlı bir fark bulunmuşken, GTK süresi 4-6 saat olan ile 1 saatten az ve 7 saat üzeri olan öğretmen adayları ile anlamlı bir fark olmadığı tespit edilmiştir.
- GTK süresi 7 saat üzeri olan öğretmen adayları ile 1-3 saat GTK süresi olan öğretmen adayları puanları arasında anlamlı bir fark bulunmuşken, GTK süresi 1 saatten az ve 7 saat üzeri olan öğretmen adayları ile anlamlı bir fark bulunamamıştır.

4.4.2.7 Dijital erişim alt boyutunun günlük toplam teknoloji kullanımına göre karşılaştırılması

Tablo 4.98

Dijital Erişim Seviyelerinin Günlük Teknoloji Kullanımı Sürelerine Göre; Kişi Sayısı, Ortalama ve Standart Sapmaları

Bağımlı Değişken	Bölüm(J)	N	M	Standart Sapma
Dijital Erişim	1 saatten az	39	3.2222	.97433
	1-3 saat	463	3.7898	.82439
	4-6 saat	509	3.9175	.79241
	7 saat ve üzeri	144	4.0093	.80591
	Toplam	1155	3.8543	.82472

(* $p < .05$, 1saatten az($M=3.22$, $SD=.97$), 1-3 saat($M=3.78$, $SD=.82$), 4-6 saat($M=3.91$, $SD=.79$), 7 saat ve üzeri($M=4.80$, $SD=.81$))

Tablo 4.98'deki betimsel istatistik sonuçları incelendiğinde GTK süresine göre dijital erişim yönünden en düşük ortalamanın 1-3 saat arası teknoloji kullanan öğretmenlere ait olduğu görülmüştür.

Tablo 4.99

Dijital Erişim Düzeyinin Günlük Teknoloji Kullanımına Göre Karşılaştırılması

	Varyans Kaynağı	Kareler Toplamı	sd	Kareler Ortalaması	F	p	Eta Kare
Dijital Erişim	Gruplar Arası	22.999	3	7.666	11.581	.000*	.029
	Gruplar İçi	761.912	1151	.662			
	Toplam	784.911	1154				

Tablo 4.99'da öğretmen adaylarının günlük toplam teknoloji kullanımının dijital erişim düzeyleri üzerine etkisini incelemek amacıyla yürütülen tek faktörlü varyans analizi sonucu verilmiştir. Yapılan analiz sonucunda GTK süresi ile dijital ticaret düzeyleri arasında istatistiksel olarak anlamlı bir fark olduğu görülmüştür. ($F(3,1151) = 11.581, p < .05$).

Tablo 4.100

Dijital Erişim Düzeyi Bakımından Anlamlı Farklılaşma Olan GTK Süreleri- Post Hoc

Bağımlı Değişken	(I) GTK Süresi	(J) GTK Süresi	Ortalamaların Farkı	p
Dijital Erişim	1 saatten az	1-3 saat	-.56755*	.000
		4-6 saat	-.69526*	.000
		7 saat ve üzeri	-.78704*	.000
	1-3 saat	1 saatten az	.56755*	.000
		4-6 saat	-.12771	.070
		7 saat ve üzeri	-.21948*	.025
	4-6 saat	1 saatten az	.69526*	.000
		1-3 saat	.12771	.070
		7 saat ve üzeri	-.09177	.630
	7 saat ve üzeri	1 saatten az	.78704*	.000
		1-3 saat	.21948*	.025
		4-6 saat	.09177	.630

Tablo 4.100'da verilen günlük toplam teknoloji kullanım süreleri farklarını detaylı incelemek amacıyla yürütülen Post-Hoc analiz sonuçları yer almaktadır. Bu sonuçlara göre;

- GTK süresi 1 saatten az olan öğretmen adayları ile 1-3 saat, 4-6 saat ve 7 saat üzeri GTK süresi olan öğretmen adayları puanları arasında anlamlı bir fark bulunmuştur.
- GTK süresi 1-3 saat olan öğretmen adayları ile 1 saatten az ve 7 saat üzeri GTK süresi olan öğretmen adayları puanları arasında anlamlı bir fark bulunmuşken, GTK süresi 1-3 saat olan öğretmen adayları ile 4-6 saat olan öğretmen adayları puanları arasında istatistiksel olarak anlamlı bir fark bulunamamıştır.
- GTK süresi 4-6 saat olan öğretmen adayları ile 1 saatten az GTK süresi olan öğretmen adayları puanları arasında anlamlı bir fark bulunmuşken, GTK süresi 4-6 saat olan ile 1-3 saat ve 7 saat üzeri olan öğretmen adayları ile anlamlı bir fark bulunamamıştır.
- GTK süresi 7 saat üzeri olan öğretmen adayları ile 1 saatten az ve 1-3 saat GTK süresi olan öğretmen adayları puanları arasında anlamlı bir fark bulunmuşken, GTK süresi 7 saat üzeri olan öğretmen adayları ile 4-6 saat olan öğretmen adayları ile anlamlı bir fark bulunamamıştır.

4.4.2.8. Dijital etik alt boyutunun günlük toplam teknoloji kullanımına göre karşılaştırılması

Tablo 4.101

Dijital Etik Seviyelerinin Günlük Teknoloji Kullanımı Sürelerine Göre; Kişi Sayısı, Ortalama ve Standart Sapmaları

Bağımlı Değişken	Bölüm(J)	N	M	Standart Sapma
Dijital Etik	1 saatten az	39	3.7179	.72764
	1-3 saat	463	3.9366	.74814
	4-6 saat	509	3.9980	.72437
	7 saat ve üzeri	144	3.8171	.73521
	Toplam	1155	3.9414	.73791

Tablo 4.101'deki betimsel istatistik sonuçlara göre dijital etik puan ortalamalarının 3.72 ile 3.74 aralığında olduğu görülmektedir. Ayrıca GTK süre ortalamaların toplam ortalamaya çok yakın olduğu da söylenebilir.

Tablo 4.102

Dijital Etik Düzeyinin Günlük Teknoloji Kullanımına Göre Karşılaştırılması

	Varyans Kaynağı	Kareler Toplamı	sd	Kareler Ortalaması	F	p	Eta Kare
Dijital Etik	Gruplar Arası	22.999	3	7.666	3.583	.013*	.029
	Gruplar İçi	761.912	1151	.662			
	Toplam	784.911	1154				

Tablo 4.102'de öğretmen adaylarının GTK sürelerinin dijital etik düzeyleri üzerine etkisini incelemek amacıyla tek faktörlü varyans analizi gerçekleştirilmiştir. Gerçekleştirilen analiz sonucunda öğrenim GTK süresi ile dijital etik düzeyi arasında anlamlı bir fark olduğu tespit edilmiştir ($F(3,1151)=3.583, p < .05, \eta^2=.029$). Günlük teknoloji kullanım süreleri arasındaki farklılaşmaları detaylı incelemek için gerçekleştirilen post hoc analiz sonuçları ise Tablo 4.103'te gösterilmiştir.

Tablo 4.103

Dijital Etik Düzeyi Bakımından Anlamlı Farklılaşma Olan GTK Süreleri- Post Hoc

Bağımlı Değişken	(I) GTK Süresi	(J) GTK Süresi	Ortalamaların Farkı	p
Dijital Etik	1 saatten az	1-3 saat	-.21870	.282
		4-6 saat	-.28009	.100
		7 saat ve üzeri	-.09918	.878
	1-3 saat	1 saatten az	.21870	.282
		4-6 saat	-.06139	.563
		7 saat ve üzeri	.11952	.322
	4-6 saat	1 saatten az	.28009	.100
		1-3 saat	.06139	.563
		7 saat ve üzeri	.18091*	.046
	7 saat ve üzeri	1 saatten az	.09918	.878
		1-3 saat	-.11952	.322
		4-6 saat	-.18091*	.046

(*p<.05, 1saatten az(M=3.71, SD=.73) , 1-3 saat(M=3.93, SD=.74), 4-6 saat(M=3.99, SD=.72), 7 saat ve üzeri(M=3.81, SD=.74))

Tablo 4.103' te yer alan post hoca analiz sonuçları incelendiğinde;

- GTK süresi 1 saatten az olan öğretmen adayları ile 1-3 saat, 4-6 saat ve 7 saat üzeri GTK süresi olan öğretmen adayları puanları arasında istatistiksel olarak anlamlı bir fark bulunamamıştır.
- GTK süresi 1-3 saat olan öğretmen adayları ile 1 saatten az, 4-6 saat ve 7 saat üzeri GTK süresi olan öğretmen adayları puanları arasında anlamlı bir fark olmadığı görülmektedir.
- GTK süresi 4-6 saat olan öğretmen adayları ile 7 saat üzeri GTK süresi olan öğretmen adayları puanları arasında anlamlı bir fark olduğu görülürken, GTK süresi 4-6 saat olan ile 1-3 saat ve 1 saatten az olan öğretmen adayları ile anlamlı bir fark tespit edilememiştir
- GTK süresi 7 saat üzeri olan öğretmen adayları ile 4-6 saat GTK süresi olan öğretmen adayları puanları arasında anlamlı bir fark tespiti yapılmışken, GTK süresi 7 saat üzeri olan öğretmen adayları ile 1 saatten az ve 1-3 saat olan öğretmen adayları ile anlamlı bir fark gözlenememiştir.

4.4.2.9. Dijital sağlık alt boyutunun günlük toplam teknoloji kullanımına göre karşılaştırılması

Tablo 4.104

Dijital Sağlık Seviyelerinin Günlük Teknoloji Kullanımı Sürelerine Göre; Kişi Sayısı, Ortalama ve Standart Sapmaları

Bağımlı Değişken	GTK Süresi	N	M	Standart Sapma
Dijital Sağlık	1 saatten az	39	3.2393	.94575
	1-3 saat	463	3.2635	.85628
	4-6 saat	509	3.0779	.86932
	7 saat ve üzeri	144	2.9537	1.03821
	Toplam	1155	3.1423	.89538

Tablo 4.104'te yer alan betimsel istatistik sonuçları incelendiğinde dijital sağlık puan ortalamalarının 3.07 ile 3.74 aralığında olduğu görülmektedir. Ayrıca GTK süresi 4-6 saat ve 7 saat üzeri olanların dijital sağlık puanının ortalamasının altında kaldığı da görülmektedir.

Tablo 4.105

Dijital Sağlık Düzeyinin Günlük Teknoloji Kullanımına Göre Karşılaştırılması

	Varyans Kaynağı	Kareler Toplamı	sd	Kareler Ortalaması	F	p	Eta Kare
Dijital Sağlık	Gruplar Arası	14.399	3	4.800	6.066	.000*	.016
	Gruplar İçi	910.775	1151	.791			
	Toplam	925.174	1154				

Tablo 4.105'te yapılan varyans analizi ile öğretmen adaylarının günlük toplam teknoloji kullanımının dijital sağlık düzeyleri üzerine etkisi incelenmiştir. Analiz sonucunda GTK süreleri ile dijital sağlık düzeyleri arasında istatistiksel olarak anlamlı fark bulunmuştur ($F(3,1151)=6.066, p < .05, n^2=.016$). Farklılaşmaları detaylı incelemek için gerçekleştirilen post hoc sonucu ise Tablo 4.5.106' de verilmiştir.

Tablo 4.106

Dijital Sağlık Düzeyi Bakımından Anlamlı Farklılaşma Olan GTK Süreleri- Post Hoc

Bağımlı Değişken	(I) GTK Süresi	(J) GTK Süresi	Ortalamaların Farkı	p
Dijital Sağlık	1 saatten az	1-3 saat	-.02418	.998
		4-6 saat	.16139	.695
		7 saat ve üzeri	.28561	.284
	1-3 saat	1 saatten az	.02418	.998
		4-6 saat	.18557*	.007
		7 saat ve üzeri	.30980*	.002
	4-6 saat	1 saatten az	-.16139	.695
		1-3 saat	-.18557*	.007
		7 saat ve üzeri	.12423	.450
	7 saat ve üzeri	1 saatten az	-.28561	.284
		1-3 saat	-.30980*	.002
		4-6 saat	-.12423	.450

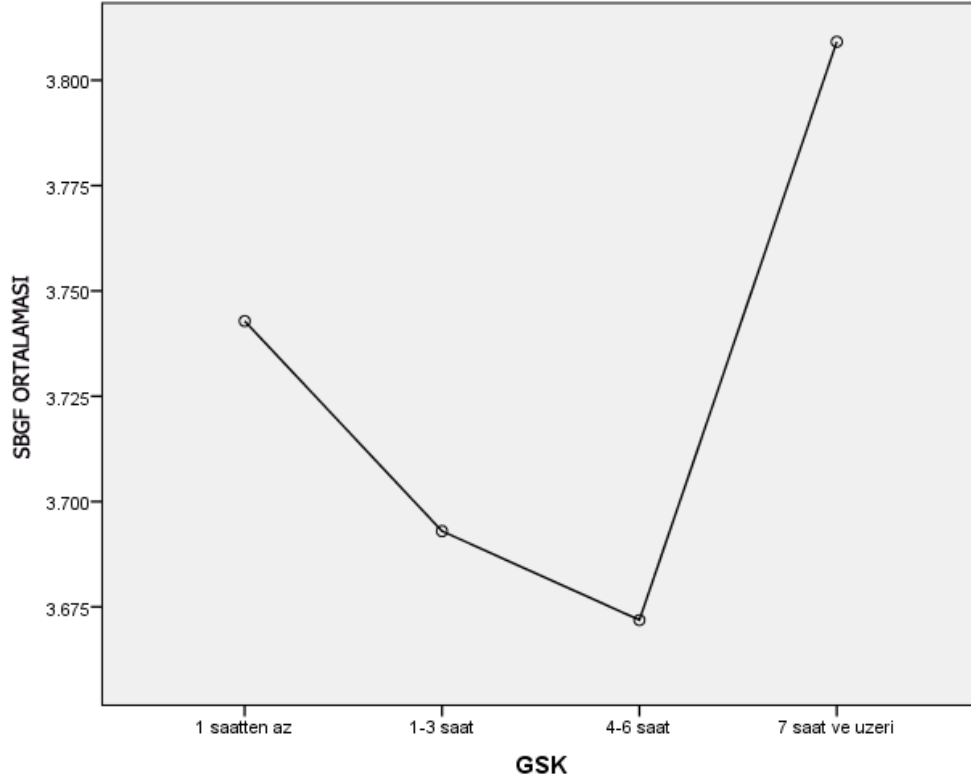
(*p<.05, 1saatten az(M=3.23, SD=.95) , 1-3 saat(M=3.26, SD=.85), 4-6 saat(M=3.07, SD=.87), 7 saat ve üzeri(M=2.95, SD=1.03))

Tablo 4.106'de günlük toplam teknoloji kullanım süreleri farklarını detaylı incelemek amacıyla yürütülen Post-Hoc analiz sonuçları verilmiştir. Bu sonuçlara göre;

- GTK süresi 1 saatten az olan öğretmen adayları ile GTK süresi 1-3 saat, 4-6 saat ve 7 saat üzeri süresi olan öğretmen adayları puanları arasında anlamlı bir fark yoktur.
- GTK süresi 1-3 saat olan öğretmen adayları ile 1 saatten az GTK süresi olan öğretmen adayları puanları arasında anlamlı bir tespit edilememişken, GTK süresi 1-3 saat olan öğretmen adayları ile 4-6 saat ve 7 saat olan öğretmen adayları puanları arasında anlamlı bir fark olduğu görülmektedir.
- GTK süresi 4-6 saat olan öğretmen adayları ile 1-3 saat GTK süresi olan öğretmen adayları puanları arasında anlamlı bir fark bulunmuşken, GTK süresi 4-6 saat olan ile 1 saatten az ve 7 saat üzeri olan öğretmen adayları ile anlamlı bir fark bulunamamıştır.
- GTK süresi 7 saat üzeri olan öğretmen adayları ile 1-3 saat GTK süresi olan öğretmen adayları puanları arasında anlamlı bir fark bulunmuşken, GTK süresi 7 saat üzeri olan öğretmen adayları ile 1 saatten az ve 4-6 saat olan öğretmen adayları ile anlamlı bir fark bulunamamıştır.

4.5. Değişkenlerin Günlük Sosyal Medya Kullanım(GSK) Sürelerine Göre Karşılaştırılması - Tek Yönlü Varyans Analizi (ANOVA)

4.5.1. Siber bilgi güvenliği farkındalığının günlük sosyal medya kullanım saatine göre karşılaştırılması



Şekil 4.7. GSK sürelerine Göre Siber Bilgi Güvenliği Farkındalık Ortalamalarının Grafiği

Şekil 4.7' deki grafikte, öğretmen adaylarının siber bilgi güvenliği farkındalıklarının en düşük 4-6 saat GSK süresine sahip olanlara ait olduğu görülmektedir. 4-6 saatten sonra ise siber bilgi güvenliği farkındalığı puanının artış eğiliminde olduğu görülmektedir.

Tablo 4.107

Siber Bilgi Güvenliği Farkındalığının Günlük Sosyal Medya Kullanımına Göre; Kişi Sayısı, Ortalama ve Standart Sapmaları

Bağımlı Değişken	GSK Süresi	N	M	Standart Sapma
SBGF	1 saatten az	223	3.7429	.70870
	1-3 saat	587	3.6930	.62772
	4-6 saat	280	3.6719	.62455
	7 saat ve üzeri	65	3.8091	.56761
	Toplam	1155	3.7040	.64039

Tablo 4.107' de yer alan betimsel analiz sonuçlarına bakılarak GSK süresinde yığılmanın 1-3 saat arasında olduğu, en az yığılmanın ise 7 saat ve üzerinde olduğu görülmektedir. Ayrıca SBGF ortalamalarının en yüksek olduğu GSK süresinin 7 saat ve üzerinde olduğu tespit edilmiştir.

