**T.C.**
**NECMETTİN ERBAKAN ÜNİVERSİTESİ**
**EĞİTİM BİLİMLERİ ENSTİTÜSÜ**

Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı
Bilgisayar ve Öğretim Teknolojileri Eğitimi Bilim Dalı

Yüksek Lisans Tezi

# TÜRKİYE'DE SİBER GÜVENLİK ALANINDA YAPILAN TEZLERİN İNCELENMESİ: BİBLİYOGRAFİK BİR ÇALIŞMA

Yavuz KAHRİMAN
ORCID: 0000-0002-2569-7102

Danışman
Prof. Dr. Ertuğrul USTA
ORCID: 0000-0001-6112-9965

Konya – 2022

# ÖN SÖZ (TEŞEKKÜR)

Teknoloji ve internetin günlük hayatımızda kullanılabilirliği günümüzde artış yönlü ivme kazanmıştır. Bu gelişim ile birlikte insan hayatı olumlu yönden fayda sağlamış ve birçok alanda teknoloji kullanılmıştır. Teknolojinin günlük hayatta bu derece yer alması siber güvenlik kavramının önemini artırmıştır. Günümüzde teknolojide yaşanan gelişmelere adaptasyon sağlanması ve bu gelişmelere bilimsel anlamda yön verilmesi için yayımlanmış olunan tezlerin incelenmesine gerek duyulduğu anlaşılmıştır. Literatürde siber güvenlik temalı birçok akademik çalışma yer almaktadır. Bu nedenle bu çalışma siber güvenlik temalı tezlerin tanımlanmasına yönelik olarak gerçekleştirilmiştir. Bu araştırmanın yapılmasında birçok kişinin katkısı olmuştur.

Tez konusunun seçimi noktasında ve tez araştırması sürecinin yürütülmesinde bana rehberlik eden ve hiçbir zaman desteğini esirgemeyen değerli danışmanım Sayın Prof. Dr. Ertuğrul USTA ’ya,

Yüksek lisans ders aşamasında akademik ve bilimsel yönden gelişmemi sağlayan ve tez hazırlama seviyesine ulaşmam için emek veren çok değerli öğretim üyelerine,

Tezimi sabırla okuyup değerlendiren ve akademik kariyerim için bana yardımcı olan Sayın jüri üyeleri Prof. Dr. Özgen KORKMAZ ve Doç. Dr. Ağah Tuğrul KORUCU ‘ya,

Eğitim hayatımın her aşamasında desteğini hiçbir zaman esirgemeyen sevgili eşim Dilek KAHRİMAN ‘a ve varlıklarıyla büyük katkıda bulunan oğullarım Said Talha ile Yağız Efe ‘ye,

Çalışmanın ilk gününden itibaren, yoğun mesai saatleri arasında bana destek olan Siber Suçlarla Mücadele Daire Başkanlığında görevli çalışma arkadaşlarıma; teşekkürlerimi sunmayı bir vazife addederim.

Yavuz KAHRİMAN

Haziran 2022

# İÇİNDEKİLER

# ŞEKİLLER

# TABLOLAR

## TEZ ÇALIŞMASI ORİJİNALLİK RAPORU

*Türkiye'de Siber Güvenlik Alanında Yapılan Tezlerin İncelenmesi: Bibliyografik Bir Çalışma* başlıklı tez çalışmamın toplam **68** sayfalık kısmına ilişkin, 14/06/2022 tarihinde tez danışmanım tarafından **Turnitin** adlı intihal tespit programından aşağıda belirtilen filtrelemeler uygulanarak alınmış olan orijinallik raporuna göre, tezimin benzerlik oranı **%13** olarak belirlenmiştir.

Uygulanan filtrelemeler:

1. Tez çalışması orijinallik raporu sayfası hariç
2. Bilimsel etik beyannamesi sayfası hariç
3. Önsöz hariç
4. İçindekiler hariç
5. Simgeler ve kısaltmalar hariç
6. Kaynaklar hariç
7. Alıntılar dahil
8. 7 kelimeden daha az örtüşme içeren metin kısımları hariç

Necmettin Erbakan Üniversitesi Tez Çalışması Orijinallik Raporu Uygulama Esaslarını inceledim ve tez çalışmamın, bu uygulama esaslarında belirtilen azami benzerlik oranının (%30) altında olduğunu ve intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

14/06/2022

Yavuz KAHRİMAN

Prof. Dr. Ertuğrul USTA

## BİLİMSEL ETİK BEYANNAMESİ

Bu tezin tamamının kendi çalışmam olduğunu, planlanmasından yazımına kadar tüm aşamalarında bilimsel etiğe ve akademik kurallara özenle riayet edildiğini, tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez hazırlama kurallarına uygun olarak hazırlanan bu çalışmada başkalarının eserlerinden yararlanılması durumunda bilimsel kurallara uygun olarak atıf yapıldığını ve bu kaynakların kaynaklar listesine eklendiğini beyan ederim.

14/06/2022

Yavuz KAHRİMAN

## SİMGELER VE KISALTMALAR

**Kısaltmalar**

| | |
|---|---|
| ABD | Amerika Birleşik Devletleri |
| Akt | Aktaran |
| Ar-Ge | Araştırma-Geliştirme |
| Arş. Gör. | Araştırma Görevlisi |
| Arş. Gör. Dr. | Araştırma Görevlisi Doktor |
| Doç. Dr. : | Doçent Doktor |
| DoS | Hizmet Reddi (Denial-of-Service) |
| DDoS | Dağıtılmış Hizmet Reddi (Distributed Denial of Service) |
| Dr | Doktor |
| Dr. Öğr. Üyesi | Doktor Öğretim Üyesi |
| HTML | Hiper Metin İşaretleme Dili (Hyper Text Markup Language) |
| HTTP | Hiper Metin Transfer Protokolü (Hyper Text Transfer Protocol) |
| HTTPS | Güvenli Hiper Metin Transfer Protokolü (Secure Hypertext Transfer Protocol) |
| MFT | Ana Dosya Tablosu (Master File Table) |
| Öğr. Gör. | Öğretim Görevlisi |
| Prof. Dr. | Profesör |
| s. | Sayfa |
| TUBISAD | Türkiye Bilişim Sanayicileri Derneği |
| TÜBESS | Türkiye Belge Sağlama Sistemi |
| UDS | Uluslararası Denetim Standartları |
| UAB | Ulaştırma ve Altyapı Bakanlığı |
| URL | Tekdüzen Kaynak Bulucu (Uniform Resource Locator) |
| vb. | ve benzeri |
| vs | Ve saire |
| Y. L. | Yüksek Lisans |
| YÖK | Yükseköğretim Kurulu |

# ÖZET

Necmettin Erbakan Üniversitesi, Eğitim Bilimleri Enstitüsü
Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı
Bilgisayar ve Öğretim Teknolojileri Eğitimi Bilim Dalı
Yüksek Lisans Tezi

## TÜRKİYE'DE SİBER GÜVENLİK ALANINDA YAPILAN TEZLERİN İNCELENMESİ: BİBLİYOGRAFİK BİR ÇALIŞMA

Yavuz KAHRİMAN

Siber güvenlik bilişim dünyasının güvenliğini ifade eden bir kavram olarak karşımıza çıkar. Teknolojinin hızla gelişmesiyle birlikte insanlar her gün çeşitli siber güvenlik tehditlerine maruz kalmaktadır. Siber suçlular, geliştirdikleri yöntem ve teknikleri kullanarak kişisel verileri, banka hesaplarını ve gizli şirket verilerini ele geçirmeye çalışırlar. Bu çalışmada siber güvenliğe yönelik tezlerde yöntemsel açıdan ne tür çalışmaların yapıldığı incelenmeye çalışılmıştır. Bu bağlamda çalışma Türkiye'de siber güvenlik ile ilgili alanda herhangi bir çalışma yapmadan, ilgili literatürün durumunu ortaya koymak amacıyla yapılmıştır. Elde edilen sonuçlara göre en fazla tez yayımlanan yıl 2019'dur, en fazla çalışma devlet üniversitelerinde yapılmıştır, çalışmaların çoğunluğu fen bilimleri enstitüsü ve bilgisayar mühendisliği anabilim dalı bünyesinde yayımlanmıştır.

**Anahtar Kelimeler:** Siber güvenlik, bilgi güvenliği, bibliyografya, bibliyometri, veri analizi

## ABSTRACT

Necmettin Erbakan University, Graduate School of Educational Sciences
Department of Computer Education and Instructional Technology
Computer Education and Instruction Technology Program
Master Thesis

**EXAMINATION OF THESIS IN THE FIELD OF CYBER SECURITY IN TURKEY: A BIBLIOGRAPHIC STUDY**

Yavuz KAHRİMAN

Cyber security emerges as a concept that expresses the security of the information technology world. People are faced with a lot of cyber security risks on a daily basis due to the rapid development of technology. Using the methods and techniques they have developed, cybercriminals try to capture personal data, bank accounts, and valuable enterprise data. This study is aimed at investigating what types of research has been published in terms of the approach in theses on cyber security. The study was carried out in this context to demonstrate the status of the relevant literature without conducting any research in the field of cyber security in Turkey. According to the findings, the largest number of postgraduate theses were published in 2019 and the majority of research has been conducted at public universities. Additionally, the majority of the studies were published by the institute's science and computer engineering department.



**Keywords:** Cyber security, information security, bibliography, bibliometrics, data analysis

# BÖLÜM 1

## 1. GİRİŞ

Günümüzde bilgi ve iletişim teknolojilerinde yaşanan gelişmeler sebebiyle günlük yaşam değişmektedir. Teknoloji günlük alışkanlıkları değiştirmeye başlamıştır. Bunun yanı sıra teknoloji hayatlarımızı kolaylaştırmaktadır. Ancak madalyonun öteki tarafında ise teknolojinin getirmiş olduğu riskler yer almaktadır. Dijital ortamlarda üretilen ve saklanan bilgide yaşanan artış sebebiyle bilgi güvenliğine ilişkin çeşitli tehdit ve riskler ortaya çıkmaktadır (Yılmaz, Şahin, & Akbulut, 2016).

İnternet eğitim-öğretim süreçlerinde aktif rol almaya başladıktan sonra bilgi sınıf ortamından çıkıp tüm dünyaya yayılmıştır. (Akkoyunlu, 2002). Eğitim ortamlarında aktarım ve iletişim teknolojilerinin kullanımının yaygınlaşması ve öğretmenlerin öğrenme ortamlarında kullandıkları teknolojik cihazlarının sayısındaki artış bilgi güvenliği konusundaki endişeleri arttırmaktadır. Teknolojide yaşanan gelişmeler öğretmenlerin teknoloji alanında kendilerini geliştirmelerini gerektirmektedir (Arslan & Şendurur, 2017).

Veri; araştırma ya da inceleme neticesinde elde edilen, işlenmemiş ve ham durumda olan bilgiler bütününe denir. Böylelikle farklı kullanıcılar tarafından üzerine yorum yapılır (Yıldız, 2006). Dijital veri ise internet ya da bilişim sistemleri aracılığıyla oluşturulmuş olunan bilgi paketleridir (Şengül, Atsan, & Bostan, 2014). Dijital veriler, çeşitli avantajlara sahiptirler. Veriyi üreten kişi tarafından uzaktan erişime açılmaları söz konusudur. Farklı formatlarda kaydedilebilirler. Dijital verilerin avantajları sayesinde birçok uygulama ve hizmetler dijital platformlara taşınmaktadır (Schroeder, Steinmetz, Pereira, & Espindola, 2016).

Siber güvenlik bilişim dünyasının güvenliğini ifade eden bir kavram olarak karşımıza çıkar. Siber güvenlik, siber ortamda yer alan sistemlerin güvenliğini sağlamak amacıyla alınmış olunan tedbirler, faaliyetler ve bu amaçlarla belirlenmiş tüm standart, politika ve kurallar bütünüdür (Çiftçi, 2013). Burada güvenlik kavramı gizlilik, bütünlük ve erişilebilirliği kapsamaktadır. Teknolojinin hızla gelişmesiyle birlikte insanlar her gün çeşitli siber güvenlik tehditlerine maruz kalmaktadır. Siber suçlular, geliştirdikleri yöntem ve teknikleri kullanarak kişisel verileri, banka hesaplarını ve gizli şirket verilerini ele geçirmeye çalışırlar.

Bu çalışmada siber güvenliğe yönelik tezlerde yöntemsel açıdan ne tür çalışmaların yapıldığı incelenmeye çalışılmıştır. Bu bağlamda çalışma Türkiye'de siber güvenlik ile ilgili

alanda herhangi bir çalışma yapmadan, ilgili literatürün durumunu ortaya koymak amacıyla yapılmıştır.

## 1.1. Problem Durumu

Geçmişten günümüze bilim tarihi süresi zarfında elde edilmiş olunan bilgiler oldukça açık ve tartışmasız olmasına karşın günümüzde yeni bilgilerin entegrasyonu eski bilgilerin sentezlenmesiyle mümkündür (Chalmers , Hedges, & Cooper, 2002). Eğitim alanında yapılan çalışmalar son yıllarda artmıştır. Ancak bu çalışmaların ortaya koymuş olduğu sonuçların sistematik hale getirilmesi gerekmektedir.

Bilginin hızlı yayılmasının olumlu sonuçları asla inkar edilemez. Çağımızın en önemli buluşu olan internet sayesinde bilgiye erişim oldukça hızlanmıştır. Ayrıca internet alt yapı hizmeti olarak da karşımıza çıkar. İnternet'e bağlı kurumlar, bilgisayarlar aracılığıyla birbirine bağlanarak hızlı bir şekilde iletişim sağlayıp külfetli birçok işlemi kısa sürede yapabilmektedir (Sarı, 2013).

Siber güvenlik, bilgilerin her türlü saldırı ve tehdide karşı genel olarak korunması anlamına gelir ve siber güvenlik, kurumların, kuruluşların ve kullanıcı varlıklarının güvenlik özelliklerini siber bir ortamda güvenlik risklerine dayanabilecek şekilde oluşturmayı amaçlar.

Teknolojinin eğitimde hızla yaygınlaşması ile siber güvenlik, bilgi güvenliği ve veri güvenliği konularında dünyada olduğu gibi ülkemizde de son yıllarda birçok çalışma hazırlanmış ve bu konularda güvenlik planları hazırlanmaya devam etmektedir.

Türkiye'de siber güvenlik, bilgi güvenliği ve veri güvenliği ile ilgili yayımlanan tezlerinin incelenmesi sonucunda bu kapsamda yapılan inceleme çalışmasına rastlanılmamıştır. Günümüzde teknolojide yaşanan gelişmelere adaptasyon sağlanması ve bu gelişmelere bilimsel anlamda yön verilmesi için yayımlanmış olunan tezlerin incelenmesine gerek duyulduğu anlaşılmıştır. Bu sebepten ötürü çalışmada Türkiye'de yayımlanmış olunan siber güvenlik tezlerinin bibliyometri ile analiz edilmesi söz konusu olmuştur.

## 1.2. Araştırmanın Amacı

Tezlerin yazımında bilgiler bilimsel yöntem ile üretilmektedir. Alanında uzman akademisyenlerin danışmanlığında gerçekleştirilen tez çalışmaları "Tez Yazım Yönergeleri" doğrultusunda rapor haline getirilirler (Ağaoğlu, Ceylan, Kesim, Madden, & Altınkurt, 2005).

Bir tezin bilimsel olarak tasdik edilmesi, sistematik ve sistematik araştırma ve araştırma sürecinin evrensel kriterlere göre rapor edilmesini gerektirir (Kolaç, 2008).

Türkiye'deki Yükseköğretim Kurumları bünyesinde, siber güvenlik, bilgi güvenliği ve veri güvenliği alanında yapılan tezlerde ele alınan konuların ve kullanılan araştırma yöntemlerinin incelenmesi bu çalışmanın genel amacını oluşturmaktadır. Bu amaç doğrultusunda Türkiye'de siber güvenlik alanında yapılan tezleri;

1. Yıllara
2. Üniversitelere
3. Üniversitelerin illerine
4. Üniversitelerin türüne
5. İlgili enstitülere
6. Anabilim dallarına
7. Bilim dallarına
8. Yazarlarının cinsiyetlerine
9. Yazım dillerine
10. Danışman unvanına
11. Sayfa Sayılarına
12. Konularına
13. Araştırma yöntemlerine
14. Veri toplama teknikleri

Belirlenen değişkenler doğrultusunda incelenerek değerlendirme sonucuna ulaşılacaktır.

## 1.3. Araştırmanın Önemi

Türkiye'de siber güvenlik, bilgi güvenliği ve veri güvenliği alanında yapılan tezlerinin incelenmesine yönelik yapılan bibliyografya çalışmalarına dair literatüre genel olarak bakıldığında, herhangi bir çalışmanın olmadığı göze çarpmaktadır. Bu çalışma, siber güvenlik,

bilgi güvenliği ve veri güvenliği alanında yapılan tezlerinin konu yönelimleri ve araştırma yöntemlerini incelemeye yönelik bir çalışma olması açısından önem taşımaktadır. Çalışma siber güvenlik, bilgi güvenliği ve veri güvenliği alanındaki tezlerin genel çerçevesi hakkında bilgi vereceğinden, tez çalışmalarında; hangi konularla ilgili çalışmaların yapıldığı, hangi araştırma yöntemlerinin kullanıldığı ve belirli ölçütlere göre analiziyle elde edilen değerlendirme sonuçları literatüre katkı sağlayıp yeni araştırmacılara da çeşitli açılardan yol gösterici olacaktır. Bu açıdan çalışmanın özgün olduğu söylenebilir.

## 1.4. Sayıltılar (Varsayımlar)

Bu çalışmada;

1. YÖK Ulusal Tez Merkezi veri tabanında yayımlanan tezlerin, siber güvenlik, bilgi güvenliği ve veri güvenliği alanında tamamlanan ve erişime açık tüm tezlerini kapsadığı,
2. Belirtilen sınırlar dâhilinde seçilen çalışma kümesinin geçerli ve güvenilir olduğu,
3. Araştırmada kullanılan ölçme araçlarının geçerli ve güvenilir olduğu,
4. Araştırmada yararlanılan kaynakların doğru ve geçerli bilgiler sağladığı, varsayılmaktadır.

## 1.5. Sınırlılıklar

Bu araştırma, Türkiye'de siber güvenlik, bilgi güvenliği ve veri güvenliği alanında yayınlanmış tezler ile sınırlandırılmıştır. Erişime kapalı olan tezlerle birlikte "siber güvenlik, bilgi güvenliği ve veri güvenliği" ifadesi geçmeyen tezler araştırmanın kapsamı dışında bırakılmıştır.

## 1.6. Tanımlar

### 1.6.1. Bilgi güvenliği ve siber güvenlik

Siber güvenlik tartışması, ilk olarak 1970'lerde ABD'de ortaya çıkmıştır. İlk başlarda hükümet bilgi sistemlerinde bulunan gizli bilgilere ilişkin kaygılar söz konusudur. Fakat yıllar geçtikçe bilgisayar ağlarının büyüyüp günlük yaşamda daha fazla yer bulmuştur. Böylelikle odak noktası değişmiştir. "Siber güvenlik" terimi ilk olarak bilgisayar bilimcileri tarafından

1990'ların başında kullanılmıştır. Odak noktası zamanla değişerek sadece bilgisayar güvenliği anlayışından öteye geçmiş ulusal güvenlik meselesi halini almıştır (Adams ve diğerleri, 2015, s. 15-16). Siber güvenlik kapsamında iş yerinizdeki bilgisayarınız, tabletiniz, cep telefonlarınız, dizüstü bilgisayarınız, internet hattınız ve benzeri milyonlarca makine yer almaktadır. Siber güvenlik, tüm bilgisayar ağlarını, onların bağlı olduğu ve kontrol ettiği her şeyi kapsamaktadır. Dolayısıyla bu durumda hepimiz siber güvenliğin bir unsuru, bir parçası olmuş oluyoruz (Clarke & Knake, 2011, s. 44).

Bilgi güvenliği kavramı kurumsal varlıklar arasında yer alan bilginin silinme, bozulma, tahribat gibi şekillerde hasar görmesini önlemek ve olası saldırılara karşı bilginin korunmasını kapsamaktadır (Önel & Dinçkan, 2007). Bilgi güvenliği kapsamında bilginin yetkisiz kişiler tarafından kullanımının önlenmesi, bütünlük ve doğruluğunun korunması ve sadece söz konusu bilgiye erişim olan kişilerce erişilmesinin sağlanması yer almaktadır (Canbek & Sağıroğlu, 2006).

Siber alanda gerçekleştirilen saldırılar çok boyutlu ve artarak devam etmektedir. Bunun yanı sıra siber saldırılar küresel anlamda derinleşmiş durumdadır. Bu sebeple siber saldırının gerçekleştirildiği yerin ve siber saldırganların kimliklerinin tespitini yapmak teknik anlamda çok zor olduğu için devletler kendi içlerinde siber tehditlere karşı çalışmalar başlatmıştır. Türkiye Cumhuriyeti Devleti 2012'den beri siber güvenlik stratejisi yayınlamaktadır. En son 2020 – 2023 Ulusal Siber Güvenlik Stratejisi yayımlanmıştır (Ulaştırma Denizcilik ve Altyapı Bakanlığı, (UDHB), 2020 – 2023 Ulusal Siber Güvenlik Stratejisi & Türkiye Bilişim Sanayicileri Derneği, (TUBISAD), Türkiye'nin Siber Güvenlik Stratejisine Yönelik Değerlendirmeler).

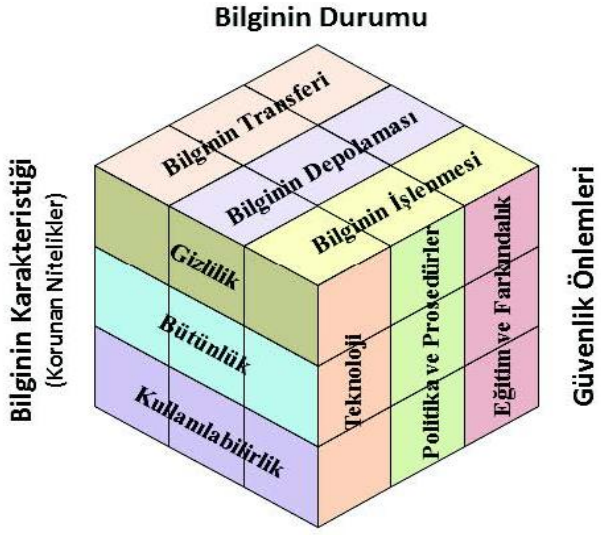
Siber tehditler dijital dünyayı elektrik şebekelerinden su kaynaklarına kadar etki altına almıştır. Bir iddiaya göre siber saldırılar ile Amerika Birleşik Devletleri başkanlık seçimlerine müdahale edebilmektedirler (Türkiye Bilişim Sanayicileri Derneği, (TUBISAD), Türkiye'nin Siber Güvenlik Stratejisine Yönelik Değerlendirmeler). Devlet kurumları, özel sektör ve bireysel kullanıcılar olarak bir siber uzayın içinde bulunmaktayız ve siber uzayın bir bileşeniyiz. Siber uzayda tüm bileşenlerin birbirleriyle bağlı olması siber güvenlik riskleri ve belirsizliklerini beraberinde getirmektedir.