Tablo 4.108

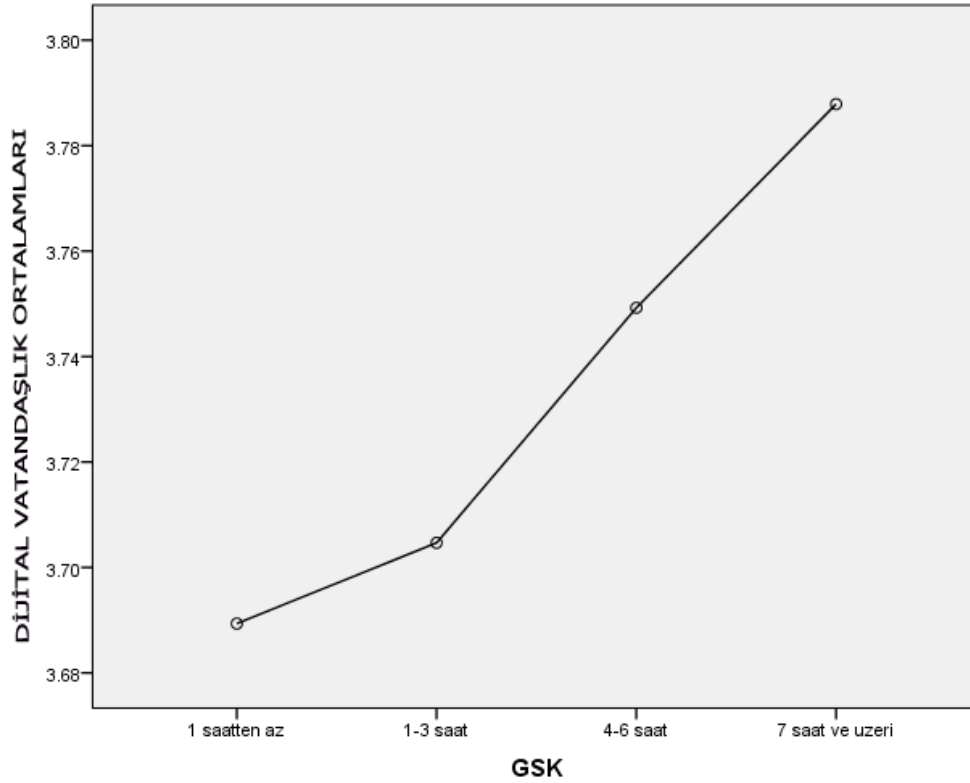
Siber Bilgi Güvenliği Farkındalığının Günlük Sosyal Medya Kullanımına Göre Karşılaştırılması

	Varyans Kaynağı	Kareler Toplamı	sd	Kareler Ortalaması	F	p
SBGF	Gruplar Arası	1.415	3	.472	1.151	.327
	Gruplar İçi	471.844	1151	.410		
	Toplam	473.260	1154			

GSK süresinin siber bilgi güvenliği farkındalığına göre istatistiksel olarak anlamlı farklılaşım farklılaşmadığını görmek için tek faktörlü varyans analizi gerçekleştirilmiştir. Analiz sonucunda SBGF ile GSK süresi arasında istatistiksel olarak anlamlı bir fark bulunamamıştır ($F(3,1151) = 1.151, p > .05$).

4.5.2. Dijital vatandaşlık düzeyinin günlük sosyal medya kullanım saatine göre karşılaştırılması

Şekil 4.8' de öğretmen adaylarının dijital vatandaşlık seviyelerinin GSK sürelerine göre değişimi gösteren grafik verilmiştir. Dijital vatandaşlık düzeyinin GSK süresi ile doğru orantılı olarak arttığı görülmektedir.



Şekil 4.8. GSK sürelerine Göre Dijital Vatandaşlık Düzeyi Ortalamalarının Grafiği

Tablo 4.109

Dijital Vatandaşlık Düzeyinin Günlük Sosyal Medya Kullanımına Göre; Kişi Sayısı, Ortalama ve Standart Sapmaları

Bağımlı Değişken	GSK Süresi	N	M	Standart Sapma
Dijital Vatandaşlık	1 saatte az	223	3.6894	.56206
	1-3 saat	587	3.7047	.45333
	4-6 saat	280	3.7492	.48734
	7 saat ve üzeri	65	3.7879	.40557
	Toplam	1155	3.7172	.48211

Tablo 4.109' da yer alan sonuçlar incelendiğinde dijital vatandaşlık ortalamalarının 3.68 ile 3.78 arasında olduğu görülmektedir.

Tablo 4.110

Dijital Vatandaşlık Düzeyinin Günlük Sosyal Medya Kullanımına Göre Karşılaştırılması

	Varyans Kaynağı	Kareler Toplamı	sd	Kareler Ortalaması	F	p
Dijital Vatandaşlık	Gruplar Arası	.877	3	.292	1.259	.287
	Gruplar İçi	267.351	1151	.232		
	Toplam	268.228	1154			

Tablo 4.110'de gerçekleştirilen tek faktörlü varyans analizine göre öğretmen adaylarının GSK süreleri ile dijital vatandaşlık seviyeleri arasında istatistiksel olarak anlamlı bir fark olmadığı görülmüştür ($F(3,1151) = 1.259, p > .05$).

4.5. 2.1. Dijital okuryazarlık düzeyinin günlük sosyal medya kullanım saatine göre farkı

Tablo 4.111

Dijital Vatandaşlık Düzeyinin Günlük Sosyal Medya Kullanımına Göre; Kişi Sayısı, Ortalama ve Standart Sapmaları

Bağımlı Değişken	GTK Süresi	N	M	Standart Sapma
Dijital Okuryazarlık	1 saatten az	223	3.4768	.80870
	1-3 saat	587	3.4472	.74482
	4-6 saat	280	3.4726	.72809
	7 saat ve üzeri	65	3.5897	.72234
	Toplam	1155	3.4671	.75212

Tablo 4.111'de gerçekleştirilen betimsel analiz incelendiğinde sadece GSK süresi 1-3 saat arasında olan öğretmen adaylarının dijital okuryazarlık ortalamaları toplam ortalamanın altında kalmıştır.

Tablo 4.112

Dijital Okuryazarlık Düzeyinin Günlük Sosyal Medya Kullanımına Göre Karşılaştırılması

	Varyans Kaynağı	Kareler Toplamı	sd	Kareler Ortalaması	F	p
Dijital Okuryazarlık	Gruplar Arası	1.240	3	.413	.730	.534
	Gruplar İçi	651.565	1151	.566		
	Toplam	652.805	1154			

Tablo 4.112’de öğretmen adaylarının dijital okuryazarlık düzeyinin GSK kullanımı yönünden anlamlı olarak farklılaşıp farklılaşmadığını tespit etmek için tek yönlü faktör analizi yapılmıştır. Sonuç olarak dijital okuryazarlık düzeyi ile GSK süresi arasında anlamlı fark tespit edilememiştir ($F(3,1151) = .730, p > .05$).

4.5.2.2. Dijital yasa alt boyutunun günlük sosyal medya kullanım saatine göre karşılaştırılması

Tablo 4.113

Dijital Yasa Düzeyinin Günlük Sosyal Medya Kullanımına Göre; Kişi Sayısı, Ortalama ve Standart Sapmaları

Bağımlı Değişken	GSK Süresi	N	M	Standart Sapma
Dijital Yasa	1 saatten az	223	4.1895	.86845
	1-3 saat	587	4.1917	.78441
	4-6 saat	280	4.2313	.81367
	7 saat ve üzeri	65	4.1885	.71675
	Toplam	1155	4.2006	.80399

Tablo 4.113’de ki betimsel istatistiklere bakıldığında dijital yasa ortalamalarının 4.18 ile 4.23 aralığında olduğu görülmektedir.

Tablo 4.114

Dijital Yasa Düzeyinin Günlük Sosyal Medya Kullanımına Göre Karşılaştırılması

	Varyans Kaynağı	Kareler Toplamı	sd	Kareler Ortalaması	F	p
Dijital Yasa	Gruplar Arası	.347	3	.116	.179	.911
	Gruplar İçi	745.590	1151	.648		
	Toplam	745.937	1154			

Tablo 4.114’te öğretmen adaylarının dijital yasa düzeyinin günlük sosyal medya kullanım süreleri yönünden anlamlı farklılaşıp farklılaşmadığını gösteren analiz sonuçları Tablo 4.6.108’de verilmiştir. Bu analiz sonuçlarına göre dijital yasa düzeyi ile GSK süreleri arasında istatistiksel olarak anlamlı fark olmadığı görülmüştür ($F(3,1151) = .179, p > .05$).

4.5.2.3. Dijital hak ve sorumluluk alt boyutunun günlük sosyal medya kullanım saatine göre karşılaştırılması

Tablo 4.115

Dijital Hak ve Sorumluluk Düzeyinin Günlük Sosyal Medya Kullanımına Göre; Kişi Sayısı, Ortalama ve Standart Sapmaları

Bağımlı Değişken	GSK Süresi	N	M	Standart Sapma
Dijital Hak ve Sorumluluk	1 saatten az	223	3.9742	.77048
	1-3 saat	587	3.9480	.70761
	4-6 saat	280	4.0080	.73913
	7 saat ve üzeri	65	4.0115	.76474
	Toplam	1155	3.9712	.73053

Tablo 4.115'deki veriler incelendiğinde sadece GSK süresi 1-3 saat olan öğretmen adaylarının dijital hak ve sorumluluk alt boyutu ortalamaları toplam ortalamasının altında kalmıştır.

Tablo 4.116

Dijital Hak ve Sorumluluk Düzeyinin Günlük Sosyal Medya Kullanımına Göre Karşılaştırılması

	Varyans Kaynağı	Kareler Toplamı	sd	Kareler Ortalaması	F	p
Dijital Hak ve Sorumluluk	Gruplar Arası	.803	3	.268	.501	.682
	Gruplar İçi	615.053	1151	.534		
	Toplam	615.855	1154			

Tablo 4.116'da gerçekleştirilen tek yönlü faktörü analizi ile öğretmen adaylarının günlük sosyal medya kullanım sürelerinin dijital hak ve sorumluluk düzeyleri üzerine etkisi incelenmiştir. Analiz sonucunda GSK süreleri arasında anlamlı bir fark olmadığı sonucuna varılmıştır ($F(3,1151) = .501, p > .05$).

4.6.6. Dijital iletişim alt boyutunun günlük sosyal medya kullanım sürelerine göre karşılaştırılması

Tablo 4.117

Dijital İletişim Düzeyinin Günlük Sosyal Medya Kullanımına Göre; Kişi Sayısı, Ortalama ve Standart Sapmaları

Bağımlı Değişken	GSK Süresi	N	M	Standart Sapma
Dijital İletişim	1 saatten az	223	3.5269	.90005
	1-3 saat	587	3.7713	.76449
	4-6 saat	280	3.9161	.84858
	7 saat ve üzeri	65	4.0846	.67932
	Toplam	1155	3.7768	.82124

Tablo 4.117' deki betimsel istatistik sonucu incelendiğinde GSK süresi ile dijital iletişim alt boyutu ortalaması doğru orantılı olarak artmıştır.

Tablo 4.118

Dijital İletişim Düzeyinin Günlük Sosyal Medya Kullanımına Göre Karşılaştırılması

	Varyans Kaynağı	Kareler Toplamı	sd	Kareler Ortalaması	F	p	Eta Kare
Dijital İletişim	Gruplar Arası	25.533	3	8.511	13.014	.000*	.033
	Gruplar İçi	752.760	1151	.654			
	Toplam	778.293	1154				

Öğretmen adaylarının günlük sosyal medya kullanım sürelerinin dijital iletişim düzeyleri üzerine etkisini incelemek amacıyla yürütülen tek faktörlü varyans analizi sonuçları Tablo 4.118'de yer almaktadır. Bu sonuçlara göre öğrenim GSK süresi ile dijital iletişim düzeyleri arasında anlamlı bir fark bulunmuştur ($F(3,1151) = 13.014, p < .05, \eta^2 = .033$).

Tablo 4.119

Dijital İletişim Düzeyi Bakımından Anlamlı Farklılaşma Olan GSK Süreleri- Post Hoc

Bağımlı Değişken	(I) Süresi	(J) GSK Süresi	Ortalamaların Farkı	p
Dijital İletişim	1 saatten az	1-3 saat	-.24439*	.001
		4-6 saat	-.38917*	.000
		7 saat ve üzeri	-.55771*	.000
	1-3 saat	1 saatten az	.24439*	.001
		4-6 saat	-.14478	.066
		7 saat ve üzeri	-.31332*	.016
	4-6 saat	1 saatten az	.38917*	.000
		1-3 saat	.14478	.066
		7 saat ve üzeri	-.16854	.430
	7 saat ve üzeri	1 saatten az	.55771*	.000
		1-3 saat	.31332*	.016
		4-6 saat	.16854	.430

(*p<.05, 1saatten az(M=3.52, SD=.90) , 1-3 saat(M=3.77, SD=.76), 4-6 saat(M=3.91, SD=.84), 7 saat ve üzeri(M=4.08, SD=.68))

Tablo 4.119'de yer alan post hoca analizi ile günlük sosyal medya kullanım süreleri farkları detaylı incelenmiştir. Bu sonuçlara göre;

- GSK süresi 1 saatten az olan öğretmen adayları ile 1-3 saat, 4-6 saat ve 7 saat üzeri GSK süresi olan öğretmen adayları puanları arasında anlamlı bir fark olduğu görülmektedir.
- GSK süresi 1-3 saat olan öğretmen adayları ile 1 saatten az ve 7 saat üzeri GSK süresi olan öğretmen adayları puanları arasında anlamlı bir fark bulunurken, GSK süresi 1-3 saat olan ile 4-6 saat olan öğretmen adayları ile anlamlı bir fark bulunamamıştır.
- GSK süresi 4-6 saat olan öğretmen adayları ile 1 saatten az GSK süresi olan öğretmen adayları puanları arasında anlamlı bir fark olduğu görülürken, GSK süresi 4-6 saat olan ile 7 saat üzeri ve 1-3 saat olan öğretmen adayları ile anlamlı bir fark olmadığı görülmüştür.
- GSK süresi 7 saat üzeri olan öğretmen adayları ile 1 saatten az ve 1-3 saat GSK süresi olan öğretmen adayları puanları arasında anlamlı bir fark tespit edilmişken, GSK süresi 7 saat üzeri olan ile 4-6 saat olan öğretmen adayları ile anlamlı bir fark bulunamamıştır.

4.5.2.5 Dijital güvenlik alt boyutunun günlük sosyal medya kullanım sürelerine göre karşılaştırılması

Tablo 4.120

Dijital Güvenlik Düzeyinin Günlük Sosyal Medya Kullanımına Göre; Kişi Sayısı, Ortalama ve Standart Sapmaları

Bağımlı Değişken	GSK Süresi	N	M	Standart Sapma
Dijital Güvenlik	1 saatten az	223	3.4753	.83364
	1-3 saat	587	3.4032	.79404
	4-6 saat	280	3.4214	.78172
	7 saat ve üzeri	65	3.5897	.86355
	Toplam	1155	3.4320	.80322

Tablo 4.120' da yer alan betimsel istatistiksel sonuçlara göre dijital güvenlik ortalamaları 3.40 ile 3.47 arasında değişmektedir. Ayrıca en yüksek dijital güvenlik ortalaması ise GSK süresi 1 saatten az olan öğretmen adaylarına aittir.

Tablo 4.121

Dijital Güvenlik Düzeyinin Günlük Sosyal Medya Kullanımına Göre Karşılaştırılması

	Varyans Kaynağı	Kareler Toplamı	sd	Kareler Ortalaması	F	p
Dijital Güvenlik	Gruplar Arası	2.555	3	.852	1.321	.266
	Gruplar İçi	741.971	1151	.645		
	Toplam	744.526	1154			

Tablo 4.121'de öğretmen adaylarının günlük sosyal medya kullanım sürelerinin dijital güvenlik düzeyleri üzerine etkisini incelemek amacıyla tek faktörlü varyans analizi yürütülmüştür. Analiz sonucunda GSK süresi ile dijital güvenlik düzeyi arasında anlamlı bir fark bulunamamıştır ($F(3,1151) = 1.321, p < .05$).

4.5.2.6 Dijital ticaret alt boyutunun günlük sosyal medya kullanım sürelerine göre karşılaştırılması

Tablo 4.122

Dijital Ticaret Düzeyinin Günlük Sosyal Medya Kullanımına Göre; Kişi Sayısı, Ortalama ve Standart Sapmaları

Bağımlı Değişken	Bölüm(J)	N	M	Standart Sapma
Dijital Ticaret	1 saatten az	223	3.5755	1.02528
	1-3 saat	587	3.5883	.99996
	4-6 saat	280	3.7726	.98792
	7 saat ve üzeri	65	3.9949	.89654
	Toplam	1155	3.6534	1.00193

Tablo 4.122' de yer alan ortalamalara bakıldığında öğretmen adaylarının sosyal medya kullanım süreleri arttıkça dijital ticaret düzeyi ortalamaları da artmıştır.

Yapılan tek faktörlü varyans analizi ile öğretmen adaylarının günlük sosyal medya kullanım sürelerinin dijital ticaret düzeyleri üzerine etkisi incelenmiştir.

Tablo 4.123

Dijital Ticaret Düzeyinin Günlük Sosyal Medya Kullanımına Göre Karşılaştırılması

	Varyans Kaynağı	Kareler Toplamı	sd	Kareler Ortalaması	F	p	Eta Kare
Dijital Ticaret	Gruplar Arası	15.400	3	5.133	5.169	.001*	.013
	Gruplar İçi	1143.063	1151	.993			
	Toplam	1158.463	1154				

Tablo 4.123'deki tek faktörlü varyans analizi sonucuna göre öğretmen adaylarının GSK süresi ile dijital ticaret düzeyleri arasında istatistiksel olarak anlamlı bir fark vardır ($F(3,1151) = 5.169, p < .05, \eta^2 = .013$).