Bu riskler ve belirsizlikler kişilerin veya devletlerin kendilerini korumak amaçlı alacağı önlemler ile en aza indirgenebilir. Teknoloji insanoğlunun ihtiyaçları ve bu ihtiyaçların çözümü noktasında ortaya çıkmış olan tüm icatlar ve buluşlardır diyebiliriz. İletişim alanında telefon,

radyo, internet; ulaşım alanında uçak, araba, tren, otomobil gibi ürünleri ile insanların günlük hayatlarının vazgeçilmezleri haline gelmiştir (Bacanak, A., Karamustafaoğlu, O., Köse, S. (2003)).

Siber güvenlik, siber uzayda verilerin, operasyonların, süreçlerin, politikaların, uzmanlığın, yeteneklerin, insanların ve sistemlerin sağlanmasıdır (Sağıroğlu Ş., Alkan M., Samet R., ve ark. (2018)). Dünya üzerinde internet kullanımı her geçen gün artmaktadır. Gelişen teknoloji ile internete ulaşımın çok kolaylaşması, yeni neslin direk internet teknolojisinin içine doğmuş olması bu artışın birkaç sebebi olarak gösterilebilir. İnternet teknolojisinin gelişmesi beraberinde kurumlara, kişilere, kritik altyapılara veya ülkelere siber saldırıların artması ve bu saldırıların maddi kayıpların dışında kamu düzeni ve güvenliği etkileyecek boyutlara gelmesi siber güvenlik alanında çalışmalara hız verilmesine sebep olmuştur (Ünver M., Canbay C., (2010).

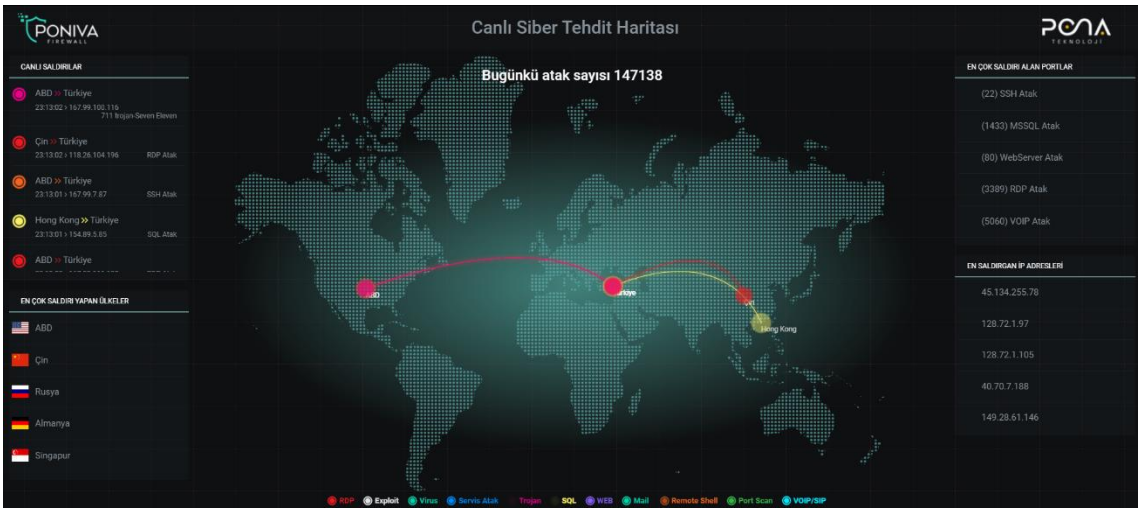
Bilgi güvenliği politikalarının oluşturulmasında ve uygulanmasında başarılı olmak için tüm yönleriyle birlikte değerlendirilmelidir. Bilginin gizliliği, bütünlüğü ve kullanışlılığının yanı sıra bu süreci etkileyen insan faktörü ve bilgi güvenliği politikaları da büyük önem taşımaktadır. Şekilde McCumber tarafından geliştirilen küp modeli, bilgi güvenliği politikalarının geliştirilmesi ve bilgi güvenliğinin tüm boyutlarıyla uygulanması için temel alınabilecek en uygun bilgi güvenliği modelidir. Bu model, bilgi güvenliğine göre gruplandırılmış bilginin üç farklı yönünü (tür, durum ve güvenlik kontrolleri) temsil eder (McCumber J.R. (1991).




**Şekil 1.1.** McCumbur Küpü

Siber güvenlik alanında kişilerin veya kurumların internet ağı içeren herhangi bir cihazını ele geçirmek, işlevini bir süreliğine aksatmak veya sisteme kalıcı hasar verebilmek üzerine kurgulanmış ve ön planda saldıran kişinin kimliğinin gizliliğini koruma ihtiyacı duyan saldırı sistemleridir. İnternet kullanımının yaygınlaşmasından bugüne kadar siber saldırı olaylarının sayısı ve siber saldırı türleri doğru orantılı olarak arttığını gözlemlemek mümkündür.

Şekil 1.2 'de 10.11.2020 saat 14:43:00 itibariyle siber saldırı ve türlerini gösterir bir harita yer almaktadır.




**Şekil 1.2.** Pona'dan alınan canlı siber saldırı haritası

(https://stm.pona.com.tr/ Erişim Tarihi: 24.12.2021 Saat 23:14)

Türkiye üzerinde en çok karşılaşılan siber saldırı çeşitleri şu şekilde sıralanabilir,

- Fidye Yazılımları: Bilgisayarlar, mobil telefonlar ve ağa çıkabilen diğer aygıtlardaki dijital verileri ellerinde tutup, bu verilere erişimin açılması için kullanıcıdan para talep eden zararlı yazılımlardır.
- Olta Saldırıları: Yemleme saldırısı olarak da adlandırılan bu saldırı türü, kişisel veya hassas verilerin bilgi teknolojileri kullanılarak kandırılarak veya ikna edilerek ele geçirilmesi ve bu verilerin kötü amaçlarla kullanılmasıdır.
- Kredi Kartı Dolandırıcılığı: E-ticaret sitelerinden yapılan alışverişlerde, alışveriş yapan kişinin kredi kartı bilgilerinin ele geçirilmesidir.

- Dağıtılmış Hizmet Reddi (Distributed Denial of Service- DDOS) Saldırıları: Bu saldırı türü botnet denilen zombi bağlantıları kullanarak bir sistemi çok fazla istek gönderme yoluyla yavaşlatma veya durdurma amacı taşır.

Gerçekleştirilmesi en kolay saldırı türlerindendir fakat verdiği zarar boyutu olarak çok etkilidir. Bu sebeple sıklıkla tercih edilebilmektedir.

- Mobil Tehditler: kötücül yazılımlar mobil cihazlardan bilgi çalmak, mobil cihazları kilitlemek, devre dışı bırakmak ya da kalıcı hasarlar vermek için kullanılabilir.

Siber saldırılar sadece kişisel düzeyde kalmamış olup devletler arasında da zarar verici ve savaş niteliğinde olaylara neden olmuştur. Gelişen teknoloji ile birlikte dünya toplumunun yüksek bir bölümü internete ulaşabilmektedir. Ülkelerin büyük bir bölümü artık vatandaşlarının işlemlerini internet üzerinden gerçekleştirmelerini sağlayan sistemler ortaya koymaktadır (Sağıroğlu Ş., Alkan M., Samet R., ve ark. (2018) & Ünver M., Canbay C., (2010)).

*Siber Saldırı Türleri*

Siber saldırı türleri aşağıda yer almaktadır. Siber saldırı türleri ayrıca ilgili alt başlıklarda açıklanmıştır.

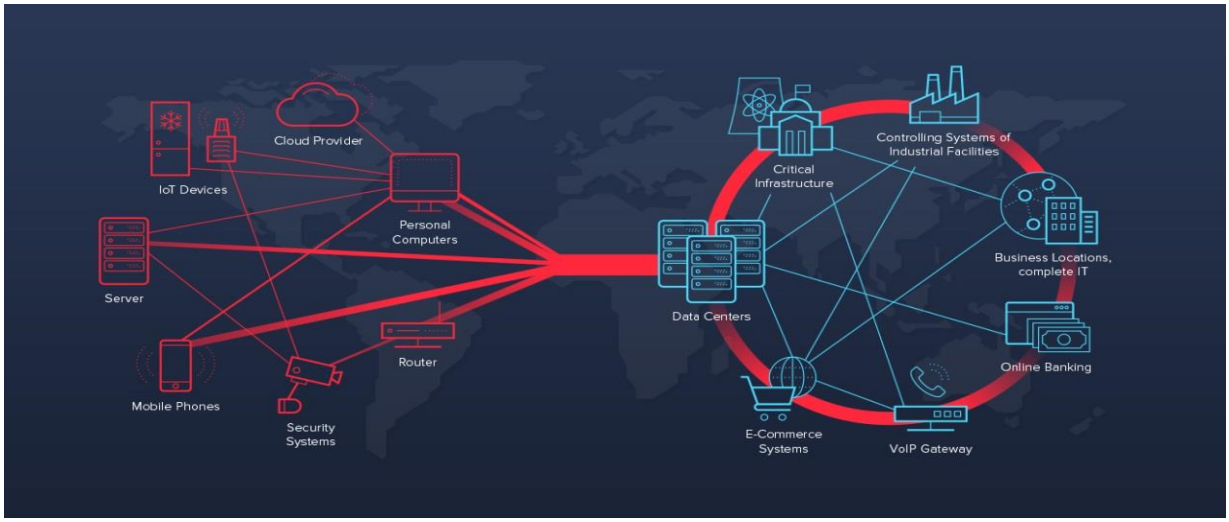
- Koklama (sniffing)
- Hizmet Dışı Bırakma (Denial of Service)
- IP Aldatması (IP Spoofing)
- Sosyal Mühendislik
- SQL Enjeksiyonu
- Arka Kapılar
- Oltalama
- Casus yazılım (Spyware)
- Kötü amaçlı yazılım (Malware)

Sniffing Saldırıları

Sniffing saldırılarının gerçekleştirilmesindeki temel amaç şifreleri ele geçirmektir. Ayrıca bunun yanı sıra e-mail içeriklerini transfer eden dosyaların ele geçirilmesi hedeflenir. Yönlendiricilere gelen paketlerin kabul edilmesi ile iki bilgisayar arasındaki tüm veriler yakalanarak saklanmaktadır (Aydın ve ark & Arslan).

*Hizmet Dışı Bırakma Saldırıları*

Bu tür saldırılar hizmeti aksatma ya da hizmeti tamamen işlevsiz hale getirmek üzere gerçekleştirilen saldırılardır. DDos (Distributed Denial of Service) saldırılarında saldırgan öncelikle makine ve bilgisayar topluluğu oluşturur. Bunun ardından hedefe saldırır ve DDos saldırılarının amacı da yine Dos saldırıları ile aynıdır. DDos saldırı türünde saldırgan kimliğini daha kolay bir biçimde gizlemektedir (Aydın ve ark & Arslan). Aşağıda yer alan şekilde DDos gösterilmiştir.



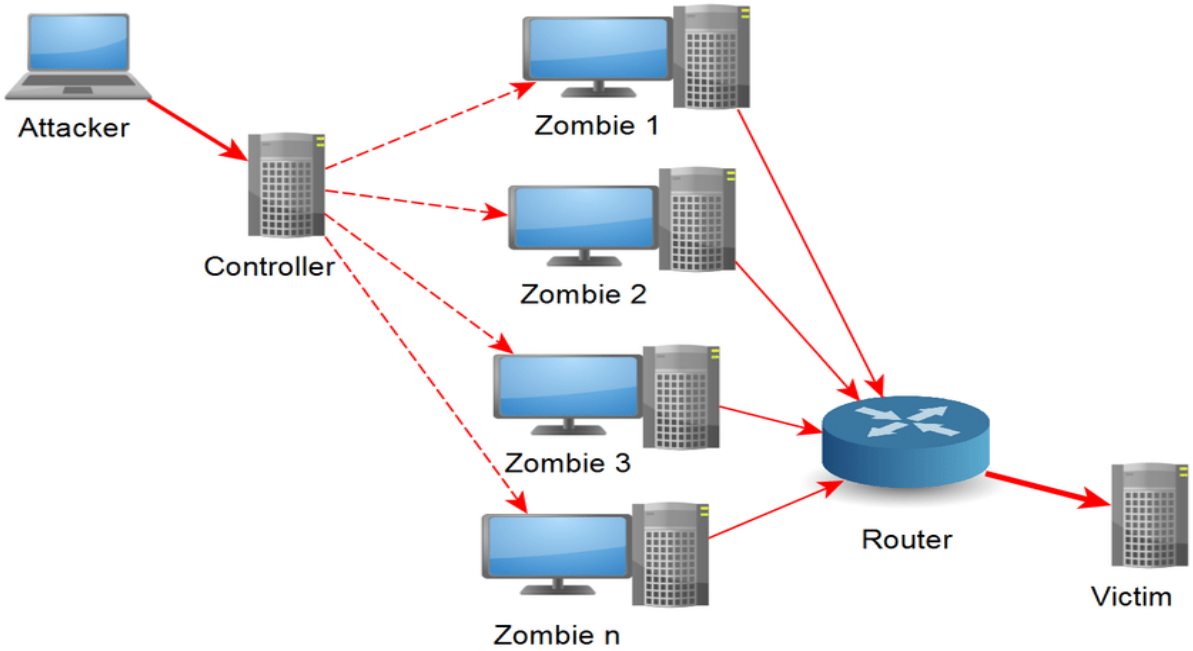

**Şekil 1.3. DDos Saldırısı**
((https://www.link11.com/en/what-are-ddos-attacks/))

Dos saldırıları tek bir IP üzerinden gerçekleştiriliyorsa Firewall ile engellenmektedir. Ancak DDos söz konusu olduğunda durum daha karmaşık bir hal almaktadır. Zira şekilde de görüldüğü üzere çok sayıda makine kullanıldığından ötürü IP tespiti zorlaşmaktadır. Firewall ile engellenemeyebilir. Log taşması sebebiyle firewall devre dışı kalmaktadır. Sonuç olarak DDos saldırıları Dos saldırılarından daha tehlikeli ve etkili saldırılardır. DDos ise Dos saldırı türünün daha sık aralıklarla saldırılar düzenlemek amacıyla ek ağların kullanıldığı çeşididir. Genel anlamda Dos saldırıları en tehlikeli ikinci saldırı türü olarak karşımıza çıkar (Aydın ve ark & Arslan).

*IP Aldatması*

Bilgisayarlar birbirleriyle çeşitli protokoller aracılığıyla iletişim kurmaktadırlar. Protokoller sayesinde bağlanan bilgisayar bağlandığı bilgisayara kimliğini tanıtmaktadır. Bağlanılan bilgisayara gerçek IP adresi gösterilmemesi dolayısıyla asıl kimliğin gizlenmesine IP spoofing adı verilmektedir (Aydın ve ark & Arslan).

Sahte IP paketi tarafına ulaşan bilgisayar paketin gerçekten o adresten gelip gelmediğini bilemez. IP spoofing genellikle web sitesini işlemez hale getirmek için saldırı esnasında kaynağı gizleme amacıyla kullanılmaktadır (Aydın ve ark & Arslan). Aşağıda yer alan şekilde IP spoofing gösterilmektedir.




**Şekil 1.4.** IP Aldatması
(https://www.researchgate.net/figure/Elements-that-constitute-a-distributed-denial-of-service-attack_fig1_319901682))

*Sosyal Mühendislik*

Sosyal mühendislik siber saldırı türünde insanların zaaflarından faydalanılmasıyla siber güvenlik süreçlerinin atlatılması ya da etkisiz hale getirilmesi olarak tanımlanmaktadır. Sosyal mühendislik yöntemleri arasında hedefe güvenilir bir kaynak olarak tanıtma, yalan senaryolar oluşturma veya ödüllendirme yer almaktadır (Aydın ve ark & Arslan).

*SQL Enjeksiyonu*

SQL enjeksiyonu veri tabanı sorgulama işlemini hedef almaktadır. Bu saldırı türünde sorgulama dili yapısı kullanılarak saldırı yapılmaktadır.

*Komut Enjeksiyonu*

Komut enjeksiyon saldırıları, doğrudan sunucuları hedefleyen bir saldırı türüdür. Amacı, bir web uygulamasının komut satırı aracılığıyla uzaktan erişim yoluyla işletim sistemi, sunucu bilgileri ve veritabanı yönetim sistemindeki bilgileri yakalamaktır (Aydın ve ark & Arslan).

*HTML Enjeksiyonu*

Bu saldırı türünde kodlama sırasında programcıların gerçekleştirmiş olduğu hatalı kodlama kullanılır. Web yazılımlarında, veri tabanından çekilen verilerin veya veri tabanına giren verilerin bir kontrol mekanizmasından geçirilmemesi sistemde açığa sebep olmaktadır. Sayfaya gönderilen istek sunucu tarafından değerlendirilir ve yanıtlanır. Ancak giriş yapılan sayfanın kötü amaçlı bir URL bağlantısına yönlendirilmesi halinde yanıt beklenildiği gibi olmayacaktır. Bu saldırı türünde hedef uygulamayı ziyaret edenlerdir. Web uygulaması hedef değildir. Web uygulamasının açıklarından faydalanılması suretiyle uygulamayı ziyaret edenlere yönelik saldırı düzenlenmesi hedeflenmektedir (Aydın ve ark & Arslan).

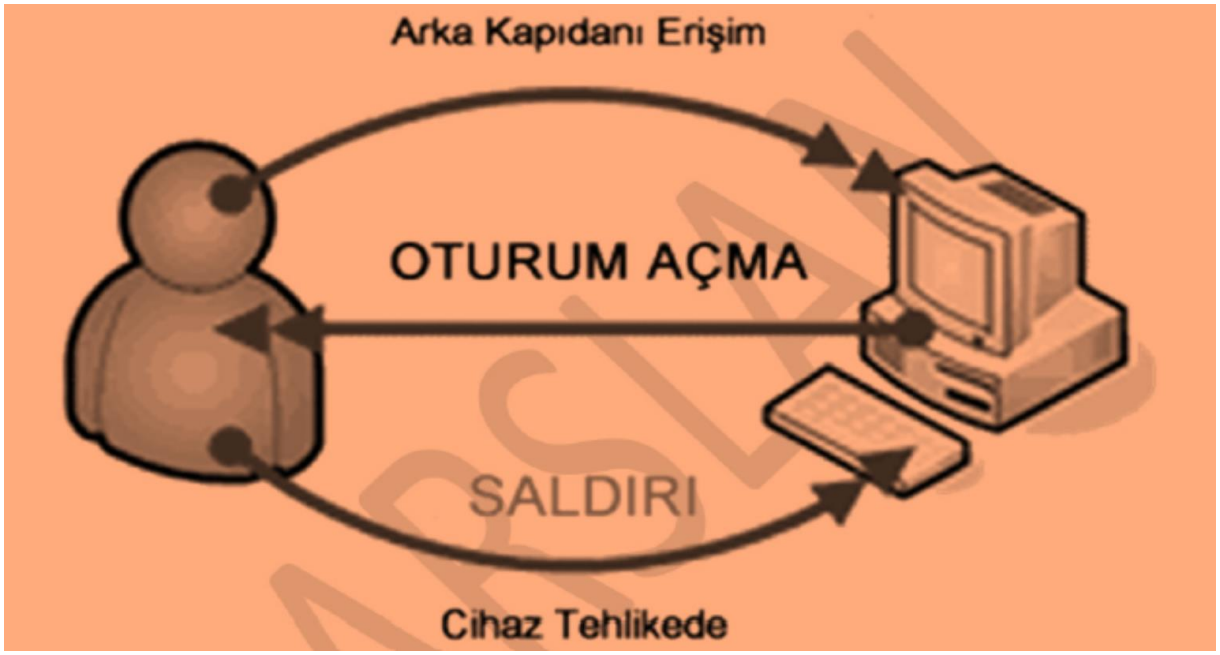
*Arka Kapılar*

Normal kimlik tanımlama süreçlerini atlamak ya da bilgisayara uzaktan erişime olanak tanıyan yöntemlere arka kapı adı verilmektedir. Siber suçlular sisteme sızmak için çok fazla çaba harcamaktadırlar. Bu sebepten ötürü aynı sisteme tekrar erişmek üzere kolay bir girişi sisteme eklemeyi arzu ederler. En yaygın arka kapı yöntemi, bağlı bir dinleme aracısı ile hedef sistemdeki çıkışı sürdürmektir.

Bu bağlamda, belirtilen güvenlik açığının keşfedilip keşfedilmediğini kontrol etmek için 1'den 65535'e kadar mevcut tüm bağlantı noktalarını (TCP ve UDP) iki kez taramak gerekir. Arka kapılar ve truva atları birbirine karıştırılmaktadır. Arka kapılar ve Truva atları, bir sisteme sızmak için tasarlanmış kötü amaçlı yazılımlardır. Ancak arka kapı sadece sisteme erişim sağlayan gizli bir yapıdır, ancak Truva atı görünüşte kullanışlı bir programdır.

Virüsler her zaman mutlaka arka kapı açmayı denerler. Arka kapılar virüsü yayan taraf için erişimde kolaylık demektir. Arka kapılar sistemi geliştiren programcı tarafından test edilen

fakat daha sonra unutulmuş olunan sistem zafiyetleri olarak karşımıza çıkabilmektedirler. Siber suçlular bu zafiyetin farkına varıp kullanabilirler. Arka kapılar aşağıda verilen şekilde gösterilmiştir (Aydın ve ark & Arslan).




**Şekil 1.5.** Arka kapılar

*Oltalama (Phishing)*

Oltalama saldırılarının temel amacı, kullanıcının banka hesap numaralarını, bankacılık işlemleri için kullanılan şifreleri ve kredi kartı bilgilerini ele geçirerek kullanıcıyı internette yanıltmaktır. Bu tür saldırılar alışveriş siteleri, havayolları, arkadaşlık siteleri vb. ile bankacılık işlemlerinin yürütüldüğü sitelerde gerçekleşmektedir. Ayrıca ATM'lere mikro kameralı kart okuyucu ve sahte klavye mekanizmaları yerleştirilerek bu tür saldırılar düzenlenmiştir.

*Casus Yazılım (Spyware)*

Casus yazılımlar kullanımı zararsız görülen ve genellikle internetten bedava olarak indirilerek bilgisayarlara bulaşan programcıkları içermektedir. Son kullanıcı sözleşmesi, programla birlikte kurulacağını belirtir. Sözleşme kabul edildiğinde programla birlikte kurulmuş olmaktadırlar.

Bu programların temel amacı, kurulu oldukları bilgisayardan bilgi toplamak ve elde edilen bilgileri yazılımı geliştiren kişilere iletmektir. Casus yazılımları virüs olarak sınıflandırılmazlar. Daha ziyade hangi sitelerin ziyaret edildiği, ne kadar süre kalındığı, bilgisayar ve sistem kurulum şifreleri ya da kredi kartı bilgilerini ele geçirmek üzere

tasarlanmaktadırlar. Gezinti bilgilerini İnternet Explorer eklentileri ile biriktirirler. Böylelikle ziyaret edilen siteleri tespit ederler. Ardından bu verileri arama siteleri sonuçlarının sıralanması amacıyla kullanabilirler. Bu tip casus yazılımlara nazaran daha tehlikeli olan türleri de vardır. Bunlar bilgisayar ya da internet ayarlarını değiştirir ve kendi istedikleri sitelere yönlendirme yaparlar. Ayrıca başlangıç sayfasını değiştirirler. Dahası nereden geldiği anlaşılmayan ve/veya bilinmeyen reklam içerikli pencereler açarlar. Bu tip casus programlara Adware adı verilmektedir (Aydın ve ark & Arslan).