Tablo 4.124

Dijital Ticaret Düzeyi Bakımından Anlamlı Farklılaşma Olan GSK Süreleri- Post Hoc

Bağımlı Değişken	(I) GSK Süresi	(J) GSK Süresi	Ortalamaların Farkı	p
Dijital Ticaret	1 saatten az	1-3 saat	-.01282	.998
		4-6 saat	-.19713	.123
		7 saat ve üzeri	-.41939*	.015
	1-3 saat	1 saatten az	.01282	.998
		4-6 saat	-.18432	.054
		7 saat ve üzeri	-.40657*	.010
	4-6 saat	1 saatten az	.19713	.123
		1-3 saat	.18432	.054
		7 saat ve üzeri	-.22225	.368
	7 saat ve üzeri	1 saatten az	.41939*	.015
		1-3 saat	.40657*	.010
		4-6 saat	.22225	.368

(*p<.05, 1saatten az(M=3.58, SD=1.02) , 1-3 saat(M=3.58, SD=.99), 4-6 saat(M=3.77, SD=.98), 7 saat ve üzeri(M=3.99, SD=.89))

Tablo 4.124'te günlük sosyal medya kullanım sürelerine göre dijital ticaret alt boyutları ortalamalarının farklarını detaylı incelemek amacıyla yürütülen Post-Hoc analiz sonuçları verilmiştir. Bu sonuçlara göre;

- GSK süresi 1 saatten az olan öğretmen adayları ile 7 saat üzeri GSK süresi olan öğretmen adaylarının dijital ticaret düzeyi puanları arasında anlamlı bir fark olmadığı görülürken, GSK süresi 1 saatten az olan ile 4-6 saat ve 1-3 saat süresi olan öğretmen adayları ile anlamlı bir fark olmadığı görülmektedir.
- GSK süresi 1-3 saat olan öğretmen adayları ile 7 saat üzeri GSK süresi olan öğretmen adaylarının dijital ticaret düzeyi puanları arasında anlamlı bir fark bulunurken, GSK süresi 1-3 saat olan öğretmen adayları ile 4-6 saat ve 1 saatten az olan öğretmen adayları puanları arasında anlamlı bir fark bulunamamıştır.
- GSK süresi 4-6 saat olan öğretmen adayları ile 1-3 saat, 4-6 saat, 1 saatten az ve 7 saat üzeri olan öğretmen adayları ile istatistiksel olarak anlamlı bir fark tespit edilmiştir.
- GSK süresi 7 saat üzeri olan öğretmen adayları ile 1 saatten az ve 1-3 saat GSK süresi olan öğretmen adaylarının dijital ticaret düzeyi puanları arasında anlamlı bir fark vardır. Fakat GSK süresi 7 saat üzeri olan ile 4-6 saat olan öğretmen adayları ile anlamlı bir fark yoktur.

4.5.2.7. Dijital erişim alt boyutunun günlük sosyal medya kullanım sürelerine göre karşılaştırılması

Tablo 4.125

Dijital Erişim Düzeyinin Günlük Sosyal Medya Kullanımına Göre; Kişi Sayısı, Ortalama ve Standart Sapmaları

Bağımlı Değişken	GSK Süresi	N	M	Standart Sapma
Dijital Erişim	1 saatten az	223	3.7205	.95551
	1-3 saat	587	3.8592	.77714
	4-6 saat	280	3.9190	.81783
	7 saat ve üzeri	65	3.9897	.74295
	Toplam	1155	3.8543	.82472

Tablo 4.125'te yer alan verilerden öğretmen adaylarının sosyal medya kullanım süreleri ile dijital erişim düzeylerinin doğru orantılı olarak arttığı görülmektedir.

Öğretmen adaylarının günlük sosyal medya kullanım sürelerinin dijital erişim düzeyleri üzerine etkisini tespit etmek amacıyla tek faktörlü varyans analizi gerçekleştirilmiştir.

Tablo 4.126

Dijital Erişim Düzeyinin Günlük Sosyal Medya Kullanımına Göre Karşılaştırılması

	Varyans Kaynağı	Kareler Toplamı	sd	Kareler Ortalaması	F	p	Eta Kare
Dijital Erişim	Gruplar Arası	6.374	3	2.125	3.141	.025*	.008
	Gruplar İçi	778.537	1151	.676			
	Toplam	784.911	1154				

Tablo 4.126'daki tek faktörlü varyans analizi sonucuna göre öğretmen adaylarının GSK süresi ile dijital erişim düzeyleri arasında anlamlı fark tespit edilmiştir. ($F(3,1151) = 5.169, p < .05, n^2=.008$).

Tablo 4.127

Dijital Erişim Düzeyi Bakımından Anlamlı Farklılaşma Olan GSK Süreleri- Post Hoc

Bağımlı Değişken	(I) Süresi	(J) GSK Süresi	Ortalamaların Farkı	p
Dijital Erişim	1 saatten az	1-3 saat	-.13869	.140
		4-6 saat	-.19857*	.036
		7 saat ve üzeri	-.26927	.093
	1-3 saat	1 saatten az	.13869	.140
		4-6 saat	-.05988	.748
		7 saat ve üzeri	-.13057	.618
	4-6 saat	1 saatten az	.19857*	.036
		1-3 saat	.05988	.748
		7 saat ve üzeri	-.07070	.924
	7 saat ve üzeri	1 saatten az	.26927	.093
		1-3 saat	.13057	.618
		4-6 saat	.07070	.924

(*p<.05, 1saatten az(M=3.72, SD=.95) , 1-3 saat(M=3.85, SD=.77), 4-6 saat(M=3.91, SD=.81), 7 saat ve üzeri(M=3.98, SD=.74))

Günlük sosyal medya kullanım süreleri farklarını detaylı incelemek amacıyla yürütülen Post-Hoc analiz sonuçları ;

- GSK süresi 1 saatten az olan öğretmen adayları ile 4-6 saat GSK süresi olan öğretmen adaylarının dijital erişim düzeyi puanları arasında anlamlı bir fark bulunurken, GSK süresi 1 saatten az olan öğretmen adayları ile 1-3 saat ve 7 saat üzeri GSK süresi olan öğretmen adayları ile anlamlı bir fark bulunamamıştır.
- GSK süresi 1-3 saat olan öğretmen adayları ile 7 saat üzeri, 4-6 saat ve 1 saatten az olan öğretmen adayları puanları arasında anlamlı bir fark bulunamamıştır.
- GSK süresi 4-6 saat olan öğretmen adayları ile 1 saatten az GSK süresi olan öğretmen adayları puanları arasında anlamlı bir fark bulunmuşken, GSK süresi 4-6 saat olan ile 1-3 saat ve 7 saat üzeri olan öğretmen adayları ile anlamlı bir fark bulunamamıştır.
- GSK süresi 7 saat üzeri olan öğretmen adayları ile 1 saatten az, 1-3 saat ve 4-6 saat üzeri olan öğretmen adayları ile anlamlı bir fark bulunamamıştır.

4.5.2.8. Dijital etik alt boyutunun günlük sosyal medya kullanım sürelerine göre karşılaştırılması

Tablo 4.128

Dijital Etik Düzeyinin Günlük Sosyal Medya Kullanımına Göre; Kişi Sayısı, Ortalama ve Standart Sapmaları

Bağımlı Değişken	GSK Süresi	N	M	Standart Sapma
Dijital Etik	1 saatten az	223	3.9701	.79356
	1-3 saat	587	3.9392	.70395
	4-6 saat	280	3.9476	.77575
	7 saat ve üzeri	65	3.8359	.67732
	Toplam	1155	3.9414	.73791

Tablo 4.128' deki betimsel istatistiksel sonuçlar incelendiğinde öğretmen adaylarının dijital etik ortalamalarının 3.97 ile 3.83 aralığında olduğu görülmektedir.

Tablo 4.129

Dijital Etik Düzeyinin Günlük Sosyal Medya Kullanımına Göre Karşılaştırılması

	Varyans Kaynağı	Kareler Toplamı	sd	Kareler Ortalaması	F	p
Dijital Etik	Gruplar Arası	.921	3	.307	.563	.639
	Gruplar İçi	627.448	1151	.545		
	Toplam	628.369	1154			

Tablo 4.129' da yer alan analiz sonucunda görüldüğü üzere öğretmen adaylarının dijital etik düzeyi ile GSK süreleri arasında istatistiksel olarak anlamlı bir fark bulunamamıştır. ($F(3,1151) = .563, p > .05$).

4.5.2.9. Dijital sağlık alt boyutunun günlük sosyal medya kullanım sürelerine göre karşılaştırılması

Tablo 4.130

Dijital Sağlık Düzeyinin Günlük Sosyal Medya Kullanımına Göre; Kişi Sayısı, Ortalama ve Standart Sapmaları

Bağımlı Değişken	GSK Süresi	N	M	Standart Sapma
Dijital Sağlık	1 saatten az	223	3.3004	.90429
	1-3 saat	587	3.1857	.84915
	4-6 saat	280	3.0286	.90881
	7 saat ve üzeri	65	2.6974	1.02693
	Toplam	1155	3.1423	.89538

Tablo 4.130'daki betimsel istatistiklere göre GSK süresi 4-6 saat olan ve 7 saat üzeri olan öğretmen adaylarının dijital sağlık alt boyutu ortalamaları toplam ortalamasının altında kalmıştır.

Tablo 4.131

Dijital Sağlık Düzeyinin Günlük Sosyal Medya Kullanımına Göre Karşılaştırılması

	Varyans Kaynağı	Kareler Toplamı	sd	Kareler Ortalaması	F	p	Eta Kare
Dijital Sağlık	Gruplar Arası	23.168	3	7.723	9.854	.000*	.025
	Gruplar İçi	902.006	1151	.784			
	Toplam	925.174	1154				

Tablo 4.131'deki tek faktörlü varyans analizi sonucuna göre öğretmen adaylarının GSK süresi ile dijital sağlık düzeyleri arasında anlamlı fark vardır. ($F(3,1151)=9.854, p < .05, n^2=0.25$).

Tablo 4.132

Dijit Dijital Sağlık Düzeyi Bakımından Anlamlı Farklılaşma Olan GSK Süreleri- Post Hoc

Bağımlı Değişken	(I) Süresi	GSK (J) GSK Süresi	Ortalamaların Farkı	p
Dijital Sağlık	1 saatten az	1-3 saat	.11476	.352
		4-6 saat	.27188*	.004
		7 saat ve üzeri	.60301*	.000
	1-3 saat	1 saatten az	-.11476	.352
		4-6 saat	.15712	.070
		7 saat ve üzeri	.48825*	.000
	4-6 saat	1 saatten az	-.27188*	.004
		1-3 saat	-.15712	.070
		7 saat ve üzeri	.33114*	.034
	7 saat ve üzeri	1 saatten az	-.60301*	.000
		1-3 saat	-.48825*	.000
		4-6 saat	-.33114*	.034

(*p<.05, 1saatten az(M=3.30, SD=.90) , 1-3 saat(M=3.18, SD=.84), 4-6 saat(M=3.02, SD=.90), 7 saat ve üzeri(M=3.69, SD=1.02))

Tablo 4.132’de günlük sosyal medya kullanım sürelerine göre dijital ticaret alt boyutları ortalamalarının farklarını detaylı incelemek için gerçekleştirilen Post-Hoc analiz sonuçları gösterilmiştir. Bu sonuçlara göre;

- GSK süresi 1 saatten az olan öğretmen adayları ile 4-6 saat ve 7 saat üzeri GSK süresi olan öğretmen adayları puanları arasında anlamlı bir fark bulunurken, GSK süresi 1 saatten az olan ile 1-3 saat süresi olan öğretmen adayları ile anlamlı bir fark bulunamamıştır.
- GSK süresi 1- 3 saat az olan öğretmen adayları ile 7 saat üzeri GSK süresi olan öğretmen adayları puanları arasında anlamlı bir fark varken, GSK süresi 1-3 saat olan ile 1 saatten az ve 4-6 saat süresi olan öğretmen adayları ile anlamlı bir fark yoktur.
- GSK süresi 4-6 saat olan öğretmen adayları ile 1 saatten az ve 7 saat üzeri GSK süresi olan öğretmen adayları puanları arasında anlamlı bir fark bulunurken, GSK süresi 4-6 saat olan ile 1-3 saat olan öğretmen adayları ile anlamlı bir fark bulunamamıştır.
- GSK süresi 7 saat üzeri olan öğretmen adayları ile 1 saatten az, 1-3 saat ve 4-6 saat üzeri olan öğretmen adayları ile anlamlı bir fark bulunmuştur.

4.6. Öğretmen Adaylarının Siber Bilgi Güvenliği Farkındalığı ve Dijital Vatandaşlık Düzeyleri Arasındaki İlişkinin İncelenmesi

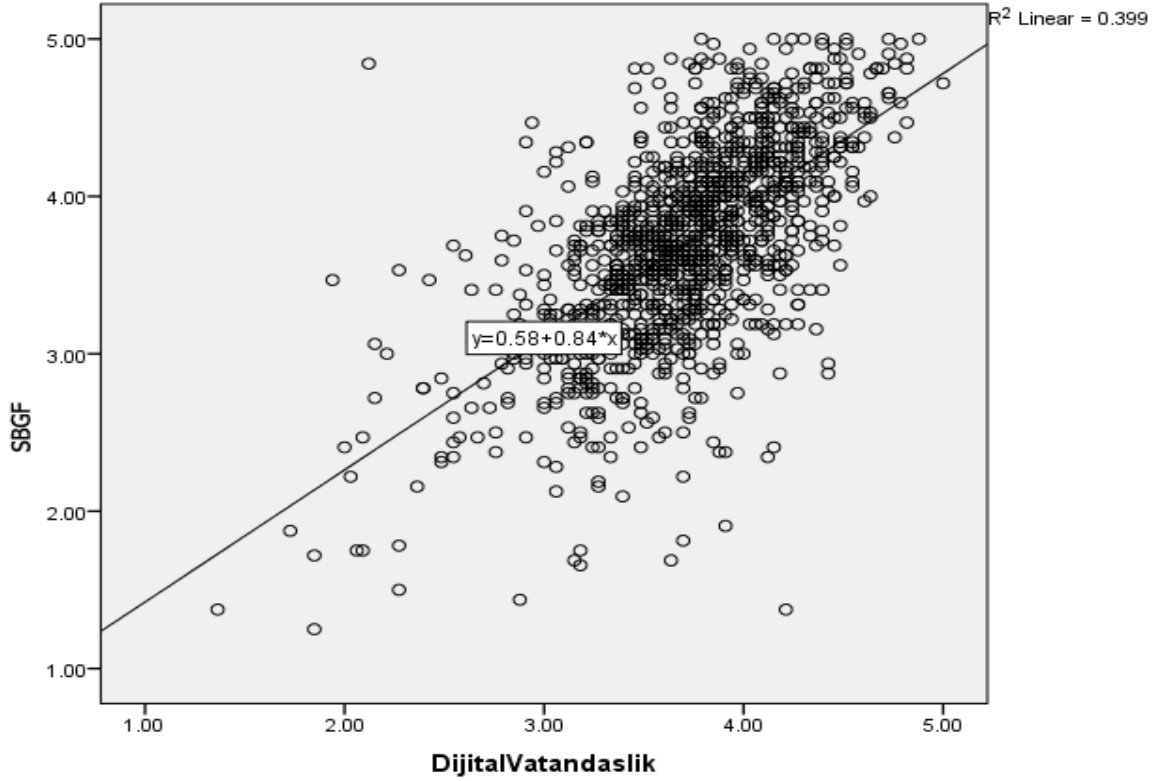
Öğretmen adaylarının -siber bilgi güvenliği farkındalığı ve dijital vatandaşlık düzeyleri arasında anlamlı bir ilişki olup olmadığının tespiti için Pearson korelasyon kat sayısı hesaplanmıştır.

Tablo 4.133

Siber Bilgi Güvenliği Farkındalığı ve Dijital Vatandaşlık Düzeyleri Arasındaki İlişkinin Çözümlemesi(Korelasyon)

	Dijital Vatandaşlık Düzeyi	r ²
Siber Bilgi Güvenliği Farkındalığı	.632**	.399
p<.05**		

Tablo 4.133'te verilen sonuçlar incelendiğinde SBGF ve dijital vatandaşlık düzeyleri arasındaki korelasyon değeri .632 olarak hesaplanmıştır. Hesaplanan korelasyon değerinin .632 olması aralarında orta düzeyde ilişki olduğunu göstermiştir(r=.0 ilişki yok, 0.01-0.29 zayıf ilişki, 0.30-0.79 orta düzey ilişki, 0.71-0.99 yüksek ilişki, 1.00 mükemmel ilişki)(Köklü, Büyükoztürk ve Çoklu, 2007). Ayrıca belirleme kat sayısı olarak belirtilen r² değeri bir değişkenin içindeki varyasyonun ne kadarının diğer değişken tarafından açıklandığını göstermektedir(Günel,2003).). Elde edilen bulgular ışığında; siber bilgi güvenliği farkındalığı değişkeni içindeki değişimin %39' u dijital vatandaşlık değişkeni ile açıklanabilir. Yani açıklanmak istenen siber bilgi güvenliği farkındalığı değişkenindeki varyansın yüzde kaçının dijital vatandaşlık düzeyi tarafından açıklandığıdır. Bu yorumu değişkenlerinin yerini değiştirerek yapmamız da mümkündür. İki değişken arası ilişkiyi gösteren grafik Şekil 4.9'da verilmiştir.



Şekil 4.9. SBGF ile Dijital Vatandaşlık Arasındaki İlişki Grafiği

Şekil 4.9’da görüldüğü gibi grafiğimizde pozitif yönde doğrusal bir dağılım var. Yani iki değişken arasında doğrusal bir ilişki var diyebiliriz.

4.8.Siber Bilgi Güvenlik Farkındalığı ve Dijital Vatandaşlık Alt Boyutları Arasındaki İlişki

Siber bilgi güvenliği farkındalığı ile dijital vatandaşlığın alt boyutları arasındaki ilişkiyi tespit etmek için Pearson korelasyon kat sayıları hesaplanmıştır. Ayrıca SBGF’nin alt boyutlar tarafından ne kadar açıklandığını göstermek için r^2 değerleri hesaplanmıştır. İstatistiksel sonuçlar Tablo 4.134’ de verilmiştir.