*Kötü Amaçlı Yazılımlar (Malware)*

Kötü amaçlı yazılımlar aşağıda yer almaktadır:

1. Virüsler
2. Truva Atları
3. Solucanlar
4. Botlar
5. Zombi Ordular (Botnetler)
6. Bankacılık Zararlıları
7. Fidye Yazılımları
8. Kaydediciler (Keyloger)
9. RAT (Remote Access Trojan)

*Virüsler*

Tüm kötü amaçlı yazılım türleri virüs olarak sınıflandırılamaz. Biyolojik virüsler gibi diğer dosyalara bulaşarak yayılan bir tür kötü amaçlı yazılıma virüs denir. Literatürdeki ilk virüs 1986 yılında ortaya çıkan "Brain" adlı bir virüstür. Bu virüs IBM – PC tabanlı boot sector virüsüdür. Sistemde virüs olduğuna dair belirtiler aşağıda verilmiştir.

- Boşta kalma süresi boyunca sürekli veri trafiği. Bunun sebebi başka kullanıcıların sistemde aktif olmaları ve kötü amaçlı işlemler yapıyor olmalarıdır.
- Sistemde güvenlik duvarı olmasına karşın bazı uygulamaların internetten bağlanmaya teşebbüs etmeleri.

- İnternet siteleri ziyaret edilirken reklam pencerelerinin kendiliğinden açılması.
- Bilgisayarın işlevsiz hale gelmesi.

*Truva Atları*

Faydalı bir işlevi varmış izlenimi uyandıran fakat güvenlik mekanizmalarını aşabilecek zararlı işlevlere sahip programlardır. Truva atları bilgisayarları uzaktan yönetmek için arka kapı açılması amacıyla kullanılır. Kullanıcılar farkında olmadan bilgisayarlarına programları indirirken aynı zamanda kötü niyetli programları da indirmektedirler. Söz konusu bu programlar arka planda çalışırlar. Böylelikle uzaktan erişim imkânı sağlarlar. Truva atları aracılığıyla sisteme arka kapıdan giren siber suçlular kullanıcı şifreleri ve diğer kişisel bilgilere ulaşma imkanına sahip olurlar. Ayrıca sistem yapılanmasını değiştirebilirler. Diğer bir ifadeyle, Truva atı sisteme bulaştıktan sonra sistem açıldığında kendisini belleğe yükler. Sistem ağlarının açıklarını kullanmak suretiyle siber suçlular amaçlarını yerine getirmeye başlarlar. Truva atlarının farklı çeşitleri mevcuttur. Amaç bakımından aynıdırlar fakat özellikleri birbirlerinden farklıdır. Truva atları altı farklı grup altında toplanır. Bunlar;

- Uzaktan kontrol edilen Truva atları
- Parola Truva atları
- İmtiyazlı Truva atları
- Anahtar kırıcı Truva atları
- Yıkıcı Truva atları
- Şaka programları olarak kullanılan Truva atları

Özetle bir siber suçlu Truva atını kullanarak program yapısına göre farklı faaliyetler gerçekleştirebilmektedir.

*Solucanlar*

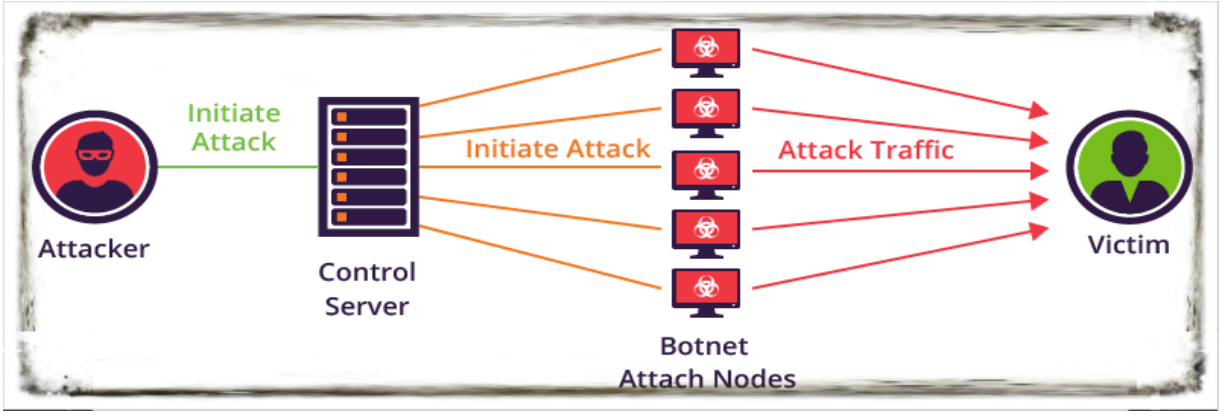
Solucanlar virüslere benzer şekilde kendilerini bir bilgisayardan başka bir bilgisayara kopyalamak üzere tasarlanırlar. Virüslerden farklı olan tarafları ise bunu kendi başlarına gerçekleştirmeleridir. Bilgisayarda veri ya da dosya transferini gerçekleştiren fonksiyonların denetimini ellerine geçirdikten sonra kendi başlarına yollarına devam edebilme becerisine sahiptirler. Solucanların bir diğer yeteneği de çoğalma becerileridir. Kullanıcıların dosya ve veri

alışveriş yöntemlerini kullanmak suretiyle kendilerini tüm e-posta ve tüm sistemlere gönderebilme becerileri vardır. Bu sebepten ötürü ağ trafiği önemli ölçüde yavaşlamaktadır. Güvenlik yazılımları solucanları kolaylıkla tanımayabilirler.

*Botlar*

Bot terimi bilişim alanındaki "robot" anlamında kullanılmaktadır. Bilgisayar işlemlerini yarı otomatik olarak yapabilirler. Sıklıkla arama motorları tarafından endeksleme teknolojisinde kullanılmaktadır. İnternetin yaygınlaşmasıyla birlikte akıllı ajan teknolojileri de yaygınlaşmaya başlamıştır. Bu sebepten ötürü internet üzerinde faaliyet göstermek üzere geliştirilen ajan yazılımları ortaya çıkmıştır.

Finansal alanda botlar ticari veri madenciliği, hisse senedi, yatırım faaliyetleri gibi alanlarda yer almaktadırlar. Aşağıdaki şekilde bot-net gösterilmiştir.




**Şekil 1.6.** Bot-net

(https://www.cybercrimeinfo.nl/van-a-tot-z/botnet)

*Zombi Ordular (Botnetler)*

Zombi ordular veya başka bir deyişle botnetler zararlı yazılımlar grubunda en tehlikeli olanlardır. Kullanıcıların bilgisi olmaksızın suç işlenmesi mümkün olmaktadır. Bot-netlere katılan bilgisayarlarda genellikle firewall bulunmamaktadır. Son yıllarda bant genişliği artmıştır. Dolayısıyla herhangi bir korumaya sahip olmayan bilgisayarlar kolayca bot-netin içerisine dahil edilebilmektedir.

Bot – netler şu şekilde oluşturulmaktadır. Açık bırakılan bir kapı (port) içerisinden daha sonra aktif hale gelecek bir Truva atı gönderilmesi sonucunda bot-netler oluşturulmaktadır. Bot-nete dahil edilen bilgisayarlar eş zamanlı olarak bir web-sitesine yönlendirilmek suretiyle söz

konusu web-sitesini hizmet veremez hale getirmek üzere kullanılabilmektedir (Aydın ve ark & Arslan).

*Bankacılık Zararlıları*

Bankacılık zararlıları, çevrimiçi bankacılık sistemleri aracılığıyla saklanan veya işlenen gizli ve/veya maddi bilgilere erişim sağlamak için tasarlanmış kötü niyetli bilgisayar programlarıdır. Bu tür bir bilgisayar programları, dış tarafların bir bilgisayara erişmesine izin veren bir arka kapı ile oluşturulmuştur ve banka müşterisinin kimlik bilgilerin kopyalanmasına imkân tanıyabilirler.

Bankacılık zararlıları, bilgisayar cihazına yüklenene kadar meşru bir yazılımın parçası olarak görünebilir. Yüklendikten sonra, saldırganların yetkisiz işlemler yapmak, müşterilerin kimliklerini çalmak veya saldırganların hesaplarına müşteri fonlarını çekmek için kullandığı bilgisayar dosyalarına ve sistemlerine erişim sağlayabilirler.

Trojanlar, yürütülebilir dosyaları çalıştırma, dosyaları uzaktan indirme ve gönderme, bir panodan bilgi çalma ve tuş vuruşlarını kaydetme gibi bir dizi işlemi gerçekleştirebilir. Çerezleri ve şifreleri toplar ve komut verildiğinde kendisini bilgisayardan kaldırabilir.

*Fidye Yazılımları*

Fidye yazılımı, şantaj yazılımı veya fidye virüsü: ransomware olarak adlandırılan fidye yazılımlarına verilen genel bir addır. Fidye virüsleri bulaştığı bilişim sistemleri üzerinde dosyaları erişimi engelleyerek kullanıcılardan fidye talep eden zararlı yazılımlardır.

Basit bir fidye virüsü, bilgili bir kişinin geriye çevirmesi zor olan bir şekilde sistemi kilitler ve kilidi açmak için ödeme isteyen bir mesaj gösterir. Daha da gelişmiş zararlı yazılımlar, kurbanın dosyalarını şifreler, bunları erişilemez kılar ve bunların şifresini çözmek için bir fidyenin ödenmesini talep eder. Fidye virüsü, bilgisayarın Ana Dosya Tablosu (MFT) veya tüm sabit sürücüsünü de şifreleyebilir. Şifreleme anahtarı olmadan dosyaların şifrelerinin çözülmesine karşı olduğu için, fidye virüsü bilgisayar kullanıcılarının dosyalarına erişimini engelleyen bir erişim dışı bırakma saldırısıdır. Fidye virüsü saldırıları, geçerli bir dosya olarak kendisini gizleyen bir Truva atı kullanılarak yürütülmektedir.

*Kaydediciler (Keyloger)*

Açıklama olarak klavye dinleme sistemi ya da klavye yakalama sistemi olarak verilebilen keyloger, temel amaç olarak klavye üzerinde basılan bir tuşu, sistemde gizli olarak var olan bir casus yazılımın dinlemesi diğer bir ifade ile o tuşun kayıt altına alınması olarak açıklanabilir. Kullanılan sisteme kötü amaçlarla bulaştırılan bu casus yazılımlar daha çok spam olarak isimlendirilen mailler, çeşitli internet sitelerinde bulunan açılır reklamlardan, internetten indirilen ve kaynağı kesin olan belli olamayan dosyalar aracılığı ile sisteme bulaşabilmektedirler.

Keyloger casus yazılımlarının temelinde amacı kötü niyetli kişilerin sistemde bulunan çeşitli ve özel dosyaların şifrelenmesi ve bu dosyalara ulaşım için para talep etmesi bulunmaktadır. Kullanılan bir sisteme keyloger bulaşmışsa eğer bu casus yazılımdan kurtulmak amacı ile güncel olarak üç farklı yol belirlenmiştir. İlk olarak Dosyaların yedeği bulunuyor ise sisteme format atmak, ikinci olarak sistem geri yükleme seçeneği kullanılabilir, son olarak çeşitli disk kurtarma programları kullanılarak dosyaların kurtarılması sağlanabilir.

*Remote Acceses Trojan (RAT)*

Remote Access Trojan kısa ifadesi ile RAT bir cihaz üzerinde arka planda çalışmaktadır. RAT cihazı kullanan kişisini haberi ve bilgisi olamadan çalışmaktadır ve cihazda bulunan çeşitli dosyaların ve bilgilerin üçüncü taraf kişilere ulaştırılması gibi bir amaç taşımaktadır. RAT yazılımları genel olarak küçük ve orta ölçekli yasa dışı işlemler için kullanılmaktadır. Bilgisayarda yasa dışı işlemler yapan ve bu işlere yeni başlayan kişiler tarafından tercih edilmektedir. Genel olarak bu kişiler tarafından eğitim ve eğlence amacı ile kullanılır fakat yine de yasa dışı bir işlem olmakla birlikte eğlence dışında kötü amaçlar içinde kullanılmaktadırlar.