Tablo 4.134

Siber Bilgi Güvenliği Farkındalığı ve Dijital Vatandaşlık Alt Boyutları Arasındaki İlişkinin Çözümlemesi(Korelasyon)

	Dijital Okuryazarlık	Dijital Yasa	Dijital Hak ve Sorumluluk	Dijital İletişim	Dijital Güvenlik	Dijital Ticaret	Dijital Erişim	Dijital Etik	Dijital Sağlık
SBGF	.490**	.431**	.536**	.342**	.331**	.294**	.510**	.344	.023
r^2	.240	.186	.287	.117	.110	.086	.260	.118	.053
p	.000	.000	.000	.000	.000	.000	.000	.000	.429

Tablo 4.134' de siber bilgi güvenliği ile dijital vatandaşlığın alt boyutları arasındaki ilişkiler gösterilmiştir. Tablodaki veriler incelendiğinde sadece SBGF ile dijital sağlık(.023) alt boyutu arasında istatistiksel olarak arasında sıfıra yakın yani çok düşük düzeyde ilişki tespit edilmiş, $r^2 = .053$ bulunmuştur. Bu iki değişken arasında anlamlı bir ilişki yok şeklinde yorumlanabilir. Diğer alt boyutlar incelendiğinde; SBGF ile dijital okuryazarlık (.490, $r^2 = .240$), dijital yasa (.431, $r^2 = .186$), dijital hak ve sorumluluk (.536, $r^2 = .287$) ve dijital erişim (.510, $r^2 = .260$) alt boyutları arasında orta düzeyde bir ilişki tespit edilmiştir. SBGF ile; dijital iletişim (.342, $r^2 = .117$), dijital güvenlik (.331, $r^2 = .110$) ve dijital ticaret (.294, $r^2 = .086$) alt boyutları arasında zayıf düzeyde ilişki tespit edilmiştir. Bu verileri şu şekilde yorumlamak mümkündür: SBGF değişkenindeki varyansın %24'ü dijital okuryazarlık, %18'i dijital yasa, %28' i dijital hak ve sorumluluk, %26'sı dijital erişim, %11'i dijital iletişim, %11'i dijital güvenlik, %08'i dijital ticaret tarafından açıklanabilir.



5. TARTIŞMA, SONUÇ ve ÖNERİLER

Araştırmada öğretmen adaylarının siber bilgi güvenliği farkındalıkları ve dijital vatandaşlık düzeyleri; cinsiyet, bölüm, sınıf kademesi, günlük akıllı telefon ve tablet kullanım saati, teknolojik aletlerden birine sahip olma (Telefon, Tablet, Bilgisayar) durumları gibi değişkenlere göre incelenmiştir. Araştırma Türkiye’de Akdeniz Bölgesinde yer alan bir devlet üniversitesinin Eğitim Fakültesi’nden 809 kız 346 erkek olmak üzere toplam 1155 öğrenci ile gerçekleştirilmiştir. Araştırmada veriler 8 farklı bölümün 4 kademesinden toplanmıştır (Bilgisayar ve Öğretim Teknolojileri Öğretmenliği (BÖTE 42 kişi), Fen Bilgisi Öğretmenliği (174 kişi), İlköğretim Matematik Öğretmenliği (150 kişi), Sınıf Öğretmenliği (176 kişi), Okul Öncesi Öğretmenliği (158 kişi), Psikolojik Danışmanlık ve Rehberlik (PDR 196 kişi), Türkçe Öğretmenliği (134 kişi), ve İngilizce Öğretmenliği (125 kişi)). BÖTE bölümünde 1.sınıf öğrencisi bulunmadığından bu bölümde 1.sınıflardan veri toplanmıştır.

Araştırma sonucunda yapılan analizler incelendiğinde öğretmen adaylarının SBGF’nin 3,704 iken, DV düzeyi ortalamalarının 3,717 olduğu görülmüştür. Öğretmen adaylarının siber bilgi güvenliği farkındalıkları farklı cinsiyete göre incelendiğinde anlamlı bir fark olduğu gözlenmiştir. Erkeklerin siber bilgi güvenliği farkındalıkları ortalaması 3.80 çıkmışken, kadınların siber güvenlik farkındalıkları ortalaması 3.66 çıkmıştır. Bu da çalışmaya katılan erkek öğretmen adaylarının siber güvenlik farkındalıkları kadınlara göre daha yüksek olduğunu, cinsiyetin SBGF’liğinde etkili olduğunu göstermektedir. Yılmaz (2015) 472 öğretmen adayı ile yaptığı çalışmada benzer bir sonuca ulaşmıştır. Dijital veri güvenliği farkındalığını erkeklerin lehine bulmuştur. Öztezcan (2017) da Marmara Üniversite bünyesinde çalışan 149 akademik, 265 idari personel ile yaptığı çalışmasında bilgi güvenliği farkındalığını erkeklerin lehine olacak şekilde bulmuştur. Gökmen ve Akgün (2014) BÖTE öğretmen adaylarının bilgi güvenliğini ölçmeye yönelik yaptıkları çalışmanın sonucunda bu sonuçlara paralel cinsiyetin erkeklerin lehine olacak şekilde bilgi güvenliğine etki ettiğini tespit etmiştir. Tüm bu çalışmalarda erkekler lehine sonuçların çıkmasına; erkeklerin teknoloji ile daha yakından ilgili olması, toplumda kadınların teknoloji hakkında daha az bilgi sahibi olduğu ön yargısının olması neden olmuş olabilir.

Çalışmada ulaşılan diğer bir sonuç ise; cinsiyet ile dijital vatandaşlık düzeyi arasında anlamlı bir fark olmadığıdır. Literatürde bu sonucu destekleyen çalışmalara bakıldığında; Sakallı ve Çiftçi (2016) de cinsiyet ile dijital vatandaşlık arasında anlamlı bir fark bulamamıştır. İşman ve Güngören (2013) öğretmen adayları ile yaptığı çalışmada; dijital vatandaşlık düzeylerini cinsiyet, sınıf, eğitim düzeyi, bilgisayara sahip olma gibi değişkenlere göre incelemiş, cinsiyet ile dijital vatandaşlık düzeyi arasında anlamlı bir fark bulamamıştır. Sakallı (2015) sınıf öğretmen adaylarının dijital vatandaşlık algısını ölçmek için yapmış olduğu çalışmada cinsiyet ile dijital vatandaşlık arasında anlamlı bir fark bulamamıştır. Bu sonuçların çıkma sebebi Türkiye’de

internet kullanım oranının cinsiyet bazında birbirine yakın olması olarak gösterilebilir. TÜİK tarafından 2019 yılında yayınlanan rapora göre kadın kullanıcı oranı %98,17 iken, erkek kullanıcı oranı %98,4'tür. Bu rapor da bunu destekler niteliktedir. Alan yazında bu sonuçların tersini söyleyen çalışmalar da mevcuttur. Lisa M Jones ve Kimberly J Mitchell (2015) ABD'de ortaokul ve lisede yaptıkları çalışmada kız öğrencilerin dijital vatandaşlık ölçeğinden aldıkları puanların erkeklerden yüksek olduğunu tespit etmiştir. Bunun sebebi farklı ülkelerde farklı eğitim sistemlerinin olması, toplumsal ön yargıların olmaması, farklı internet kullanım oranları olabilir.

Öğretmen adaylarının GTK saatleri 'ortalama puanlarına bakıldığında 2.66 gibi bir sonuç çıkmaktadır. Bu sonuç ölçekte 1-3 saat ile 4-6 saat arasına denk gelmektedir. Yine bu saatler kadınlar için 2.64 iken, erkekler için ise 2.68 olarak çıkmış, aynı aralıkta kalmıştır. Öğretmen adaylarının GSK oranlarına bakıldığında ise 2.16 gibi bir sonuç çıkmıştır. Ölçekte bu 1-3 saat ile 4-6 saat aralığına gelmektedir. Bu saat cinsiyete göre bakıldığında ise kadınlar için 2.19 erkekler için ise 2.09 olarak bulunmuştur. Yılmaz (2015) öğretmen adayları ile yaptığı çalışmada katılımcıların % 63,ü bilgisayar başında 1-2 saat, %19,8 'i 3-4 saat zaman geçirmektedir. Gökmen (2014) BÖTE öğretmen adayları ile yaptığı çalışmada internet kullanım oranını ve bilgisayar kullanım oranını 4 saatin üzerinde olduğunu bulmuştur. Mart (2012) da farklı meslekten bireyler ile yapmış olduğu çalışmasında bilgisayar kullanım oranını 4 saatin üzerinde bulmuştur. Çolak (2019) üniversite öğrencileri ile yaptığı çalışmada internet kullanım oranını 3-5 saat ile 5-7 saat arasında yoğunlaştığını belirtmiştir. Berrier (2007) ortaokul öğrencilerinin günlük kullanım saatlerini ise 30 dakika ile 2 saat 20 dakika arasında bulmuştur. Alan yazında bu konuyla ilgili çalışmalar incelendiğinde GTK kullanımı ve GSK ortalama 2 saat ile 4 saat arasında olduğu görülmektedir. Bu oranların yüksek çıkmasını en büyük nedeni akıllı telefonlar ve sosyal medyanın hayatımıza girmiş olması olarak gösterilebilir. Zira Mart (2012) yapmış olduğu çalışmada katılımcıların teknoloji ile tanışma yaşının 15-19 yaş aralığında olduğunu belirtmiştir. Erken yaşta teknoloji ile tanışma ve bireyde oluşan sosyal medya ve akıllı telefon kullanma isteği bu oranların yüksek çıkmasına neden olmuş olabilir. Ayrıca eğitim ortamlarının, devlet kurumlarının, oyun alanlarının dijitalleşmesi bu oranın artmasına neden olmuş olabilir.

Yine çalışmada öğretmen adaylarının siber güvenlik farkındalıkları, dijital vatandaşlık düzeyleri ve alt boyutları olan; dijital okuryazarlık, dijital yasa, dijital hak ve sorumluluk, dijital iletişim, dijital güvenlik, dijital ticaret, dijital erişim, dijital sağlık, dijital etik GTK oranı ve GSK oranına göre farkı incelenmiştir. Siber bilgi güvenliği farkındalığı ile GTK oranı arasında anlamlı bir fark bulunamamıştır. Gökmen ve Akgün (2014) de yapmış oldukları çalışmada günlük bilgisayar ve internet kullanım oranının bilgi güvenliğine etkisi olmadığını belirtmiştir. Mart (2012) bilgi güvenliği farkındalığının internet ve bilgisayar kullanım süresine göre değişmediğini bulmuştur. Bu sonuçlardan farklı olarak Yılmaz (2015) öğretmenlerin dijital veri güvenliğini

etkileyen nedenlerden birinin günlük teknoloji kullanımı olduğunu belirtmiştir. Diğerlerinden farklı gibi görünen bu sonucun nedeni; çalışmanın görev yapmakta olan öğretmen adayları ile yapılmış olması olabilir. Milli eğitimde görev yapan öğretmenlerin almış oldukları hizmet içi eğitimler ve mesleki tecrübeler GTK oranı ile SBGF'ni paralel artırmış olabilir. Yine bu sonuca benzer bir sonuç bulan Çolak (2019) dijital güvenlik öz yeterlilik düzeyi ile internet kullanım sıklığı arasında istatistiksel olarak anlamlı bir fark bulmuştur. Yapılan çalışmada örneklemin sadece eğitim fakültesini kapsamaması bu sonucun çıkmasına neden olmuş olabilir. 21. yüzyıl ile birlikte iletişim araçlarında ve sosyal medya platformlar sayılarında hızlı bir artış yaşanmıştır. Dolayısı ile GSK süreleri ve GTK oranları buna paralel artmış, SBGF etkilenmemiş olabilir.

Bu çalışmanın sonuçlarına paralel olarak Sakallı ve Çiftçi (2016) ise günlük internette harcanan süre ile dijital vatandaşlık düzeyi arasında anlamlı bir fark bulmuştur. Kocadağ (2012)'da internet kullanım süresi yüksek olanların lehine olacak şekilde anlamlı bir fark bulmuştur. Sakallı (2015) sınıf öğretmenleri ile yapmış olduğu çalışmada dijital vatandaşlık toplam puanı ile internette geçirilen zaman arasında anlamlı bir fark bulmuştur. Farmer'ın (2010) yapmış olduğu dijital vatandaşlık tanımı da bu sonuçlara paraleldir. Yapmış olduğu tanımda internet aracılığı ile bilgilere kolay bir şekilde ulaşan, dijital ortamları etkin kullanan, günlük hayatta kendinden beklenenleri dijital mecralarda da sergileyen bireylere dijital vatandaş demiştir. Bu tanımdan da yol çıkarak GTK oranı ile dijital vatandaşlık düzeylerinin paralel artabileceğini söylemek mümkündür.

Dijital vatandaşlık Ribbe ve Mike (2011) tarafından 9 boyuta ayrılmıştır. Bu çalışmada dijital vatandaşlığın 9 boyutu ayrı ayrı analiz edilmiştir. Dijital okuryazarlık düzeyi ve günlük teknoloji kullanım arasında anlamlı bir fark bulunmuştur. Bu sonuca göre günlük teknoloji kullanım süresi fazla olan öğretmen adaylarının dijital okuryazarlık düzeyi de fazla çıkmıştır. Dijital yasa düzeyi ve teknoloji kullanım arasında anlamlı bir fark bulunamamıştır. Yani günlük teknoloji kullanım süresi dijital yasa düzeyini büyük oranda etkilememiştir. Dijital hak ve sorumluluk ile günlük teknoloji kullanım arasında anlamlı bir fark bulunamamıştır. Bu sonuç günlük teknoloji kullanımının dijital hak ve sorumluluk üzerinde etkisinin düşük olduğunu göstermektedir. Dijital iletişim düzeyi ve günlük teknoloji kullanım arasında anlamlı bir fark bulunmuştur. Bu sonuca göre günlük teknoloji kullanım oranı artıkça dijital iletişim düzeyi de artmaktadır.

Dijital güvenlik düzeyi ile günlük teknoloji kullanım arasında anlamlı bir fark bulunamamıştır. Bu çalışmada iki farklı ölçek kullanılmıştır. Temel olarak ölçeklerden bir tanesi siber bilgi güvenliği farkındalığını ölçerken diğeri ise dijital vatandaşlık düzeyini ölçmektedir. Dijital vatandaşlık ölçeğinin bir alt boyutu da siber güvenlik ile benzer olan dijital güvenlik boyutudur. Çalışma sonuçları incelendiğinde günlük teknoloji kullanımı ile hem siber güvenlik

farkındalığı hem de dijital vatandaşlığın alt boyutu olan dijital güvenlik düzeyi arasında anlamlı fark bulunamamıştır. Buna benzer olarak Mart'da (2012) günlük bilgisayar kullanım süresi ile bilgi güvenliği arasında anlamlı fark tespit edememiştir. Bu sonuç iki boyutun benzer olduğunu destekleyen bir sonuç olabilir.

Dijital ticaret düzeyi ve günlük teknoloji kullanım arasında anlamlı bir fark bulunmuş, günlük teknoloji kullanım süresi fazla olan öğretmen adaylarının dijital ticaret düzeyinin daha yüksek olduğu tespit edilmiştir. E-ticaret kullanıcısının 2017 yılında 1.61 milyara ulaşmıştır (Wearesocial, 2017). Son yıllarda e-ticaret oranında yaşanan artış bu anlamlı farkın oluşmasına neden olmuş olabilir.

Beklendiği üzere dijital erişim düzeyi ile günlük teknoloji kullanım arasında anlamlı bir fark bulunmuştur. Bulduğumuz dijital çağ, teknoloji ile iç içe olmamızı zorunlu kılmıştır. Bu nedenle neredeyse her vatandaş teknoloji ile doğrudan ya da dolaylı temas etmek zorunda kalmıştır. Bu da beraberinde günlük teknoloji kullanımı ve dijital erişim düzeyi arasındaki anlamlı farklılaşmaya neden olmuş olabilir.

Günlük sosyal medya kullanım saatinin farklı değişkenlere göre incelemesi sonucunda; günlük sosyal medya kullanım süresi ile siber güvenlik, dijital vatandaşlık, dijital okuryazarlık, dijital yasa, dijital hak ve sorumluluk, dijital güvenlik, dijital etik arasında anlamlı fark bulunamamıştır. Oyedemi (2012)' de internet kullanım sıklığı ile dijital vatandaşlık düzeyi arasında anlamlı bir fark olmadığını belirtmiştir. Yiğit ve Seferoğlu (2019) ise internet kullanım süresinin siber güvenlik davranışını etkileyecek yeterlilikte bir değişken olmadığını belirtmiştir. Fakat sosyal medya kullanım süresi ile dijital iletişim, dijital ticaret, dijital erişim, dijital sağlık arasında anlamlı bir fark tespit edilmiştir. Bu çalışmaya paralel olarak Vural ve Kurt(2018) üniversite öğrencileri ile yaptığı çalışmada internet kullanım oranı ile dijital erişim ve dijital sağlık değişkeni arasında anlamlı fark olduğunu tespit etmiştir.

Araştırmada değişkenlerin bölümlere göre karşılaştırılması sonucu öğretmen adaylarının öğrenim gördükleri bölümler ile SBGF ve DV düzeyleri arasında anlamlı bir fark bulunmuştur. Alan yazın incelendiğinde buna benzer sonuçları görmek mümkündür. Özbek (2019) öğretmen adaylarının siber güvenlik farkındalıklarını incelediği çalışmada, bölüm ve siber güvenlik farkındalığı arasında istatistiksel olarak anlamlı bir fark tespit etmiştir. Seferoğlu ve Yiğit'in (2019) 420 lisans ve ön lisans öğrencisi ile yapmış olduğu çalışmada da siber güvenlik puanlarının bölüme göre farklılaştığı tespit edilmiştir. Yılmaz (2015) ise dijital veri güvenliğini sınıf öğretmeni branş öğretmeni şeklinde karşılaştırmış, istatistiksel olarak anlamlı fark bulamamıştır. Bu sonucun çıkmasında sınıf ile diğer tüm branş ları aynı anda karşılaştırması etkili olmuş olabilir. SBGF yönünden farklılaşmanın olduğu bölümler incelendiğinde en dikkat çeken nokta; BÖTE bölümü İngilizce Öğretmenliği bölümü dışında kalan tüm bölümler ile anlamlı farklılaşmıştır. Farklılaşma

ise BÖTE bölümünün lehine olacak şekildedir. Fakat DV düzeyleri bakımından incelendiğinde; BÖTE bölümünün sadece sınıf öğretmenliği ve okul öncesi öğretmenliği bölümleri ile anlamlı farklılaştığı görülmektedir. Farklılaşma ise BÖTE bölümü lehinedir. Yine İngilizce öğretmenliği bölümünün; BÖTE ve Türkçe öğretmenliği bölümleri dışında kalan tüm bölümler ile anlamlı farklılaştığı görülmektedir.

Bölümler bazında SBGF ortalamaları incelendiğinde en yüksek ortalamanın BÖTE bölümünde olduğu görülmektedir. Seferoğlu ve Yiğit'in (2019) çalışmasında BÖTE bölümü öğrencilerinin siber güvenlik farkındalıklarının diğer bölümlerden daha fazla olduğu ortaya çıkmıştır. Bu sonucun çıkmasının nedeni; bölümün lisans düzeyinde bu konuda ders alması olarak gösterilebilir. Ayrıca diğer bölümler incelendiğinde en yüksek ikinci ortalamanın Yabancı Dil Öğretmenliği bölümünde olduğu görülmektedir. Bunun sebebi olarak; siber bilgi güvenliği ile ilgili birçok terimin yabancı dilden Türkçe'ye girmesi, teknolojik terimlerin birçoğunun İngilizce olması, bu bölüme gelen öğretmen adaylarının üniversitelere giriş sınavından yüksek puanlar alarak yerleşmesi, yine bu bölüme yerleşen öğretmen adaylarının diğer bölümlere göre sosyal ekonomik düzeyinin diğer bölümlere göre daha iyi olması gösterilebilir. En düşük ortalamanın Sınıf Öğretmenliği bölümünde olduğu da görülmektedir.

Bölümler bazında DV düzeyleri incelendiğinde en yüksek ortalamanın BÖTE bölümünde olduğu görülmektedir. Bu sonucun çıkmasının nedeni olarak; bölümün ders içeriklerinde buna yönelik eğitimlerin veriliyor olması gösterilebilir. Ayrıca diğer bölümler incelendiğinde SBGF'nda olduğu gibi; en yüksek ikinci ortalamanın Yabancı Dil Öğretmenliği bölümünde olduğu görülmektedir. Bunun sebebi olarak dijital vatandaşlıkta birçok terimin yabancı dilden Türkçe'ye girmesi veya İngilizce olması bu ortalamanın oluşmasına neden olmuş olabilir. Anlamlı farklılaşmasa da en düşük ortalamanın Sınıf Öğretmenliği bölümünde olduğu görülmektedir. Görmez (2016) de Sınıf, Sosyal Bilgiler ve Türkçe öğretmenlerinin dijital vatandaşlık algısını incelediği nitel çalışmada; sınıf öğretmenleri adaylarının dijital vatandaşlık düzeylerini diğer bölümlere göre düşük bulmuştur. Araştırma sonuçlarına bakıldığında; SBGF ve DV düzeylerinde diğer bölümler ile en çok farklılaşma olan iki bölüm BÖTE ve İngilizce öğretmenliğidir. Farklılaşmalar ise bu iki bölümün lehinedir. SBGF ve DV düzeyi ortalaması en yüksek olan bölümün de bu iki bölüm olduğu görülmektedir.

Dijital vatandaşlığın 9 alt boyutundan anlamlı farklılaşma olanlar incelendiğinde; Dijital okuryazarlık düzeyinin bölümlere göre farkının incelenmesinde bölümler ile dijital okuryazarlık arasında anlamlı bir fark tespit edilmiştir. Dijital okuryazarlık ortalama puanlarına bakıldığında yine en düşük puana sahip olan bölümün sınıf öğretmenliği bölümü öğretmen adayları olduğu görülürken en yüksek puan ortalamasında BÖTE bölümü öğretmen adayları olduğu görülmüştür. Yine BÖTE bölümünün; Fen Bilgisi, Türkçe ve İngilizce Öğretmenliği bölümleri ile anlamlı

farklılaşmadığı görülmektedir. Verinin toplandığı fakültenin ders programı incelendiğinde; Türkçe Öğretmenliği ve Fen Bilgisi Öğretmenliği bölümlerinin 2.sınıfta bahar ve gıze döneminde, diđer bölümlerde 1.sınıfta bilgisayar dersi aldığı görülmektedir. Bilgisayar dersinin 2.sınıfta veriliyor olması bu farklılaşmanın olmasını sağlamış olabilir. İngilizce öğretmenliği için ise; dijital ortamlarda İngilizce terimlerin fazla olması bu bölümdeki öğretmen adaylarının bu terimleri daha iyi anlamasını sağlamış olabilir.

Diđer yandan dijital erişim düzeyinin de bölümlere göre anlamlı farklılaştığı görülmektedir. Sonuçlar incelendiğinde BÖTE bölümünün Yabancı Dil Öğretmenliği bölümü dışında diđer tüm bölümlerle anlamlı farklılaştığı tespit edilmiştir. Ribble (2011) dijital erişimi; teknolojiye her yerden yüksek kalitede erişim sağlama bilme olarak tanımlamıştır. BÖTE bölümü ders içeriklerinin genelde teknoloji kullanımı üzerine olduğu bilinmektedir. Dolayısı ile bu anlamlı farkın oluşması beklenen bir sonuçtur.

Dijital etik düzeylerinin bölümlere göre anlamlı farklılaştığı analiz sonunda görülen bir diđer bulgudur. Burada dikkat çeken nokta ise PDR bölümü ile Okul Öncesi öğretmenliği bölümünde PDR bölümünün lehine olacak şekilde bir farklılaşma olmasıdır. PDR bölümünün ders programı incelendiğinde “Gelişim Psikolojisi” dersi göze çarpmaktadır. Bu dersin içeriğinde genel etik ve ahlak kuramları yer almaktadır. Okul Öncesi Öğretmenliği bölümünde ise daha çok erken çocukluk dönemi gelişine yönelik dersler yer almaktadır. Dolayısı ile PDR bölümünün farkındalığının yüksek olması beklenen bir sonuçtur. Yine ortalamalara bakıldığında Yabancı Dil, PDR, BÖTE, Matematik Öğretmenliği bölümleri ortalamanın üstünde dijital etik puanına sahipken diđer bölümler ortalamanın altında kalmıştır. BÖTE ve Yabancı Dil öğretmenliği bölümlerinin diđer bölümler ile arasında bir fark oluşmuştur, fakat bu fark anlamlı değildir.

Öğretmen adaylarının öğrenim gördükleri kademenin farklı değişkenlere göre incelenmesi sonucunda ise; siber güvenlik, dijital vatandaşlık, dijital iletişim, dijital yasa, dijital ticaret, dijital hak ve sorumluluk, dijital güvenlik, dijital etik, dijital sağlık arasında anlamlı fark bulunamamıştır. İşman ve Güngören (2013), Sakallı ve Çiftçi (2016) ile Bardakçı ve diđerleri (2014) yapmış oldukları çalışmalarda dijital vatandaşlık ile sınıf kademesi arasında anlamlı bir fark bulamamıştır. Karacı ve diđerleri (2017) tarafından yapılan araştırmada da siber güvenlik farkındalığı ile sınıf kademeleri arasında anlamlı fark bulunamamıştır. Yine bu çalışmaya paralel olarak Gökmen ve Akgün (2015) de öğrenim görülen kademenin bilişim güvenliği ile anlamlı farklılaşmadığını belirtmiştir. Araştırmada dikkat çeken bir husus da öğretmen adaylarının siber güvenlik farkındalıkları puanları 1. sınıftan 2. sınıfa kadar neredeyse hiç değişmemiş olarak ortaya çıkmış olmasıdır. Daha sonrasında anlamlı olmasa da bir artış eğilimine girmiştir. Dijital vatandaşlık ortalamaları da yine benzer şekilde 2. sınıftan sonra anlamlı olmasa da artış göstermiştir. Seferoğlu ve Yiğit (2019) de üniversite öğrencilerinin siber güvenlik

farkındalıklarının 3. ve 4. sınıfta daha yüksek olduğunu belirtmiştir. Araştırma sonucunda SBGF ve DV düzeyinde sınıf kademesine göre anlamlı olmamasına karşın 2. sınıftan itibaren artış görülmüştür. Araştırma yapılan devlet üniversitesinin Eğitim Fakültesi ders programları incelendiğinde; BÖTE hariç araştırmaya katılan 1.sınıflar verinin toplandığı Ekim ve Kasım aylarında henüz bilgisayar dersi almaya yeni başlamışlardır. 2. Sınıflar ise 1.sınıfta sadece 1 dönem bilgisayar dersi almışlardır. 3. ve 4. sınıflar ise öğrenim gördükleri ilk iki eğitim-öğretim yılında 2 dönem Bilgisayar dersi almışlardır. Ortalamaların 2. sınıftan itibaren artmasının nedeni olarak bu derslerin içeriği gösterilebilir. Ayrıca sınıf kademesiyle birlikte artan yaş ve deneyim de bu ortalamanın oluşmasına neden olmuş olabilir. Ünver (2012) de öğretmen adayları ile yaptığı çalışmada DV düzeyi ile yaş arasında yaşı büyük olanların lehine anlamlı fark bulmuştur. Yine çalışmada elde edilen sonuçlar incelendiğinde öğrenim gördükleri kademe ile dijital erişim ve dijital okuryazarlık düzeyleri arasında anlamlı bir fark tespit edilmiştir. Özellikle dijital okuryazarlık düzeyi bakımından incelendiğinde 1. sınıf ve 2. sınıfın öğrencilerinin ortalamaları, 4. sınıf öğrencilerin ortalamaları ile anlamlı farklılaştığı, bu farklılaşmanın 4. sınıf öğrencilerinin lehine olduğu görülmektedir.

Gerçekleştirilen korelasyon analizi neticesinde öğretmen adaylarının SBGF seviyeleri ile DV düzeyleri arasında orta düzeyde pozitif bir ilişki tespit edilmiştir. Bu ilişkiye göre; siber bilgi güvenliği farkındalığı yüksek olan öğretmen adaylarının belirli bir kısmının dijital vatandaşlık düzeylerinin de yüksek olduğu ve siber bilgi güvenliği farkındalığı düşük olan öğretmen adaylarının bazılarının da dijital vatandaşlık düzeylerinin de düşük olduğu şeklinde yorumlanabilir. Bu orta düzeydeki pozitif ilişkinin oluşmasının nedeni dijital vatandaşlığın alt boyutlarından birinin de dijital güvenlik olması olabilir. Dijital vatandaşlığın alt boyutları ile SBGF arasındaki ilişki incelendiğinde; SBGF ile dijital sağlık alt boyutu arasında istatistiksel olarak sifıra yakın yani çok düşük düzeyde ilişki tespit edilmiştir. Ribble ve Mike(2011) dijital sağlığı kullanıcın teknoloji kullanımı sırasında psikolojik ve fiziksel risk alıp almama durumu olarak belirtmiştir. SBGF ise Şahinaslan, ve diğerleri (2009) tarafından; kişilerin geçmiş veya güncel ne tür tehlikeler olduğu konusunda bilgilendirilmesi, bu tehlikelerin olası etkilerinden nasıl korunacağı konusunda bilgilendirilmesi olarak tanımlanmıştır. Yani dijital sağlık teknoloji kullanımı sırasında psikolojik ve fiziksel sorunlarla alakalı iken, SBGF daha çok teknoloji kullanımı sırasında oluşabilecek güvenlik açıkları ile alakalıdır. Dolayısı ile bu iki değişken arasında sifıra yakın ilişkinin beklenen bir sonuç olduğu söylenebilir. Bir diğer sonuca göre ise; SBGF ile dijital güvenlik düzeyi arasında zayıf düzeyde ilişki tespit edilmiştir. Çalışma sonucunda bu iki değişken arasında yüksek ilişki olması beklenirken zayıf ilişki tespit edilmiştir. Aslan(2018) ölçekteki madde sayısının nitelik ve nicelik bakımın istenen kalitede ve sayıda olması gerektiğini vurgulamıştır. Ayrıca ölçekteki madde sayısı arttığında ölçeğin ölçmek istenen davranışı daha iyi

ölçeğini belirtmiş, ölçeğin geçerliliğinin bundan olumlu etkileneceğinin üzerinde durmuştur. Kullanmış olduğumuz DV ölçeğinin alt boyutu olan dijital güvenlik bu ölçekte sadece 3 madde ile ölçülmeye çalışılmıştır. Bu maddeler bu değişkeni ölçmede tam anlamıyla yeterli olmamış olabilir.

Sonuç olarak bölüm bazında SBGF ve DV düzeyleri incelendiğinde; SBGF bakımından bölümlerin yarısı ortalamanın altında kalmışken, diğer bölümlerle anlamlı farklılaşma sadece BÖTE ve Yabancı Dil Öğretmenliği bölümlerindedir. Toplam SBGF puanlarına bakıldığında ise orta düzeyde bir farkındalıklarının olduğunu söylemek mümkündür. MEB (2012) tarafından çalışanlarına yönelik siber bilgi güvenliği anketi uygulanmıştır. Şifre güvenliği konusunda sorulan soruya yalnızca %6.81'i "Şifremi çok sık değiştiriyorum", %21.28'i "Şifremi altı aydan daha kısa sürede değiştiriyorum şeklinde cevap vermiştir. Ayrıca %31,83'ü şifre belirlerken unutmayacağı kolay şifre koymaktadır. Bu anket sonuçları da göstermektedir ki görevdeki öğretmenlerin de siber bilgi güvenliği yeterli seviyede değildir. Bilindiği üzere yeni eğitim yaklaşımları daha çok önleyici yöntemler izlemektedir. Yani bir sorun yaşanmadan varsayımlar üzerine sorunu çözmeye odaklanır. Görevdeki öğretmenlerin siber bilgi güvenliği farkındalıklarının düşük çıkması bu yaklaşımla örtüşmemektedir. Öğretmenler göreve başlamadan; yani henüz öğretmen adayı iken, hem siber bilgi güvenliği farkındalıkları hem de dijital vatandaşlık düzeylerini artırmaya yönelik gerekli önlemler alınmalıdır. Bu bağlamda üniversite müfredatlarında yapılacak bazı düzenlemelerin bu sorunların önüne geçeceği öngörülmektedir.

Alan yazın incelendiğinde çalışmalarda benzer sonuçlar bulunsa da aksi sonuçlara rastlamak da mümkündür. Bunun nedeni olarak farklı meslek grupları ile çalışmalar yapılıyor olması, üniversitelerde ders programlarının farklılığı gösterilebilir. Bizim çalışmamızda olduğu gibi öğretmen adayları içerisinde BÖTE bölümü diğer bölümlerden farklılaşma sebebi bölümüm ders içeriğidir. Bu bağlamda BÖTE bölümünün eğitim fakültelerinde daha etkin kullanılması gerektiği düşünülmektedir. Eğitim fakültelerinde BÖTE' bölümüne ayrı bir önem verilmeli, diğer bölümlerdeki akademisyenlere ve öğretmen adaylarına kılavuzluk yapmaları sağlanmalıdır. Bunun sağlanması için eğitim fakültesinin diğer bölümlerine siber bilgi güvenliği ve dijital vatandaşlık konularını kapsayan dersler eklenmeli, bu derslerin ise BÖTE bölümü akademisyenleri tarafından verilmesi sağlanabilir.

Yine bilgisayar mühendisliği ve yazılım mühendisliği gibi teknoloji ile daha fazla iç içe olan bölümler ile sağlık çalışanları, bazı kamu personelleri gibi teknoloji ile daha az iç içe olanların farkındalıkları aynı değişkenlere göre benzer sonuçlar vermeyebilir. Ayrıca çalışmaların farklı yıllarda yapılıyor olması ve teknolojinin hızla ilerliyor olması bu sonuçların farklılaşmasına neden olmuş olabilir. Birkaç yıl içinde çıkan yeni teknoloji veya sosyal medya platformları bu farkındalıkları etkilemiş olabilir. Sensortower'in (2020) verileri incelendiğinde 2016 yılında kurulan 2017 yılında ise indirmede ilk 10 sırada bile olmayan "Tiktok" uygulaması 2020 yılında

1.6 Milyar indirme ile dünya genelinde en çok indirilen 2. uygulama olmuştur. Türkiye'nin ise en çok indirenler sıralamasında Hindistan ve ABD'den sonra 3. sırayı aldığı görülmektedir. Yine bazı çalışmalarda örneklem sayısının düşük olması genellemelerin yapılamamasına neden olabilir.

5.1.Uygulamaya Yönelik Öneriler

Toplumların siber bilgi güvenliği farkındalığı ve dijital vatandaşlık seviyelerinin artırılmasında öğretmenler, okul yöneticileri, Milli Eğitim Bakanlığı ve hükümet politikaları önemli olabilmektedir. Bunlara ek olarak önümüzdeki yıllarda eğitim-öğretim kurumlarında görev alacak öğretmen adayları da dijital çağ olarak adlandırılan günümüzde toplumların bilgi güvenliği ve dijital vatandaşlık alanlarında önemli rol oynayabileceklerdir. Bu iki değişkene yönelik farkındalıkların artırılması için;

Yapmış olduğumuz alan yazın çalışmasında da vurguladığımız gibi üniversitelerin eğitim fakültelerinde siber güvenlik ve dijital vatandaşlığa yönelik dersler yok denecek kadar azdır. Bazı üniversitelerin mühendislik fakültelerinde siber bilgi güvenliğine yönelik dersler mevcuttur. Fakat bunların neredeyse tamamı Yüksek Lisans seviyesindedir. Bazı eğitim fakültelerinde sosyal bilgiler öğretmenliği ders içeriğinde dijital vatandaşlık kavramına yönelik dersler verilse de ne siber bilgi güvenliğine ne de dijital vatandaşlığa yönelik direkt bir ders tespit edilememiştir. Bu bağlamda üniversitelerin başta eğitim fakültelerinde siber bilgi güvenli ve dijital vatandaşlık zorunlu ders kapsamına alınması geleceğin toplumlarını yetiştirecek öğretmen adaylarının siber bilgi güvenliği farkındalıklarının ve dijital vatandaşlık seviyelerinin artmasına ve yetiştirdikleri öğrencilere bu konuda daha iyi yol gösterici olmalarına imkan sağlayabilir.

Ayrıca, üniversitelerde siber bilgi güvenliği ve dijital vatandaşlık toplulukları oluşturulması desteklenerek üniversitelerdeki dijital teknoloji ve güvenlik kültürü oluşturulabilir.

Üniversitelerde düzenlenecek seminerlerle siber bilgi güvenliği ve dijital vatandaşlık farkındalıkları artırılması sağlanabilir.

Özellikle çalışma sonuçlarında siber bilgi güvenliği ve dijital vatandaşlık düzeyleri düşük çıkan bölümlerin YÖK programları incelenerek siber bilgi güvenliğine ve dijital vatandaşlığa yönelik dersler eklenebilir.

BÖTE bölümü öğretmen adayları tarafından diğer öğretmen adaylarına akran eğitimi sunulabilir.

Belli dönemlerde uzaktan eğitimler ile tüm eğitim fakültesi bölümü öğretmen adaylarına siber bilgi güvenliği eğitimi verilebilir.