Genel olarak RAT yazılımları crack dosyalarının içinde veya oyunlarda hile amacı ile kullanılan programlar aracılığı ile bulaşabilmektedir. RAT bulaşmış olan bir sistemde kötü amaçlı kişi veya kişiler sistemin kamerasına, ekranına, klavye ve faresine, sistemde bulunan dosyalara, mikrofona vs. sistemde olan hemen her şeye erişebilir veya bilirler.

### 1.6.2. Genel Kavramlar

*Eğitim*

Bireyin davranışlarında kendi yaşantıları yoluyla ve kasıtlı olarak istendik değişme meydana getirme sürecidir (Ertürk, 1984, s. 12).

*Öğretim*

Öğrenmenin gerçekleşmesi için planlanan, kasıtlı ve sistematik eğitim olarak tanımlanabilir (Demirel, 2003).

*Eğitim Teknolojisi*

Eğitim teknolojisi, eğitim hakkındaki teorik bilgilerin pratik hale dönüştürülmesi olarak ifade edilmektedir (Alkan, 2011).

*Öğretim Teknolojisi*

Çeşitli şekillerde tanımı yapılmakta olan öğretim teknolojileri, eğitim teknolojileri ile karıştırılmaktadır. Genel anlamda öğretimin eğitimin içerisinde olduğu düşünüldüğünde, öğretim teknolojileri; öğrenmede kullanılan nesneleri yani, öğrenme ve öğretme sürecinde yer alması düşünülen her çeşit materyal ve araç-gereçleri tanımlamaktadır (Demirel & Altun, 2009, s. 1-127).

Bibliyografya

Bir disiplin olarak bibliyografya, geleneksel olarak kitapların fiziksel, kültürel nesneler olarak akademik çalışmasıdır; bu anlamda bibliyoloji olarak da bilinir. Bibliyografyaların nicel çalışması bibliyometri olarak bilinmektedir (Wikipedia, Bibliography).

Bibliyometri; makale, kitap ve diğer yayınları analiz etmek üzere istatistiksel yöntemlerin kullanılmasına verilen addır. Bilimsel yayınların analizi ile ilgilenen bibliyometri alt alanına bilimetri adı verilmiştir (Wikipedia, Bibliometrics).

Atıf analizi, belgeler arasında atıfların bir ağ veya grafik ile temsil edilmesini, atıf grafiği oluşturulmasına dayanan bibliyometrik bir yöntemdir. Bibliyometrik yöntemler çeşitli araştırma alanlarında söz konusu araştırma alanına araştırmacının etkisini, belirli bir makalenin etkisinin

belirlenmesi veya belirli bir araştırma alanında özellikle etkili olmuş makalelerin tespiti için kullanılan bir yöntemdir (Wikipedia, Bibliometrics).

## 1.7. İlgili Araştırmalar

Eğitimde önemli bir yeri olan tezler, bilgi ve bilim üretimi konusunda araştırma ve etkinliklere katkı sağlar niteliktedir. Tez çalışmaları aynı zamanda çalışmayı yapan bireye alanı hakkındaki güncel durumları takip etme fırsatı da sunmaktadır.

Eğitim sürecinde hazırlanan tezler, ele alındıkları konular bakımından bir yandan yazara gelecekte akademik çalışma alanı sunarken bir yandan da literatüre katkıda bulunmaktadır. Bu noktada hazırlanan tezlerin sayısı ve ele alınan konulardaki çeşitlilik de bilginin miktarı ve kapsamına dair durum tespitlerinde önem taşımakta olup öğrencilerine ve tez danışmanlarına tez konusunu belirleme sürecinde yardımcı olmaktadır. Yine aynı şekilde kullanılan araştırma yöntemleri ve veri toplama teknikleri de bilgiye ve sonuca ulaşım noktasında öngörü oluşturmaktadır.

Çalışmalarda konu seçimlerinde dikkat edilmesi gereken en önemli husus kapsamlı bir literatür taramasıdır. Konu seçiminin ardından ise konu uygunluğuna göre yöntem seçimi yapılacak olan çalışmanın özgünlüğü açısından önem taşımaktadır.

Birçok disiplin belirli bir olgunluk seviyesine ulaştığından ötürü gelişmiş bilgisayar programlarıyla disiplinlerin gelişimini betimlemeye ve değerlendirmeye yönelik çalışmalara olan ilgi artmıştır (Zupic & Cater, 2015, s. 430). Bir araştırma alanının gelişimi için yapılması gereken en önemli çalışmalardan birisi de o alanda daha önce yürütülmüş araştırma bulgularının sentezlenmesidir (Zupic & Cater, 2015, s. 429). Bununla ilgili olarak bibliyografik araştırmalara yönelim zamanla artış göstermektedir. Bibliyografik araştırmalarda çözümlemeyle bulgular elde edilmektedir.

# BÖLÜM 2

## 2. VERİ SETİ VE YÖNTEM

Nitel özellik taşıyan bu araştırmada kaynak taraması yapılacak olup veriler doküman analizi yöntemiyle toplanacaktır. Tezler, sayısal olarak elektronik ortama aktarılmak suretiyle, YÖK Ulusal Tez Merkezinden elde edilmiştir. Bu bölümde araştırmanın modeli, veri toplama aşamaları, toplanan verilerin analizi yer almaktadır.

### 2.1. Araştırmanın Modeli

Model denildiğinde akla ilk gelen şey araştırılan konunun tasarlanması, planlanması yani dizayn edilmesidir. Bu çalışma tarama modeli ile yürütülecektir. Yıldırım'a göre, "tarama modelinde bilimin gözleme kaydetme, olaylar arasındaki ilişkileri tespit etme, kontrol edilen değişmez ilişkiler üzerinde genellemelere varma vardır. Yani bilimin tasvir fonksiyonu ön plandadır." (Yıldırım C., 1966, s. 67)

Bu çalışmada nitel araştırma yöntemi kullanılacaktır. Nitel araştırma, Yıldırım ve Şimşek (2011, s. 39)'e göre gözlem, görüşme ve doküman analizi gibi nitel veri toplama tekniklerinin kullanıldığı, algıların ve olayların doğal ortamda gerçekçi ve bütüncül bir biçimde ortaya konmasına yönelik nitel bir sürecin izlendiği araştırma olarak tanımlanmaktadır.

Araştırmada nitel araştırma yöntemlerinden biri olan betimsel çalışma yöntemi kullanılacaktır. Betimsel çalışmalar ilişkiyi ya da farkı göz etmeksizin neyin ne olduğunu belirlemeye yönelik çalışmalardır. Dolayısıyla betimsel çalışmalar, bilimin betimleme amacına hizmet etmektedirler. Ancak bunun yanı sıra aynı zamanda sonraki çalışmalar için de fikir üretmeye yönelik fikir sahibi olunmasına imkân sağlamaktadırlar. Akademik yayınların istatistiksel ve metodoloji bakımından ele alınmalarına yine betimsel çalışma adı verilmektedir (Erkuş, 2009).

### 2.2. Araştırmanın Evreni ve Örneklemi

Araştırmanın evrenini siber güvenlik, bilgi güvenliği ve veri güvenliği alanlarında yapılan ve Yükseköğretim Kurulu Ulusal Tez Merkezinde yer alan tezleri oluşturmaktadır.

Araştırmanın örneklemi ise, amaçlı örneklem yöntemiyle seçilen siber güvenlik, bilgi güvenliği ve veri güvenliği alanlarında yapılan ve Yükseköğretim Kurulu Ulusal Tez Merkezinde erişimi açık olan tezleridir.

Literatür taraması Aralık 2021'de gerçekleştirilmiştir. Türkiye'de siber güvenlik, bilgi güvenliği ve veri güvenliği alanında yapılmış olan 234 adet tez bulunmuştur. Erişim izni olmayan ya da tamamlanmadığı düşünülen tezler kapsam dışı bırakılmıştır. Çalışma kapsamında 225 adet tez üzerinden analiz yapılacaktır.

### 2.3. Veri Toplama Araç ve/veya Teknikleri

Araştırmada veri toplama aracı olarak nitel araştırmalarda sıkça kullanılan doküman analizinden yararlanılacaktır. Tezlerin yer aldığı YÖK Ulusal Tez Merkezi veri tabanında yapılan tarama sonucunda erişilen ilgili tez çalışmaları, öncelikle konu ve yöntem olarak; sonrasında yıllara, üniversitelere, üniversitelerin bulunduğu illere, tez sayılarının hazırlandığı üniversitelerin bulunduğu illere, üniversite türlerine, enstitülere, anabilim dallarına, bilim dallarına, tez yazarlarına ve danışmanlarına, tez sayfa sayılarına, tez erişim durumlarına, veri toplama tekniklerine göre incelenerek, mevcut durum ortaya konulacaktır.

### 2.4. Verilerin Toplanması

Türkiye'de siber güvenlik, bilgi güvenliği ve veri güvenliği alanında yapılmış olan tezlerinin yer aldığı bu çalışmada, veriler YÖK Ulusal Tez Merkezinden (https://tez.yok.gov.tr) elde edilmiştir. Toplamda 234 tezinden erişimi sağlanan 225 adet tezi değerlendirilmek üzere ele alınacaktır.

### 2.5. Veri analizi

Bu bölümde Türkiye'de siber güvenlik, bilgi güvenliği ve veri güvenliği alanında yapılan tezlerinin dağılımları verilecektir. Yapılacak dağılımda tez çalışmaları YÖK Tez Merkezi'nden pdf formatında indirilerek tam metinlere erişim sağlanmış olup; yıllara, üniversitelere, üniversitelerin bulunduğu illere, tez sayılarının hazırlandığı üniversitelerin bulunduğu illere, üniversite türlerine, enstitülere, anabilim dallarına, bilim dallarına, tez yazarlarına ve danışman unvanlarına, tez sayfa sayısı aralıklarına, tez konularına, araştırma yöntemlerine ve veri toplama tekniklerine göre incelenerek Microsoft Excel programında tablo olarak kodlanacak ve çözümlemelerde bulunulacaktır. Çözümleme sonucu elde edilen veriler, SPSS programına aktarılarak verilerin frekans dağılımları yapılacak, sonuçlar sayı (N) ve yüzde (%) ile belirlenecektir. Gruplandırılan bilgilerin dağılımları, tablolar ve grafikler hâlinde sunulacak ve yorumlanacaktır. Veri setinde yer alan değişkenlerin frekans dağılım tablolarının hazırlanması, verilerin özetlenmesi bakımından önem taşımaktadır. Frekans tablosu; veri setinde yer alan bir

değişkenin kolay bilgi edinilebilir biçimde küçükten büyüğe doğru dizilerek tekrarlı ölçümlerin bir araya getirilmesi ve bu değerlere sahip birim sayılarının belirli bir düzende gösterilmesidir. Bu işleme frekans serisi adı da verilmektedir. Tablolaştırmada esas amaç n>30 biriminden oluşan veri setini özetlemek ve kolay bilgi elde edilir biçimde düzenlemektir. Grupları sıralı biçimde dizmek ve verilerin genel dağılım ve yayılım eğilimini tablodan sezmek amaçlanır (Şenol, 2008, s. 52-53).