Milli Eğitim Bakanlığı ile iş birliğinde olunarak Bilişim Teknolojileri ve Yazılım Dersi (BTY) müfredatı yeniden düzenlenebilir. Müfredatta var olan siber güvenlik ve dijital vatandaşlık

konularının kapsamı genişletilebilir. BTY dersi dışında siber güvenlik ve dijital vatandaşlık dersi adı altında bir ders müfredata eklenebilir. Sosyal Bilgiler dersi kapsamında bulunan dijital vatandaşlık konusunun kapsamı genişletilerek ünite sayısı ve kademe sayısı arttırılabilir.

Hali hazırda görevde bulunan öğretmenlerin siber bilgi güvenliği farkındalığını ve dijital vatandaşlık düzeyini arttırmaya yönelik hizmet içi eğitimler gerçekleştirilebilir. Okul yöneticilerine verilecek hizmet içi eğitimler ile farkındalıkları arttırılabilir.

Ara tatil dönemlerinde ve yaz tatili döneminde gerçekleştirilen seminer etkinliklerine siber bilgi güvenliği ve dijital vatandaşlık eğitimleri eklenerek görevdeki öğretmenlerin farkındalıkları arttırılabilir.

İlkokul hayat bilgisi dersi müfredatına siber bilgi güvenliği ve dijital vatandaşlık konuları eklenerek erken yaşta farkındalık oluşturulabilir.

Eğitim Bilişim Ağı (EBA) içerisinde bulunan siber güvenlik portalı içerik olarak düzenlenerek zenginleştirilebilir. EBA'ya dijital vatandaşlık portalı eklenerek yeni içerikler eklenebilir.

Okul bir bütün olduğu düşünüldüğünde velilerin de bundan soyutlanamayacağı bir gerçektir. Bu kapsamda gerek uzaktan gerekse yüz yüze eğitimler ile velilere yönelik de siber bilgi güvenliği farkındalığı ve dijital vatandaşlık farkındalığı verilebilir.

Bu kadar önemli bir konu hususunda devlet eli ile kamu spotları medyada yayınlanabilir.

Milli Eğitim Bakanlığı ve Üniversitelerin iş birliği ile siber güvenlik toplulukları ve dijital vatandaşlık toplulukları veli ziyaretleri ile farkındalık çalışmaları gerçekleştirebilir.

5.2.Yapılacak Araştırmalara Yönelik Öneriler

Bu çalışma Akdeniz Bölgesi'nde bir devlet üniversitesinin Eğitim Fakültesi öğretmen adaylarını kapsamaktadır. Alan yazın taramaları sonuçlarında Siber Bilgi Güvenliği ve Dijital Vatandaşlık düzeylerini bölümlere göre inceleyen çalışmaya rastlanamamıştır. Çalışmanın genellenebilmesi için sadece bir üniversitenin Eğitim Fakültesindeki öğretmen adaylarından oluşan bir örneklem yeterli olmayabilir. Bunun için örneklem genişletilerek Türkiye'nin her bölgesinden çeşitli üniversitelerin Eğitim Fakültelerinde ve daha farklı bölümlerde öğrenim gören öğretmen adayları ile çalışılabilir. Başka bir çalışmada siber bilgi güvenliği ve dijital vatandaşlık düzeyleri düşük çıkan bölümler ile derinlemesine bir nitel çalışma yapılabilir.

Farklı Üniversitelerden aynı bölümler arası farklılaşmalar ve nedenlerinin tespiti çalışması yapılabilir.

Siber Güvenlik Farkındalığını ve Dijital Vatandaşlığı düzeyini etkileyen birçok farklı etkenin olduğu düşünülmektedir. Bunu için farklı değişkenlerin etkisi incelenebilir.

Bu çalışma sadece öğretmen adayları ile gerçekleştirilmiştir. Farklı meslek grupları ile öğretmen adaylarının siber bilgi güvenliği karşılaştırılabilir.

Çalışma, görev yapmakta olan farklı branştan öğretmenlerin siber bilgi güvenliği ve dijital vatandaşlık düzeylerinin tespiti ile genişletilebilir. Gelecekte okul yöneticilerinin siber bilgi güvenliği farkındalıklarını ve dijital vatandaşlık düzeylerini tespite yönelik çalışma yapılabilir.

Eğitim sürecinin bir parçası olan veliler de çalışmaya dâhil edilerek farkındalıkları araştırılabilir. Dijital vatandaşlığın 9 alt boyutu ayrı ayrı ele alınarak her biri ile ilgili farkındalık çalışmaları yapılabilir.

BTY derslerindeki siber güvenlik ve dijital vatandaşlık derslerinin etkinliğinin tespitine yönelik çalışmalar yapılabilir. Eğitim fakültelerine siber bilgi güvenliği dersi eklenmesi durumunda dersin etkililiğinin tespitine yönelik çalışmalar gerçekleştirilebilir



KAYNAKÇA

- [1.] Acun, R. (2000). İnternet ve telif hakları. *Bilgi Dünyası*, 1(1), 5-26.
- [2.] Alnajim, A., & Munro, M. (2008, November). An evaluation of users' tips effectiveness for phishing websites detection. In 2008 Third International Conference on Digital Information Management (pp. 63-68). IEEE.
- [3.] Alptekin.H.,(2018). Stuxnet Virüsü.(2018, 6 Aralık). Erişim Adresi:<http://www.halitalptekin.com/stuxnet-virusu.html>
- [4.] Ankara Üniversitesi. Bilgi Toplumu ve Toplumun Bilgilenmesinde Kütüphanelerin Rolü.(2018,5 Eylül). Erişim Adresi: <http://acikarsiv.ankara.edu.tr/browse/5/>
- [5.] Aslan, Ş., Güzel Ş. (2018) Sosyal Bilimlerde Araştırma Yöntemleri. Aslan, Ş(Ed) Nicel, Nitel ve Karma Tasarımlar İçin Bir Rehber (s.150-160) içinde Ankara= Eğitim Yayınevi
- [6.] Avast. What is Malware.(2018, 20 Ekim) Erişim Adresi: <https://www.avast.com/c-malware>
- [7.] AVG. Keyloggers: what they are, where they come from, and how to remove them.(2018, 25 Ekim). Erişim Adresi:<https://www.avg.com/en/signal/keyloggers-what-they-are-where-they-come-from-and-how-to-remove-them>
- [8.] Aytekin.A.(2015) Türkiye'nin siber güvenlik stratejisi ve eylem planının değerlendirilmesi.(Yüksek Lisans Tezi). Gazi Üniversitesi Bilişim Enstitüsü, Ankara.
- [9.] Barışkan,M.,A.(2017). Türkiye'deki siber güvenlik bilinci ve sosyal mühendislik ataklarına karşı savunma önlemlerinin geliştirilmesi. (Yüksek lisans tezi).İstanbul üniversitesi fen bilimleri enstitüsü, İstanbul.
- [10.] Barrett, N. (2003). Penetration testing and social engineering-Hacking the weakest link. *Information Security Technical Report*, 4(8), 56-64. Doi: 10.1016/S1363-4127(03)00007-4
- [11.] BAYRAK, T. (2017). Sosyal Medyada Dijital Etik: Twitter'da Şiddet İçerikli İletilerin İncelenmesi. *Yeni Medya Elektronik Dergisi*, 1(1), 32-46.
- [12.] Bayrak.H., (2017).İstatistiksel Analiz Türleri.(2018,12 Ocak). Erişim Adresi:<https://dijilopedi.com/dijital-pazarlamada-istatistiksel-analiz-turleri/>
- [13.] Bayraktar, G., & Hiperlink (Firm). (2015). Siber savaş ve ulusal güvenlik stratejisi. İstanbul: İstanbul.
- [14.] Bayraktaroğlu, S., Özdemir, Y., ARAS, A. G. M., & Özdemir, A. G. S. (2015). Mavi Yakalı Çalışanlar: Neden Akademik Çalışmalar İçin Cazip Bir Örneklem Değil?. *ISGUC The Journal of Industrial Relations and Human Resources*, 17(3), 138-157.
- [15.] Berberoğlu, B. (2010). Bilgi toplumu ve bilgi ekonomisi oluşturma yolunda Türkiye ve Avrupa birliği. *Marmara Üniversitesi İktisadi ve İdari Bilimler Dergisi*, 29(2), 111-131.
- [16.] Berrier, T. (2007). Sixth-, Seventh-, and Eighth-Grade Students' Experiences with the Internet and Their Internet Safety Knowledge.
- [17.] Beyer, A. ve Westendorf, C. (2009). How to establish security awareness in schools. Pohlmann, N., Reimer, H. ve Schneider, W. (Ed.), *Securing Electronic Business Processes*. (177-186). Kranzberg: Vieweg.
- [18.] BIÇAKCI, S. (2014). Nato'nun gelişen tehdit algısı: 21. yüzyılda siber güvenlik. *Uluslararası İlişkiler Dergisi*, 10(40), 100-130.
- [19.] Bıçakçı, S., Ergun, D., & Çelikpala, M. (2015). Türkiye'de siber güvenlik. *EDAM Siber Politika Kağıtları Serisi*, (1).
- [20.] Bilgi Teknolojileri ve İletişim Kurulu. Siber Güvenlik(2018, 6 Aralık). Erişim Adresi:<https://www.btk.gov.tr/siber-guvenlik-mevzuat>
- [21.] Büyükköztürk, Ş., Çakmak, E. K., Akgün, Ö. E., Karadeniz, Ş., & Demirel, F. (2016). Bilimsel araştırma yöntemleri: *Örnekleme Yöntemleri*.(1-350)Ankara:Pegem Akademi.
- [22.] Canpolat, Ö. (2001). *E-ticaret ve Türkiye'deki gelişmeler*. Sanayi ve Ticaret Bakanlığı.
- [23.] Cisco. What is The CyberSecurity.(2018, 5 Ekim). Erişim Adresi: <https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html>

- [24.] Clarke, R. A., Knake, R. K., & Erduran, M. (2011). *Siber savaş: ulusal güvenliğe yönelik yeni tehdit*. İstanbul Kültür Üniversitesi.
- [25.] Çakır, H., Hava, K., Gülen, Ş. B., & Özudođru, G. (2015). Öğretmen adaylarının sosyal ağ sitelerinde güvenlik farkındalıklarının incelenmesi. *International Journal of Human Sciences*, 12(1), 887-902.
- [26.] Çakmak, V. (2016). Çocuk ve dijital oyun etkileşimine etiksel bir bakış. *ICHACS*, 430.
- [27.] ÇEPNİ, O., OĞUZ, S., & KILCAN, B. (2014). İlköğretim Öğrencilerinin Dijital Vatandaşlığa Yönelik Görüşleri. *Turkish Journal of Social Research/Turkiye Sosyal Arastirmalar Dergisi*, 18(3).
- [28.] ÇETİN, H. (2014). Kişisel veri güvenliği ve kullanıcıların farkındalık düzeylerinin incelenmesi. *Akdeniz Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 14(29), 86-105.
- [29.] Çubukcu, A., & Bayzan, Ş. (2013). Türkiye’de dijital vatandaşlık algısı ve bu algıyı internetin bilinçli, güvenli ve etkin kullanımı ile artırma yöntemleri. *Middle Eastern & African Journal of Educational Research*, 5, 148-174.
- [30.] Çukurçayır, M. A., & Çelebi, E. (2012). Bilgi toplumu ve e-devletleşme sürecinde Türkiye. *Uluslararası Yönetim İktisat ve İşletme Dergisi*, 5(9), 59-82.
- [31.] Dağhan, G, Nuhoglu Kibar, P , Menzi Çetin, N , TELLİ, E , Akkoyunlu, B . (2017). BİLİŞİM TEKNOLOJİLERİ ÖĞRETİM ADAYLARININ BAKIŞ AÇISINDAN 21. YÜZYIL ÖĞRENEN VE ÖĞRETİM ÖZELLİKLERİ. *Eğitim Teknolojisi Kuram ve Uygulama*, 7 (2) , 215-235. DOI: 10,17943/etku.30506
- [32.] Daneels, A., & Salter, W. (1999). Selection and evaluation of commercial SCADA systems for the controls of the CERN LHC experiments.(2019, 26, Ağustos). Erişim Adresi:<http://cds.cern.ch/record/532627/files/ta2o01.pdf>
- [33.] Delialiođlu, Ö. (2014). Bilişim Sistemleri Güvenliği ve İlgili Etik Kavramlar. A. Şentürk (Ed.), *Temel Bilgi Teknolojileri ve Bilgisayar Kullanımı* (509-538). Bursa: Ekin Yayınevi.
- [34.] Digitalguardin. What is Cyber Security? Definition, Best Practices & More.(2018,5 Ekim). Erişim Adresi: <https://digitalguardian.com/blog/what-cyber-security>
- [35.] Dlamini, M. T., Eloff, J. H., & Eloff, M. M. (2009). Information security: The moving target. *computers & security*, 28(3-4), 189-198. Erişim Adresi:<https://doi.org/10.1016/j.cose.2008.11.007>
- [36.] Dutch Ministry of Security and Justice, ‘The National Cyber Security Strategy (NCSS). Strength through Cooperation,’ (The Hague: National Coordinator for Counterterrorism and Security, 2011), 4.
- [37.] ELÇİ, A, SARI, M . (2016). Bilişim Teknolojileri Ve Yazılım Dersi Öğretim Programına Yönelik Öğrenci Görüşlerinin Dijital Vatandaşlık Bağlamında İncelenmesi. *Çukurova Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 25 (3) , 87-102. Retrieved from<https://dergipark.org.tr/tr/pub/cusosbil/issue/32038/353253>
- [38.] EMİNAĞAOĞLU, M., & GÖKŞEN, Y. (2009). Bilgi Güvenliği Nedir, Ne Değildir? Türkiye’de Bilgi Güvenliği Sorunları ve Çözüm Önerileri.
- [39.] Ercan,M.(2015). Kritik altyapıların korunmasına ilişkin belirlenen siber güvenlik stratejileri.(Yüksek lisans tezi). Gebze teknik üniversitesi sosyal bilimler enstitüsü. Gebze. ErişimAdresi:<https://www.statista.com/statistics/617136/digital-population-worldwide/>
- [40.] Erol,S.E. (2016) SİBER GÜVENLİK FARKINDALIĞI İÇİN YETENEK TABANLI DİNAMİK MODEL(Yayınlanmış Yüksek Lisans Tezi) Gazi Üniversitesi, Ankara
- [41.] Eset İnternet Securty. Antivirüs ve Zararlı Yazılım Koruması.(2018, 20 Ekim). Erişim Adresi:https://www.eset.com/tr/internet-security/?gclid=CjwKCAjwpKveBRAwEiwAo4Pqm4v1AnhS_E6NKjafK1_Li8l20YxbsFUjiNdAXkYQ35h6Sdp9VN00YhoCZMsQAvD_BwE
- [42.] Eshet, Y. (2004). Digital literacy: A conceptual framework for survival skills in the digital era. *Journal of educational multimedia and hypermedia*, 13(1), 93-106.

- [43.] Eurostat Statistics Explained. E-commerce Statistics For Individuals.(2018,15 Ağustos). ErişimAdresi:http://ec.europa.eu/eurostat/statistics-explained/index.php/E-commerce_statistics_for_individuals#General_overview.
- [44.] Evrin, V., & Demirer, M. (2011). Kurumsal Bilgi Güvenliği Süreç Çalışmaları: ISO/IEC-27001 Örneği. *IV. Ağ ve Bilgi Güvenliği Sempozyumu Bildiriler Kitabı*, 25-33.
- [45.] Farmer, L. (2010). 21. Century standarts for information literacy. *Leadership*, 39(4), 20-
- [46.] Farmer, L. (2014). How AASL learning standards inform ACRL's information literacy framework. Erişim Adresi: <http://library.ifa.org/831/1/072-farmer-en.pdf>
- [47.] Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. *Survival*, 53(1), 23-40. <https://doi.org/10.1080/00396338.2011.555586>.
- [48.] Field, A. (2013). *IBM SPSS istatistiklerini kullanarak istatistikleri keşfetme*. Adaçayı.
- [49.] Fraenkel, J. R., Wallen, N. E. & Hyun, H.H. (2012). *How to design and evaluate research in education. 8th Edition*. The McGraw-Hill Companies, ABD.
- [50.] Good, N., Grossklags, J., Thaw, D., Perzanowski, A., Mulligan, D. K., & Konstan, J. (2006). User choices and regret: Understanding users' decision process about consensually acquired spyware. *I/S: A Journal of Law and Policy for the Information Society*, 2(2), 283-344.
- [51.] Göçoğlu, V. (2018). Türkiye'nin Siber Güvenlik Politikalarının Kamu Politikası Analizi Çerçevesinde Değerlendirilmesi.(Doktora Tezi).
- [52.] Gökçearslan(2005). İlk Ve Ortaöğretim Öğrencilerinin Evde Bilgisayar Kullanımına İlişkin Öğrenci Ve Veli Görüşleri. Hacettepe Üniversitesi. Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı. Ankara
- [53.] Gökmen.Ö.,F.(2014).Bilgisayar ve öğretim teknolojileri eğitimi öğretmen adaylarının bilişim güvenliği eğitimi verebilme yeterliklerinin incelenmesi.(Yüksek Lisans Tezi). Bilgisayar ve öğretim teknolojileri eğitimi bilim dalı. Sakarya.
- [54.] GÖRMEZ, E. (2016). ÖĞRETMEN ADAYLARININ" DİJİTAL VATANDAŞLIK VE ALT BOYUTLARI" HAKKINDAKİ GÖRÜŞLERİ (BİR DURUM ÇALIŞMASI). *Electronic Turkish Studies*, 11(21).
- [55.] Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *computers & security*, 73, 345-358.
- [56.] Güldüren, C.(2015) Yükseköğretim kurumlarındaki öğretim elemanlarının bilgi güvenliği farkındalık düzeylerinin değerlendirilmesi(Doktora Tezi). Erişim Adresi:<http://acikarsiv.ankara.edu.tr/browse/27740/>
- [57.] Güldüren, C., Çetinkaya, L., & Keser, H. (2016). Ortaöğretim öğrencilerine yönelik bilgi güvenliği farkındalık ölçeği (BGFÖ) geliştirme çalışması. *İlköğretim Online*, 15(2).
- [58.] Günel, A. (2004). Regresyon denkleminin başarısını ölçmede kullanılan belirleme katsayısı ve kritiği.
- [59.] Hanewald, R. (2008). Confronting the pedagogical challenge of cyber safety. *Australian journal for teacher education*, 33(3), 1-16.
- [60.] Hauben, M. (2007). History of ARPANET. Site de l'Instituto Superior de Engenharia do Porto, 17.
- [61.] Hekim, H., & BAŞIBÜYÜK, O. (2013). Siber Suçlar ve Türkiye'Nin Siber Güvenlik Politikaları. *Uluslararası Güvenlik ve Terörizm Dergisi*, 135-158.
- [62.] Henkoğlu, H. Ş., Mahiroğlu, A., & Keser, H. (2015). Ortaokul öğrencilerinin bilgiye erişim aracı olarak İnternete yaklaşımları: Betimleyici bir çalışma. *Turkish Online Journal of Qualitative Inquiry*, 6(1), 72-110.
- [63.] Hollandsworth, R., Dowdy, L., & Donovan, J. (2011). Digital citizenship in K-12: It takes a village. *TechTrends*, 55(4), 37-47.
- [64.] Iğure, V. M., Laughter, S. A., & Williams, R. D. (2006). Security issues in SCADA networks. *Computers & Security*, 25(7), 498-506.
- [65.] International Telecommunication Union. (2008). Series X: Data Networks, Open System Communications and Security, Overview of Cybersecurity; ITU-T Recommendation, 8-12.

- [66.] İŞEVI, A. S., & ÇELME, B. (2005). Bilgi çağında yeni hazine: Entelektüel sermayeyle rekabeti yakalamak. *Bilgi Dünyası*, 6(2), 251-267.
- [67.] İŞMAN, A., & CANAN GÜNGÖREN, O. (2014). Digital citizenship. *Turkish Online Journal of Educational Technology-TOJET*, 13(1), 73-77.
- [68.] JACKSON, A. L., INGER, R., PARNELL, A. C., & BEARHOP, S. (2011). Comparing isotopic niche widths among and within communities: SIBER–Stable Isotope Bayesian Ellipses in *R. Journal of Animal Ecology*, 80(3), 595-602. Erişim Adresi:<https://doi.org/10.1111/j.1365-2656.2011.01806.x>
- [69.] JANG-JACCARD, J., & NEPAL, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, 80(5), 973-993. Erişim Adresi: <https://doi.org/10.1016/j.jcss.2014.02.005>
- [70.] JARGON File(2019, 16, Ağustos).Erişim Adresi:<http://www.catb.org/~esr/jargon/oldversions/jarg447.txt>
- [71.] 3756 Nolu Kanun. (2019,08 Aralık).Erişim Adresi:<https://www.resmigazete.gov.tr/arsiv/20901.pdf>
- [72.] 5237 Kanun. (2019,08 Aralık). Erişim Adresi:<https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf>
- [73.] KAPLAN, A. M., & HAENLEIN, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business horizons*, 53(1), 59-68.
- [74.] KARA,M.(2013). Siber saldırılar - siber savaşlar Ve Etkileri. İstanbul bilgi üniversitesi sosyal bilimler enstitüsü bilişim ve teknoloji hukuku yüksek lisans Programı. İstanbul.
- [75.] KARABULUT, B. (2015). Bilgi Toplumu Çağında Dijital Yerliler, Göçmenler ve Melezler. *Pamukkale Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, (21), 11-23.
- [76.] KARASAR, N. (1991). Bilimsel araştırma teknikleri. *Ankara: Sanem Matbaacılık*, 4.
- [77.] KARASAR, N. (2012). Bilimsel araştırma yöntemi (23. bs.).(1-292) *Ankara: Nobel Yayıncılık*.
- [78.] KASPERSKY. Bilgisayar Virüsü veya Bilgisayar Solucanı Nedir?.(2018, 20 Ekim). Erişim Adresi:<https://www.kaspersky.com.tr/resource-center/threats/viruses-worms>
- [79.] KASPERSKY. Reklam Yazılımı Nedir? (2018, 28 Ekim).Erişim Adresi:<https://www.kaspersky.com.tr/resource-center/threats/adware>
- [80.] KASPERSKY. Truva Atı Virüsü Nedir?.(2018, 20 Ekim). Erişim Adresi:<https://www.kaspersky.com.tr/resource-center/threats/trojans>
- [81.] KAYA, A., & KAYA, B. (2014). Teacher candidates' perceptions of digital citizenship Öğretmen adaylarının dijital vatandaşlık algısı. *Journal of Human Sciences*, 11(2), 346-361.
- [82.] KAYA, A., & ÖĞÜN, M. (2013). Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler. *Güvenlik Stratejileri Dergisi*, 158-170
- [83.] KEMP,S.,(2017). Wearesocial. Digital In 2017: Global Overview.(2018.5 Ağustos).Erişim Adresi: <https://wearesocial.com/uk/special-reports/digital-in-2017-global-overview>
- [84.] KESKİN, Ş. (2017). Realizm Ve Liberalizm Işığında Siber Savaş Ve Alternatif Bir Kavram Olarak Siber Barış'ın Değerlendirilmesi. *TURAN-SAM*, 9(35), 287-297. Erişim Adresi:<https://doi.org/10.1111/j.1365-2656.2011.01806.x>
- [85.] KIRIK, A. M., BÖLÜKBAŞ, K., & CENGİZ, G. Sosyal Medya Bağlamında Dijital Vatandaşlık: TRT İstanbul Radyosu Prodüktörleri Üzerinden Bir Değerlendirme. *Mavi Atlas*, 7(2), 1-27.
- [86.] Kişisel Verilerin Korunması Kanunu Tasarısı. (2019,08 Aralık). Erişim Adresi:https://www.tbmm.gov.tr/develop/owa/komisyon_tutanaklari.mv_goruntule?pTutanakId=6269
- [87.] KLIMBURG, A. (2012). NATIONAL CYBER SECURIT. Estonia: NATO CCD COE Publication.
- [88.] KÖKLÜ, N., BÜYÜKÖZTÜRK, Ş., & ÇOKLUK-BÖKEOĞLU, Ö. (2007). *Sosyal bilimler için istatistik*. Pegem A Yayıncılık.
- [89.] KÖKLÜ, N., BÜYÜKÖZTÜRK, Ş., & ÇOKLUK-BÖKEOĞLU, Ö. (2007). *Sosyal bilimler için istatistik*. Pegem A Yayıncılık.
- [90.] KROGH, V., ICHIGO, K. ve NONAKA, I. (2002). *Bilginin üretimi*. İstanbul: Dışbank Yayınları.
- [91.] LANGNER, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy*, 9(3), 49-51. DOI: 10.1109/MSP.2011.67

- [92.] Luo, X. R., Zhang, W., Burd, S., & Seazzu, A. (2013). Investigating phishing victimization with the Heuristic-Systematic Model: A theoretical framework and an exploration. *Computers & Security*, 38, 28-38. Erişim Adresi: <https://doi.org/10.1016/j.cose.2012.12.003>
- [93.] Mahabi, V. (2010). *Information security awareness: system administrators and end-user perspectives at Florida State University* (Doctorate of Philosophy). The Florida State University, Florida. Erişim Adresi: <http://diginole.lib.fsu.edu/islandora/object/fsu:181044/datastream/PDF/view>
- [94.] Mahmutoğlu, A. (2009). Etik ve Ahlak, Benzerlikler, Farklılıklar ve İlişkiler. *Türk İdare Dergisi*, 81(463-464), 225-249.
- [95.] Mart 2019 itibariyle en fazla internet kullanıcısı olan ülkeler (milyonda). (2019, 21 Ağustos). Erişim Adresi: <https://www.statista.com/statistics/262966/number-of-internet-users-in-selected-countries/>
- [96.] Mart, İ. (2012). Bilişim kültüründe bilgi güvenliği farkındalığı. (Yüksek lisans tezi). Bilgisayar ve öğretim teknolojileri eğitimi anabilim dalı. Kahramanmaraş.
- [97.] Meral, M. (2015). Siber Güvenlik Kapsamında Kritik Altyapıların Korunmasının Önemi (Yayımlanmış Yüksek lisans tezi). Harp Akademileri Stratejik Araştırmalar Enstitüsü, İstanbul.
- [98.] Milli Eğitim Bakanlığı. Anket Programı. (2018, 6 Aralık). Erişim Adresi: http://mebk12.meb.gov.tr/meb_iys_dosyalar/20/01/747411/dosyalar/2016_04/19092506_02044116_bilgigvenliianketsonu.pdf
- [99.] METİN, A. (1999). İnternet ve Dermatolojide Kullanımı. *Turkiye Klinikleri Journal of Dermatology*, 9(3), 175-186.
- [100.] Mitnick, K.D., Simon, L.W. ve Wozniak, S., (2003) , *The Art Of Deception: Controlling The Human Element Of Security*, Wiley Publishing, New York.
- [101.] Muradoğlu, C., (2020). Stuxnet Virüsü. (2020, 19 Mart). Erişim Adresi: <https://webrazzi.com/2020/03/19/istegelsin-e-gelen-siparis-talebi-bir-haftada-yuzde-80-artti/>
- [102.] Nalbant, F. (2014). Türkiye’de vatandaşlık anlayışının gelişimi. *Bildiriler Kitabı-I*, 79.
- [103.] Ocak, M.A. (2013). Aile ve İnternet. Aile Eğitim Programı: (2020, 5 Ocak). Erişim Adresi: <http://www.aep.gov.tr/wp-content/uploads/2012/10/AileVeInternet.pdf>
- [104.] Ohler, J. B. (2010). *Digital community, digital citizen*. Corwin Press. DOI: <http://dx.doi.org/10.4135/9781452219448.n8>
- [105.] Ortadoğu Teknik Üniversitesi. Dünya’da İnternet’in Gelişimi. (2018, 12 Kasım). Erişim Adresi: <http://www.internetarsivi.metu.edu.tr/tarihce.php>
- [106.] Oyedemi, T. T. D. (2012). *The partially digital: Internet, citizenship, social inequalities, and digital citizenship in South Africa*. University of Massachusetts Amherst.
- [107.] Ozcan, N., & Buzlu, S. (2005). PROBLEMLİ İNTERNET KULLANIMINI BELİRLEMEDE YARDIMCI BİR ARAÇ: "İNTERNETTE BİLİŞSEL DURUM ÖLÇEĞİ" NİN ÜNİVERSİTE. *Journal of Dependence*, 6(1), 19-26.
- [108.] ÖNAÇAN, M , Atan, H . (2016). SİBER GÜVENLİKTE LİSANSÜSTÜ EĞİTİM: DENİZ HARP OKULU ÖRNEĞİ. *Trakya Üniversitesi Mühendislik Bilimleri Dergisi*, 17 (1), 13-21. Erişim Adresi: <http://dergipark.org.tr/tujes/issue/21551/37029>
- [109.] Özbilgin, İ.G., (2018). Kamu Bilişimcileri Derneği. Twitter’da Oltaya Gelme. (2018, 20 Ekim). Erişim Adresi: <http://www.kbd.org.tr/kategori/yazilar/67025/twitter-da-oltaya-gelme>
- [110.] Özdemir, M. (2010). Nitel veri analizi: Sosyal bilimlerde yöntem bilim sorunsalı üzerine bir çalışma. *Eskişehir Osmangazi Üniversitesi Sosyal Bilimler Dergisi*, 11(1).
- [111.] Özsoy, T. (2009). *Fastfood’dan Facebook’a: İnternet Bağımlılığı*. Akademik Bilişim. Harran Üniversitesi: Şanlıurfa.
- [112.] Öztürk, Ö. (2009). E-postalarda spam sorunu ve çözüm önerileri. (Uzmanlık Tezi), Erişim Adresi: http://afyonluoglu.org/PublicWebFiles/Reports-TR/Uzmanlik_Tez/BTK/siber/2009%20Temmuz%20ePostalarda%20Spam%20Sorunu.PDF

- [113.] Parlak,A.(2005). İnternet ve Türkiye'ye internetin gelişi.(Bitirme Tezi). Fırat Üniversitesi Mühendislik Fakültesi, Elazığ.
- [114.] Pekel,A.(2010). Bilişim Teknolojilerinde Yönetişim. Bilgi Teknolojileri Yönetişim ve DenetimKonferansı(BTYD),Ankara(2010).ErişimAdresi:<http://www.btyd.org.tr/documents/451b318c0fc45015d3c495185c23628e?1350291535>
- [115.] Puhakainen, P., & Ahonen, R. (2006). Design theory for information security awareness.
- [116.] Pusey, P., & Sadara, 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), 82-85.
- [117.] Rao,U.H, and Nayak,U.(2014). The InfoSec Handbook: An Introduction to Information Security New York, Apress Media LLC. (2019,15 Aralık). Erişim Adresi:https://play.google.com/store/books/details/Umesha_Nayak_The_InfoSec_Handbook?id=Qe9lBAAAQBAJ
- [118.] Rao,U.H, and Nayak,U.(2014). The InfoSec Handbook: An Introduction to Information Security New York, Apress Media LLC. (2019,15 Aralık). Erişim Adresi:https://play.google.com/store/books/details/Umesha_Nayak_The_InfoSec_Handbook?id=Qe9lBAAAQBAJ
- [119.] Revenue from information security and vulnerability management market worldwide from 2015 and 2016, by vendor (in million U.S. dollars).(2019,23 Ağustos). Erişim Adresi:<https://www.statista.com/statistics/498270/security-and-vulnerability-management-vendor-revenue-worldwide/>
- [120.] Ribble, M. (2009). Raising a digital child: A digital citizenship handbook for parents, Washington DC: The International Society for Technology in Education (ISTE).
- [121.] Ribble, M. (2011). DigitalCitizenship in Schools, (Cilt 2nd Edition). Washington DC: *The International SocietyforTechnology in Education* (ISTE).
- [122.] RUKANCI, Fatih ve H. ANAMERİÇ (2004) "Bilgi Toplumu ve Toplumun Bilgilenmesinde Kütüphanelerin Rolü", *Kütüphaneciliğin Destanı Uluslararası Sempozyumu (21-24 Ekim 2004)*, Ankara,
- [123.] S.Filiz,(2012). Siber güvenlikte biyometrik sistemler Ve yüz tanıma. GAZİ Üniversitesi Bilişim enstitüsü. Ankara
- [124.] Sağiroğlu. ve Erol,E.E. (2018) Siber Bilgi Güvenliği Farkındalığı, Farkındalık Ölçüm Yöntemleri ve Modelleri. Sağiroğlu ve M. Alkan(Ed) Siber Güvenlik ve Savunma(s.104-134) içinde Ankara= Grafik Yayınları
- [125.] Sağiroğlu. ve Erol,E.E. (2018) Siber Bilgi Güvenliği Farkındalığı, Farkındalık Ölçüm Yöntemleri ve Modelleri. Sağiroğlu ve M. Alkan(Ed) Siber Güvenlik ve Savunma(s.104-134) içinde Ankara= Grafik Yayınları
- [126.] Saini, H., Rao, Y. S., & Panda, T. C. (2012). Cyber-crimes and their impacts: A review. *International Journal of Engineering Research and Applications*, 2(2), 202-209.
- [127.] Sarı,O.(2013). Uluslararası hukuk ve Türk ceza hukuku bağlamında siber güvenlik ve bilişim sistemine yönelik suçlar.(Yüksek Lisans Tezi). Harp akademileri stratejik araştırmalar enstitüsü,İstanbul.
- [128.] Sarıbay, A. Y. (1992). *Siyasal sosyoloji: bir çözümleme çerçevesi*. Ankara: Gündoğan Yayınları.
- [129.] Schmitt, M. (2013). Genelde silahlı çatışma yasası. In Siber Warfare Uygulanabilecek Uluslararası Hukuku Talin Kılavuzuna (s. 75-94). Cambridge: Cambridge Üniversitesi Yayınları. doi: 10,1017 / CBO9781139169288.006
- [130.] Security Throught Education. What is Social Engineering?. (2018, 20 Ekim). Erişim Aderesi: <https://www.social-engineer.org/about/>
- [131.] Sevri, Mehmet & Topaloglu, Nurettin. (2016). TÜRKİYE' DE SİBER GÜVENLİK EĞİTİMİNİN DURUMU (CYBER SECURITY EDUCATION IN TURKEY).
- [132.] Size Of The Cyber Security Market Worldwide, From 2017 to 2023 (in billion u.s. dollars). (2018,9 Eylül). Erişim Adresi: <https://www.statista.com/statistics/595182/worldwide-security-as-a-service-market-size/>