# BÖLÜM 3

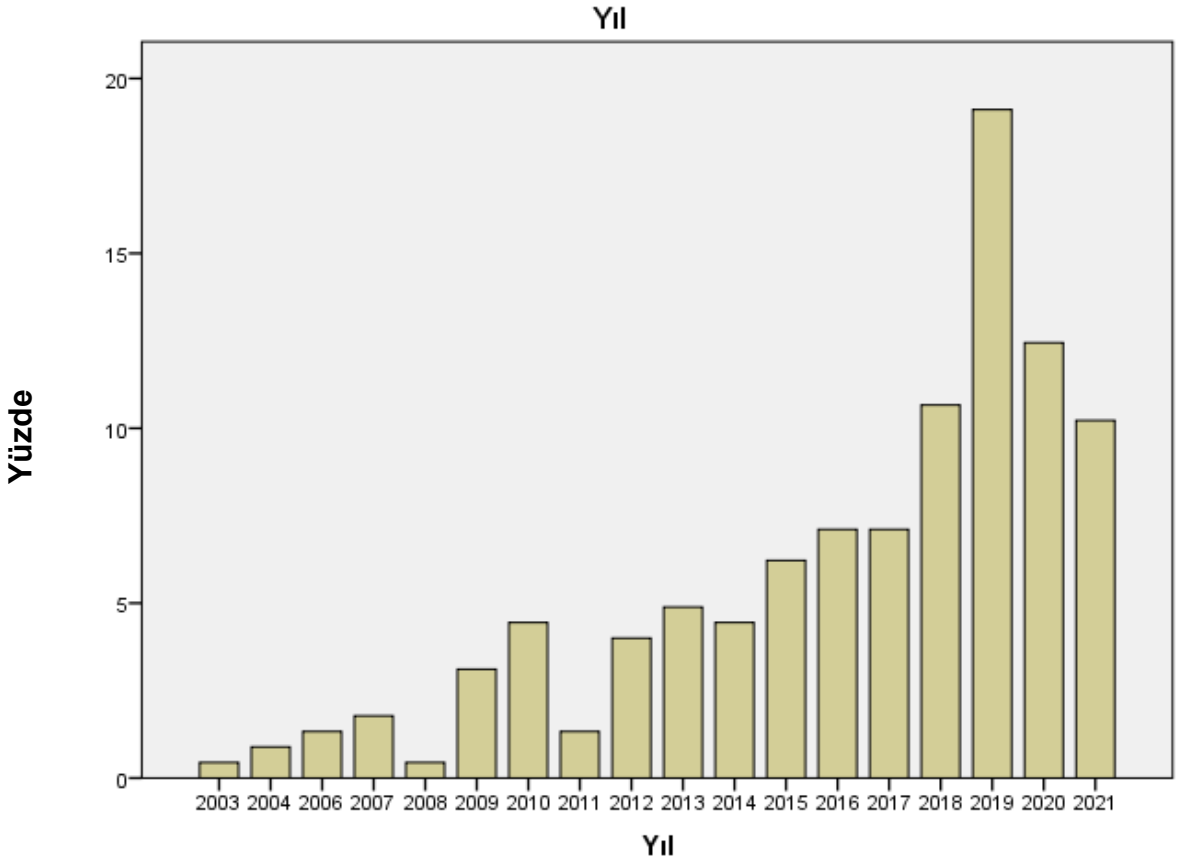
# 3. BULGULAR VE YORUMLAR

## 3.1. Tezlerin Yıllara Göre Dağılımı

Siber güvenlik alanındaki tezler yıllar bazında analiz edilmiştir. Elde edilen veriler Tablo 3.1'de yer almaktadır. Şekil 3.1'de ise tezlerin yıllara göre dağılımı çubuk grafikle gösterilmiştir.

Tablo 3.1. Tezlerin yıllara göre dağılımı

| Yıllar | N | % (Yüzde) |
|---|---|---|
| 2003 | 1 | 0,4 |
| 2004 | 2 | 0,9 |
| 2006 | 3 | 1,3 |
| 2007 | 4 | 1,8 |
| 2008 | 1 | 0,4 |
| 2009 | 7 | 3,1 |
| 2010 | 10 | 4,4 |
| 2011 | 3 | 1,3 |
| 2012 | 9 | 4,0 |
| 2013 | 11 | 4,9 |
| 2014 | 10 | 4,4 |
| 2015 | 14 | 6,2 |
| 2016 | 16 | 7,1 |
| 2017 | 16 | 7,1 |
| 2018 | 24 | 10,7 |
| 2019 | 43 | 19,1 |
| 2020 | 28 | 12,4 |
| 2021 | 23 | 10,2 |
| **Toplam** | **225** | **100** |




**Şekil 3.1. T**ezlerin yıllara göre dağılımı

Yayımlanan tezlerin sayılarına bakıldığında dalgalanmalar görülmektedir. En yüksek sayıda tez yayımlanan yıl 2019'dur. Tezlerin %19,1'i 2019 yılında yayımlanmıştır. En düşük sayıda tez yayımlanan yıllar 2003 ve 2008'dir. Tezlerin %0,4'ü bu yıllarda yayımlanmıştır. Yayımlanan toplam tez sayısı 225'dir.

## 3.2. Tezlerin Üniversitelere Göre Dağılımı

Siber güvenlik alanında yayımlanmış olunan toplam 225 tez 60 üniversite bünyesinde yazılmıştır. Siber güvenlik alanındaki tezler üniversiteler bazında analiz edilmiştir. Elde edilen veriler Tablo 3.2'de yer almaktadır. Şekil 3.2'de ise tezlerin yıllara göre dağılımı çubuk grafikle gösterilmiştir.

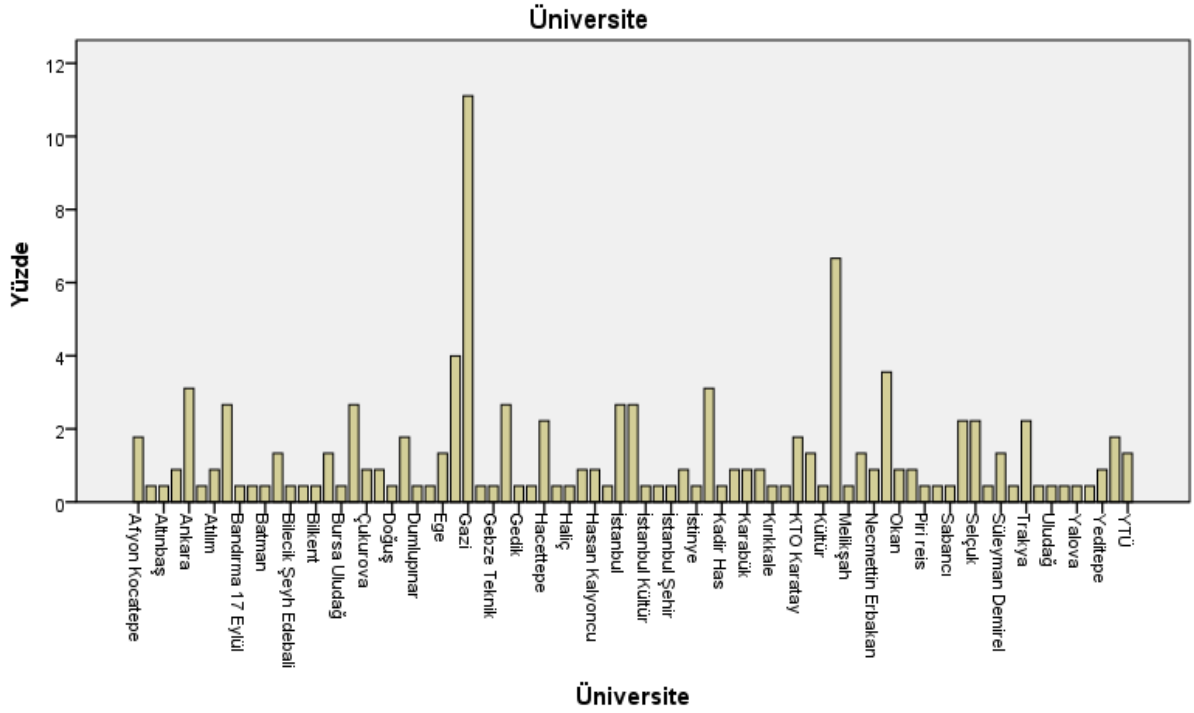
Tablo 3.2. Tezlerin üniversitelere göre dağılımı

| **Üniversiteler** | **N** | **% (Yüzde)** |
|---|---|---|
| Afyon Kocatepe | 4 | 1,8 |
| Ahi Evran | 1 | 0,4 |

| | | |
|---|---|---|
| Altınbaş | 1 | 0,4 |
| Anadolu | 2 | 0,9 |
| Ankara | 7 | 3,1 |
| Ankara Sosyal Bilimler | 1 | 7,1 |
| Atılım | 2 | 0,9 |
| Bahçeşehir | 6 | 2,7 |
| Bandırma 17 Eylül | 1 | 0,4 |
| Başkent | 1 | 0,4 |
| Batman | 1 | 0,4 |
| Beykent | 3 | 1,3 |
| Bilecik Şeyh Edebali | 1 | 0,4 |
| Bilgi | 1 | 0,4 |
| Bilkent | 1 | 0,4 |
| Boğaziçi | 3 | 1,3 |
| Bursa Uludağ | 1 | 0,4 |
| Çankaya | 6 | 2,7 |
| Çukurova | 2 | 0,9 |
| Dicle | 2 | 0,9 |
| Doğuş | 1 | 0,4 |
| Dokuz Eylül | 4 | 1,8 |
| Dumlupınar | 1 | 0,4 |
| Düzce | 1 | 0,4 |
| Ege | 3 | 1,3 |
| Fırat | 9 | 4,0 |
| Gazi | 25 | 11,1 |
| Gaziosmanpaşa | 1 | 0,4 |
| Gebze Teknik | 1 | 0,4 |
| Gebze YTE | 6 | 2,7 |

| | | |
|---|---|---|
| Gedik | 1 | 0,4 |
| Giresun | 1 | 0,4 |
| Hacettepe | 5 | 2,2 |
| Hacı Bayram Veli | 1 | 0,4 |
| Haliç | 1 | 0,4 |
| Harp Akademileri | 2 | 0,9 |
| Hasan Kalyoncu | 2 | 0,9 |
| İnönü | 1 | 0,4 |
| İstanbul | 6 | 2,7 |
| İstanbul Bilgi | 6 | 2,7 |
| İstanbul Kültür | 1 | 0,4 |
| İstanbul Okan | 1 | 0,4 |
| İstanbul Şehir | 1 | 0,4 |
| İstanbul Ticaret | 2 | 0,9 |
| İstinye | 1 | 0,4 |
| İTÜ | 7 | 3,1 |
| Kadir Has | 1 | 0,4 |
| Kara Harp Okulu | 2 | 0,9 |
| Karabük | 2 | 0,9 |
| Kayseri | 2 | 0,9 |
| Kırıkkale | 1 | 0,4 |
| Kocaeli | 1 | 0,4 |
| KTO Karatay | 4 | 1,8 |
| KTÜ | 3 | 1,3 |
| Kültür | 1 | 0,4 |
| Marmara | 15 | 6,7 |
| Melikşah | 1 | 0,4 |
| Mersin | 3 | 1,3 |

| | | |
|---|---|---|
| Necmettin Erbakan | 2 | 0,9 |
| ODTÜ | 8 | 3,6 |
| Okan | 2 | 0,9 |
| Ondokuz Mayıs | 2 | 0,9 |
| Piri reis | 1 | 0,4 |
| Polis Akademisi | 1 | 0,4 |
| Sabancı | 1 | 0,4 |
| Sakarya | 5 | 2,2 |
| Selçuk | 5 | 2,2 |
| Sıtkı Koçman | 1 | 0,4 |
| Süleyman Demirel | 3 | 1,3 |
| Sütçü İmam | 1 | 0,4 |
| Trakya | 5 | 2,2 |
| Ufuk | 1 | 0,4 |
| Uludağ | 1 | 0,4 |
| Université Paris Dauphine | 1 | 0,4 |
| Yalova | 1 | 0,4 |
| Yaşar | 1 | 0,4 |
| Yeditepe | 2 | 0,9 |
| Yıldırım Bayezıt | 4 | 1,8 |
| YTÜ | 3 | 1,3 |
| **Toplam** | **225** | **100,0** |




**Şekil 3.2.** Tezlerin üniversitelere göre dağılımı

Elde edilen sonuçlara göre en yüksek sayıda tez Gazi Üniversitesi bünyesinde yayımlanmıştır. 25 tez yayımlanmıştır ve tüm tezlerin yüzde 11,1'ini oluşturmaktadır. Tablo 3.3'de tezlerin ilk 3 üniversiteye göre dağılımı bulunmaktadır.