- [133.] Small, T. ve Sage, P. (2005). Knowledge management and knowledge sharing: A Review, *IOS Press: Information, Knowledge, Systems Management*, 5 (3), 153-169.
- [134.] Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippett, N. (2008). Cyberbullying: Its nature and impact in secondary school pupils. *Journal of child psychology and psychiatry*, 49(4), 376-385. Doi:10.1111/j.1469-7610.2007.01846.x.
- [135.] Sullivan, C. (2016). Digital citizenship and the right to digital identity under international law. *Computer Law & Security Review*, 32(3), 474-481.
- [136.] Şahinaslan, E., Kandemir, R. ve Şahinaslan, Ö. (2009). Bilgi güvenliği farkındalık eğitimi örneği. *Akademik Bilişim '09 - XI. Akademik Bilişim Konferansı Bildirileri* içinde (s. 189-194). Urfa.
- [137.] ŞANLISOY, S. (1999). BİLGİ TOPLUMUNDA ORTAYA ÇIKABİLECEK SORUNLAR. *Dokuz Eylül Üniversitesi İktisadi İdari Bilimler Fakültesi Dergisi*, 14(2).
- [138.] Şimsek, E , Şimsek, A . (2013). New Literacies for Digital Citizenship. *Contemporary Educational Technology*, 4 (2), 126-137.
- [139.] 2018 Ocak -Mart dönemi siber tehdit rapor durumu.(2019,27,Ağustos).Erişim Adresi:<https://www.stm.com.tr/tr/yayinlar/makalelerraporlar>
- [140.] Tandoğan, M. ve diğerleri. (1998). Çağdaş eğitimde yeni teknolojiler. Eskişehir: Anadolu Üniversitesi Yayınları.
- [141.] Tath, A. (2018). *Öğretmenlerin dijital vatandaşlık düzeylerinin bilgi okuryazarlığı ile internet ve bilgisayar kullanım öz yeterlikleri bağlamında değerlendirilmesi*. Yayımlanmış yüksek lisan tezi. Necmettin Erbakan Üniversitesi. Konya.
- [142.] Tekerek, M., & Tekerek, A. (2013). Öğrencilerin bilgi güvenliği farkındalığı üzerine bir araştırma. *Turkish Journal of Education*, 2(3), 61-70. DOI: 10.19128/turje.181065
- [143.] Temmuz 2019 itibarıyla küresel dijital nüfus (milyonda). (2019, 21 Ağustos).
- [144.] The Statistic Portal. Average cost per information security incidents in organizations worldwide from 2016 to 2018 (in U.S. dollars).(2018, 9 Eylül). Erişim Adresi:<https://www.statista.com/statistics/790759/cost-of-information-security-incidents-in-companies/>
- [145.] The statistic Portal. Percentage of Total IT Budgets Spent on IT Security from FY2005 to FY2017.(2018,9 Eylül). Erişim Adresi:<https://www.statista.com/statistics/536764/worldwide-it-security-budgets-as-share-of-it-budgets/>
- [146.] TMT Global Security Survey Full Report, .(2019,19 Kasım). Erişim Adresi:[https://www.mynewsdesk.com/material/document/17190/download?resource_type=resource document](https://www.mynewsdesk.com/material/document/17190/download?resource_type=resource%20document)
- [147.] Turak, Y. (2015). Nesnelerin interneti ve güvenliği. İstanbul, .(2019, 26, Ağustos). Erişim Adresi:www.yigitturak.com/wpcontent/uploads/loTGuvenligi.pdf.
- [148.] TURAN, S., & AVCI, E. K. (2018). 2018 Sosyal Bilgiler Öğretim Programı'nın Dijital Vatandaşlık Bağlamında İncelenmesi. *Eğitim ve Yeni Yaklaşımlar Dergisi*, 1(1), 28-38.
- [149.] Turan, S.,& AVCI, E .K (2018). 2018 Sosyal Bilgiler Öğretim Programı'nın Dijital Vatandaşlık Bağlamında İncelenmesi. *Eğitim ve Yeni Yaklaşımlar Dergisi*, 1 (1), 28-38. Erişim Adresi: <http://dergipark.org.tr/jena/issue/42984/519671>.
- [150.] Türkiye İstatistik Kurum. Hane halkı Bilişim Teknolojileri Kullanım Araştırması.(2018,13 Mayıs). Erişim Adresi: <http://www.tuik.gov.tr/PreHaberBultenleri.do?id=18660>
- [151.] Türkiye İstatistik Kurumu. Basın Odası Haberleri. (2018,13 Mayıs). Erişim Adresi:http://www.tuik.gov.tr/basinOdasi/haberler/2015_69_20151217.pdf
- [152.] Türk dil kurumu sözlükleri. (2019, 26, Ağustos). Erişim Adresi: <http://sozluk.gov.tr/>
- [153.] Teknolojiyle kapıyı çalan tehlike: Siber saldırı (2019,22 Kasım). Erişim Adresi:<https://www.aa.com.tr/tr/info/infografik/13532>
- [154.] USOM Hakkında. (2019,22 Kasım). Erişim Adresi: <https://www.usom.gov.tr/>
- [155.] Ünal, Y. (2009). Bilgi toplumunun tarihçesi. *Tarih Okulu*, 5, 123-144.
- [156.] Ünal.Y.(2012). Bilişim ve dijital insan. *Ankara barosu dergileri*. 2012(2),31-34.

- [157.] Üniversitemiz Birim Program Bazında Öğrenci Sayıları (2020, 22 Ocak). Erişim Adresi:http://mersin.edu.tr/bulut/birim_594/Sayilarla_Universitemiz/2019_Aralk_Orenci_Saylar_Raporu.pdf
- [158.] Ünver,M., Mirzaoğlu, A.G. & Canbey, C. (2011). Siber Güvenliğin Sağlanması: *Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler* . Ankara: BTK
- [159.] Van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior*, 75, 547-559.
- [160.] Vardal, N.(2009). Yüksek öğretimlerde bilgi güvenliği: bilgi güvenlik yönetim sistemleri için bir model önerisi ve uygulaması. Gazi üniversitesi eğitim teknolojisi anabilim dalı. Ankara.
- [161.] Virus:W32/Melissa. .(2019, 26, Ağustos).Erişim Adresi: <https://www.f-secure.com/v-descs/melissa.shtml>
- [162.] Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, 38, 97-102. Erişim Adresi:<https://doi.org/10.1016/j.cose.2013.04.004>
- [163.] VURAL, Y., & SAĞIROĞLU, Ş. (2011). Kurumsal Bilgi Güvenliğinde Güvenlik Testleri ve Öneriler. Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi, 26(1).
- [164.] Warnes, K., PhD. (2017). Cybersecurity. Salem Press Encyclopedia. Retrieved from<http://search.ebscohost.com/login.aspx?direct=true&db=ers&AN=89677538&lang=tr&site=eds-live&authtype=uid>
- [165.] Weeden, S., Cooke, B., & McVey, M. (2013). Underage children and social networking. *Journal of Research on Technology in Education*, 45(3), 249-262.
- [166.] Whittaker, J., Curran, J. (2004). *The Cyberspace Handbook*. London: Routledge.
- [167.] YILDIZ, Ö. R. (2010). BİLİŞİM DÜNYASININ YENİ MODELİ: BULUT BİLİŞİM (CLOUD COMPUTING) VE DENETİM. *Sayıstay Dergisi*, 74-75.
- [168.] Yılmaz,E.(2015).Öğretmenlerin dijital veri güvenliği farkındalığı.(Doktora Tezi). Anadolu Üniversitesi Eğitim Bilimleri Enstitüsü, Eskişehir.
- [169.] YİĞİT, M. F., & SEFEROĞLU, S. S. (2019). Öğrencilerin siber güvenlik davranışlarının beş faktör kişilik özellikleri ve çeşitli diğer değişkenlere göre incelenmesi. *Mersin Üniversitesi Eğitim Fakültesi Dergisi*, 15(1), 186-215.
- [170.] YİĞİT, M. F., & SEFEROĞLU, S. S. (2019). Öğrencilerin siber güvenlik davranışlarının beş faktör kişilik özellikleri ve çeşitli diğer değişkenlere göre incelenmesi. *Mersin Üniversitesi Eğitim Fakültesi Dergisi*, 15(1), 186-215.
- [171.] YİĞİT, T., & AKYILDIZ, M. (2014). Sızma Testleri İçin Bir Model Ağ Üzerinde Siber Saldırı Senaryolarının Değerlendirilmesi. *Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, 18(1). doi:<http://dx.doi.org/10.19113/sdufbed.22798>
- [172.] Yiğit,T.(2013). Siber Güvenlik Açısından Sızma Testlerinin Uygulamalar İle Değerlendirilmesi.(Yüksek lisans tezi). Elektronik Haberleşme Anabilim Dalı.
- [173.] Yüksek eğitim kurumu tez merkezi. .(2019, 26, Ağustos).Erişim Adresi:<https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp>

EK.1. Mersin Üniversitesi Araştırma İzin Yazısı



T.C.
MERSİN ÜNİVERSİTESİ REKTÖRLÜĞÜ
Eğitim Fakültesi Dekanlığı
Öğrenci İşleri Birimi

Mersin Üniversitesi - ÖĞRENCİ
İŞLERİ BİRİMİ
Tarih: 09/05/2019
Sayı: 98161189.044.E.00001041228



0001041228

Sayı : 98161189-044
Konu : Anket

BİLGİSAYAR VE ÖĞRETİM TEKNOLOJİLERİ EĞİTİMİ BÖLÜM BAŞKANLIĞINA

Bölümünüz Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı Başkanlığı öğretim üyesi Dr. Öğr. Üyesi Ali GÖK'ün danışmanlığını yaptığı Yüksek Lisans öğrencisi tez çalışması 16-01100171-007 numaralı öğrencisi Murat SOLMAZ'ın Yüksek Lisans Tez Çalışması kapsamında yapacak olduğu "**Öğretmen Adaylarının Siber Güvenlik Farkındalık Düzeylerinin İncelenmesi**" adlı anket çalışması uygulama isteği Dekanlığımızca uygun görülmüştür.

Bilgilerinizi ve gereğini rica ederim.

e-İmzalıdır
Prof.Dr. Mutlu Nisa ÜNALDI CORAL
Dekan V.



Adres: yenişehir kampüsü eğitim
fakültesi
E-posta: senem33@mersin.edu.tr
Telefon: +90 42013

Ayrıntılı bilgi için: senem bal

Fax: +90 03243412823

Elektronik ağ: www.mersin.edu.tr



1 / 1

EK.2. Kişisel Bilgi Formu

ÖĞRETMEN ADAYLARININ SİBER GÜVENLİK FARKINDALIKLARININ VE DİJİTAL VATANDAŞLIK DÜZEYLERİNİN İNCELENMESİ

Değerli Öğretmen Adayları,

Bu veri toplama aracı öğretmen adaylarının siber güvenlik farkındalıklarını ve dijital vatandaşlık düzeylerini ortaya koymak amacı ile hazırlanmıştır. Toplanan veriler araştırmacı tarafından gizli tutulacak, araştırmanın amacı dışında hiçbir şekilde kullanılmayacaktır. Araştırmanın daha güvenilir sonuçlara ulaşması için, lütfen soruları samimi, tam ve doğru bir şekilde cevaplandırınız. Her ifadeyi dikkatlice okuyarak size en uygun seçeneğe (x) işareti koyarak yanıt veriniz ve boş bırakmayınız. Form 3 aşamadan oluşmakta ve cevaplama süreniz yaklaşık 15 dakikadır.

Katkılarınız için teşekkürler.

Murat SOLMAZ
Mersin Toroslar Bahriye Orta Okulu

Bilişim Teknolojileri Öğretmeni

Dr. Öğretim Üyesi Ali GÖK

MERSİN ÜNİVERSİTESİ

C) Kişisel Bilgiler
Cinsiyet <input type="checkbox"/> Kadın <input type="checkbox"/> Erkek
Üniversite:
Bölüm:
Sınıf <input type="checkbox"/> 1.Sınıf <input type="checkbox"/> 2.Sınıf <input type="checkbox"/> 3.Sınıf <input type="checkbox"/> 4.Sınıf
Günlük Toplam Akıllı Telefon, Tablet, Bilgisayar Kullanım Saati: <input type="checkbox"/> 1saatten az <input type="checkbox"/> 1-3 Saat <input type="checkbox"/> 4-6 Saat <input type="checkbox"/> 7saat ve Üzeri
Günlük Sosyal Medya Kullanım Saati: : <input type="checkbox"/> 1saatten az <input type="checkbox"/> 1-3 Saat <input type="checkbox"/> 4-6 Saat <input type="checkbox"/> 7saat ve Üzeri
<input type="checkbox"/> Kendime ait tabletim var <input type="checkbox"/> Kendime ait bilgisayarım var <input type="checkbox"/> Kendime ait akıllı telefonum var

EK.3. A) Siber Bilgi Güvenliği Farkındalığı Ölçeği	Kesinlikle Katılmıyorum	Katılmıyorum	Kısmen Katılıyorum	Katılıyorum	Kesinlikle Katılıyorum
1. Zararlı yazılımlar (virüs, solucan, truva atı vb.) konusunda bilgi sahibiyim.					
2. Parola oluştururken harf, sayı ve özel karakter kullanmanın önemini bilirim.					
3. Farklı işlemler için farklı parola kullanmanın önemini bilirim.					
4. İzinsiz kullanılmaması için dosyalara parola konulabileceğinin farkındayım.					
5. Güvenlik duvarı yazılımları konusunda bilgi sahibiyim.					
6. Flash bellekleri, veri saklamak yerine sadece veri taşımak için kullanmanın farkını bilirim					
7. İşletim sisteminin (Windows, Android vb.) güncel olmasına dikkat ederim.					
8. E-posta ile gelen kimlik bilgilerini doğrulama mesajlarına (parola, kredi kartı vb.) itibar edilmemesi gerektiğini bilirim.					
9. Taşınabilir depolama birimlerini (Flash bellek, taşınabilir sabit disk) kullanmadan önce virüs taraması yapılması gerektiğini bilirim.					
10. Güvenli olmadığını düşündüğüm e-postaları açmadan silmeye dikkat ederim.					
11. Programların, üreticinin kendi sitesinden indirilmesinin önemini bilirim.					
12. Anti virüs yazılımı kullanmanın önemini bilirim.					
13. Parola hatırlatmak için kullanılan güvenlik sorularına başkalarının tahmin edemeyeceği cevaplar verilmesi gerektiğini bilirim.					
14. Parola oluştururken karakter sayısının fazla olmasının önemini bilirim.					
15. Parolaların herhangi bir ortamda saklanmasının güvenlik riski oluşturacağını farkındayım.					
16. Verilerin, çeşitli uygulamalar (dropbox, google drive vb.) kullanılarak İnternet ortamında saklanabileceğini bilirim.					
17. Üzerinde çalışma yapılan dosyaların birden fazla ortamda yedeklenmesi gerektiğini bilirim.					
18. Başkalarının tahmin edemeyeceği parolalar oluşturmaya dikkat ederim.					
19. İnternet adres çubuğunda yanlış yönlendirme olup olmadığına dikkat ederim.					
20. Taşınabilir depolama birimlerini (Flash bellek, taşınabilir sabit disk) "Donanımı Güvenle Kaldır" seçeneğini kullanarak çıkartmaya dikkat ederim.					
21. Karmaşık yapıdaki parolaların kırılabilceğini bilirim.					
22. Parolaların belirli aralıklarla değiştirilmesi gerektiğinin farkındayım.					
23. Almak istemediğim çöp e-postaları "spam/gereksiz/önemsiz" olarak işaretlemeye dikkat ederim.					
24. İzinsiz kullanılmaması için cihazlara (akıllı telefon, tablet, bilgisayar vb.) parola konulabileceğinin farkındayım.					
25. Kendime ait olmayan cihazlarda, parola gerektiren işlemler yapmamaya dikkat ederim.					
26. İşletim sisteminin (Windows, Android vb.) güvenlikle ilgili uyarılarını dikkate alırım.					
27. Elektrik kesintisine karşı dizüstü bilgisayarları bataryası ile kullanmanın önemini bilirim.					
28. Cep telefonuna gelen tek kullanımlık parola ile yapılan giriş işlemlerinin, güvenliği arttırdığını bilirim.					
29. Sanal klavye kullanmanın önemini bilirim.					
30. İnternet sitelerinde kullanıcı oturumunu kapatırken "güvenli çıkış" bağlantısını kullanmanın önemini bilirim.					
31. İnternet sitelerinde kullanılan güvenlik sertifikaları hakkında bilgi sahibiyim.					
32. Lisanslı olmayan yazılımların güvenlik açıkları oluşturabileceğinin farkındayım.					

EK.4.	Kesinlikle Katılmıyorum	Katılmıyorum	Kısmen Katılıyorum	Katılıyorum	Kesinlikle Katılıyorum
B) Dijital Vatandaşlık Ölçeği					
1. Çevremle iletişim kurmak amacıyla dijital ortamları kullanırım.					
2. Sosyal ilişkilerimi dijital ortamlarda da yürütürüm.					
3. Dijital ortamlarda bilgi paylaşıyorum.					
4. Dijital ortamlarda gelen mesajlara cevap veririm.					
5. Dijital ortamlara rahatlıkla erişebilirim.					
6. Dijital ortamlara erişimde yaşadığım sorunları çözebilirim.					
7. Dijital ortamlara erişmek için gerekli olan teknolojileri kullanabilirim.					
8. Kendimi dijital okuryazar olarak tanımlıyorum.					
9. Dijital ortamlarda araştırma yapma konusunda kendime güvenirim.					
10. Dijital ortamlar işbirlikli projeler yürütürüm.					
11. Dijital ortamları rahatlıkla kullanabilmek için gerekli olan becerilere sahibim.					
12. Dijital ortamlarda araştırma yaparken bilgileri eleştirel bir şekilde analiz eder ve değerlendiririm.					
13. Dijital ortamlarda bilgiyi nasıl oluşturacağımı ve paylaşacağımı bilirim.					
14. Dijital ortamlarda kendimi güvende hissetmem.					
15. Dijital ortamlarda farklı kullanıcı adı ve şifre kullanırım.					
16. Dijital ortamlarda farklı güvenlik önlemleri alırım.					
17. Dijital ortamlarda kişisel gizliliğe saygı duyarım.					
18. Dijital ortamlarda başkalarına zarar vermem.					
19. Dijital ortamlarda başkalarının paylaşımına açık olmayan fikirlerini kaynak göstermeden kullanırım.					
20. Dijital ortamlarda sahip olduğum hakların farkındayım.					
21. Dijital ortamların kullanımına yönelik kuralları bilirim.					
22. Dijital ortamlarda iletişim kurarken saygılı davranırım.					
23. Dijital ortamlardaki sorumluluklarımı yerine getiririm.					
24. Dijital ortamlarda başkalarının etkinliklerine ya da işlerine zarar vermek suçtur.					
25. Dijital ortamlarda programları yasadışı yollarla indirmek suçtur.					
26. Dijital ortamlarda yer alan kopyalama izni verilmeyen metinleri kopyalamak suçtur.					
27. Dijital ortamlara spamlar, virüsler ve Trojanlar göndermek suçtur.					
28. Dijital ortamları bağımlılık derecesinde kullanırım.					
29. Dijital ortamlar sağlığımı olumsuz etkiler.					
30. Dijital ortamlar psikolojimi bozar.					
31. Dijital ortamlarda alışveriş yaparım.					
32. Dijital ortamlarda satın almak ya da satmak ile ilgili işleyişi bilirim.					
33. Dijital ortamlardaki alışveriş sitelerini takip ederim.					

EK.5.

ÖZGEÇMİŞ

Adı ve Soyadı : Murat SOLMAZ

Doğum Tarihi : 1990

E-mail : solmazmurat66@gmail.com

Öğrenim Durumu :

Derece	Bölüm/Program	Üniversite /Okul	Yıl
Ortaokul		Mustafa Kemal Ortaokulu	2003-2006
Ortaöğretim	Yazılım Sistemleri	Yahya Günsür MTAL	2006-2010
Lisans	BÖTE	Erzincan Üniversitesi	2011-2015
Yüksek Lisans	BÖTE	Mersin Üniversitesi	2017-2019

Görevler :

Görev Ünvanı	Görev Yeri	Yıl
Öğretmen	Gaziantep/ Nizip Enver Mebrure Okan Ortaokulu	2017-2018
Öğretmen	Bahriye Ortaokulu	2017-Devam