Tablo 3.3. Tezlerin ilk 3 üniversiteye göre dağılımı

| **Üniversiteler** | **N** | **% (Yüzde)** |
|---|---|---|
| Gazi | 25 | 11,1 |
| Marmara | 15 | 6,7 |
| Fırat | 8 | 4,0 |
| **Toplam** | **48** | **21,8** |

## 3.3. Tezlerin İllere Göre Dağılımı

Tezlerin illere göre dağılımı Tablo 3.4'de yer almaktadır. Tezlerin illere göre dağılımının çubuk grafikle gösterimi ise Şekil 3.3'de yer almaktadır. Tezlerin illere göre dağılımında ilk 3 üniversite ise tablo 3.5'de gösterilmiştir.

Tablo 3.4. Tezlerin illere göre dağılımı

| İl | N | % (Yüzde) |
|---|---|---|
| Adana | 2 | 0,9 |
| Afyon | 4 | 1,8 |
| Ankara | 68 | 30,2 |
| Balıkesir | 1 | 0,4 |
| Batman | 1 | 0,4 |
| Bilecik | 1 | 0,4 |
| Bursa | 2 | 0,9 |
| Diyarbakır | 2 | 0,9 |
| Edirne | 5 | 2,2 |
| Elâzığ | 9 | 4,0 |
| Eskişehir | 2 | 0,9 |
| Gaziantep | 2 | 0,9 |
| Giresun | 1 | 0,4 |
| Isparta | 3 | 1,3 |
| İstanbul | 69 | 30,7 |
| İzmir | 7 | 3,1 |
| İzmit | 7 | 3,1 |
| Kahramanmaraş | 1 | 0,4 |
| Karabük | 2 | 0,9 |
| Kayseri | 3 | 1,3 |
| Kırıkkale | 1 | 0,4 |
| Kırşehir | 1 | 0,4 |
| Kocaeli | 2 | 0,9 |
| Konya | 11 | 4,9 |
| Kütahya | 1 | 0,4 |
| Malatya | 1 | 0,4 |

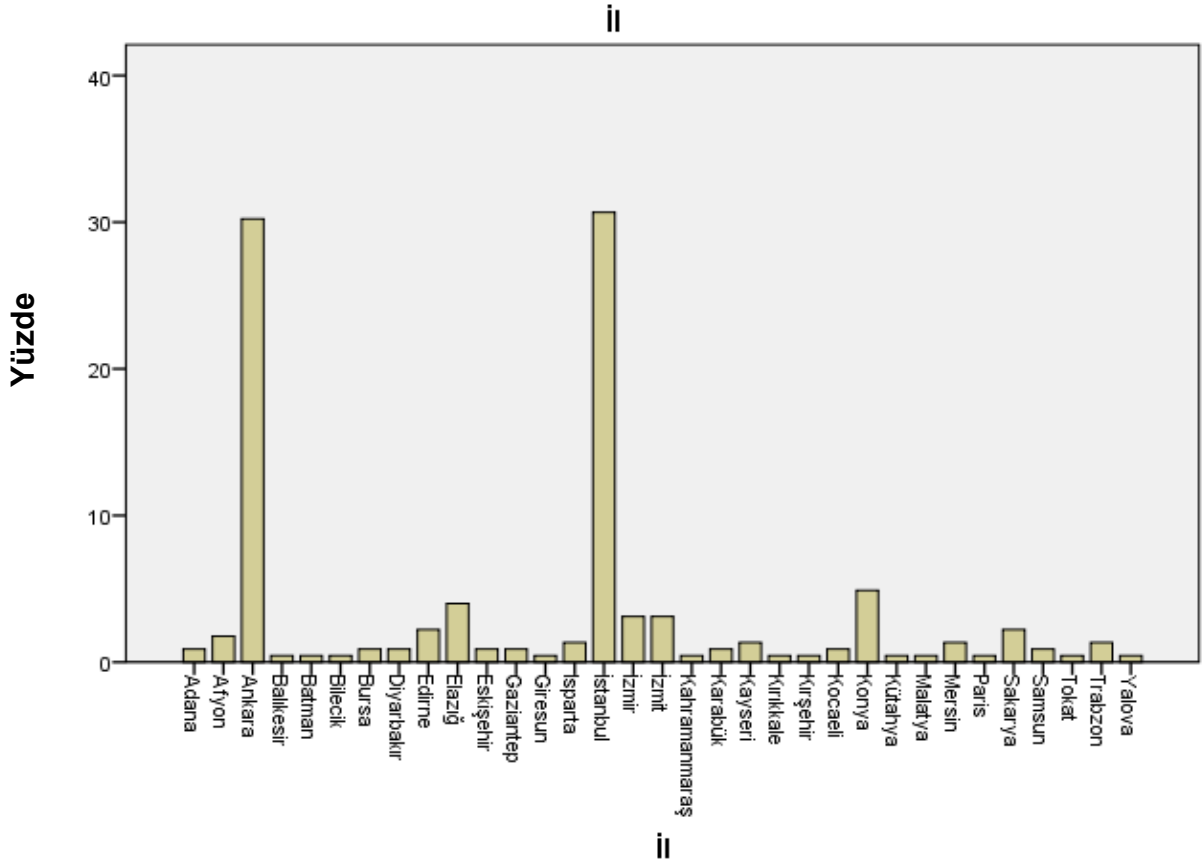
| | | |
|---|---|---|
| Mersin | 3 | 1,3 |
| Paris | 1 | 0,4 |
| Sakarya | 5 | 2,2 |
| Samsun | 2 | 0,9 |
| Tokat | 1 | 0,4 |
| Trabzon | 3 | 1,3 |
| Yalova | 1 | 0,4 |
| **Toplam** | **225** | **100** |

Tablo 3.5. Tezlerin ilk 3 ile göre dağılımı

| **İller** | **N** | **% (Yüzde)** |
|---|---|---|
| İstanbul | 69 | 30,7 |
| Ankara | 68 | 30,2 |
| Konya | 11 | 4,9 |
| **Toplam** | **148** | **65,8** |

Elde edilen bulgulara göre ilk sırada İstanbul yer almaktadır. İkinci sırada Ankara yer almaktadır ve sadece 1 tez farkla ikinci sırayı almıştır. Üçüncü sırada ise Konya yer almaktadır. Söz konusu 3 ilden çalışmaların toplamda %65,8'i yayımlanmıştır.

Genellikle tez çalışmalarında en fazla yayımlanan tez İstanbul'dan olmaktadır ve İstanbul tez sayısı açısından ilk sıradadır. Ankara'nın sadece 1 tez farkla ikinci sırada olması savunma sanayinin ağırlıklı olarak Ankara'da olmasından kaynaklandığı söylenebilir. Dolayısıyla savunma sanayinin etkisi olarak yorumlanabilir.




**Şekil 3.3. T**ezlerin illere göre dağılımı

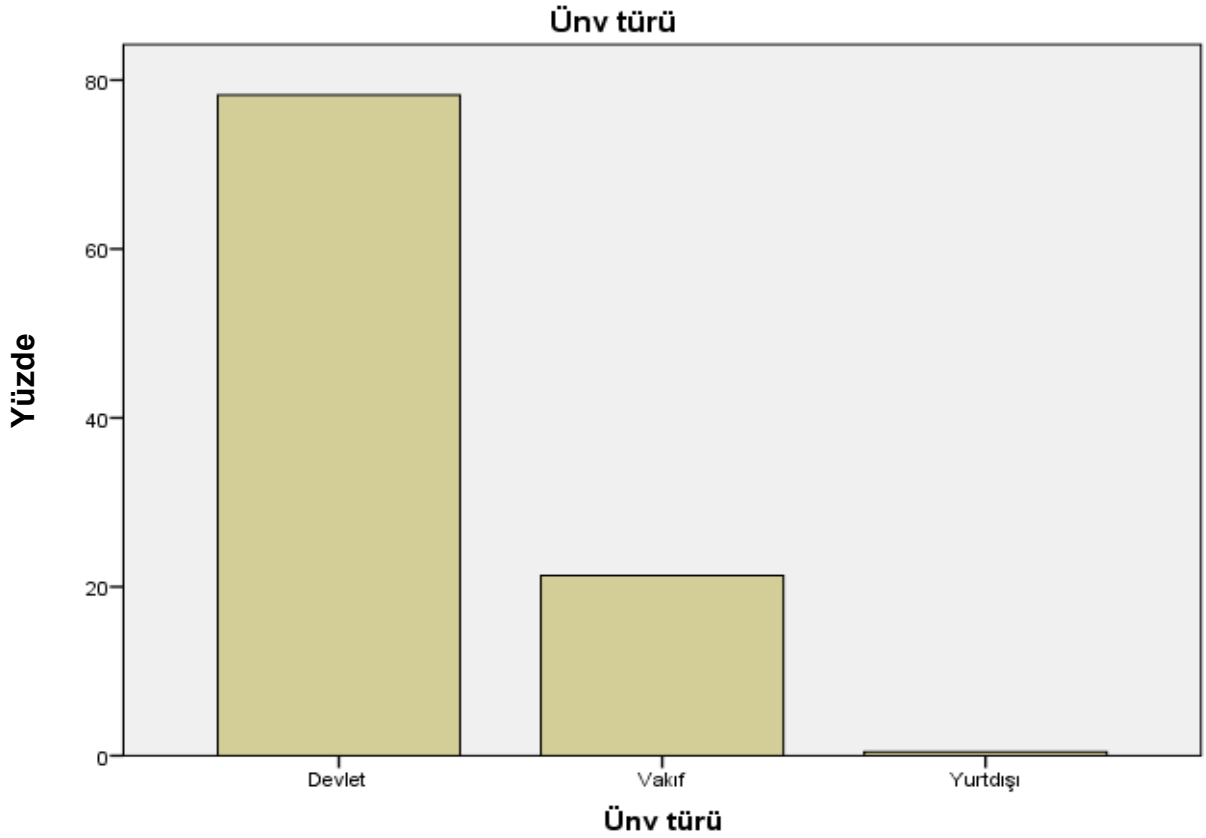
## 3.4. Tezlerin Üniversite Türlerine Göre Dağılımı

Tezlerin üniversite türleri devlet ve vakıf olmak üzere 3 kategoride toplanmıştır. Yurtdışı olarak belirtilen tez çalışması YÖK Ulusal Tez Merkezi veri tabanında yer almaktadır ve çalışma kapsamına dahil edilmiştir.

Tablo 3.6. Tezlerin üniversite türlerine göre dağılımı

| **Üniversite Türü** | **N** | **% (Yüzde)** |
|---|---|---|
| Devlet | 176 | 78,2 |
| Vakıf | 48 | 21,3 |
| Yurtdışı | 1 | 0,4 |
| **Toplam** | **225** | **100** |

Tablo 3.6'da tezlerin üniversite türlerine göre dağılımı yer almaktadır. Şekil 3.4'de ise Tezlerin üniversite türlerine göre dağılımı çubuk grafikle gösterilmiştir.




**Şekil 3.4. T**ezlerin üniversite türlerine göre dağılımı

Buna göre tezlerin %78,2'si devlet üniversiteleri bünyesinde yayımlanmıştır. Dolayısıyla siber güvenlik alanında devlet üniversitelerine kayıtlı öğrenciler tarafından daha fazla tez yazılmıştır.

## 3.5. Tezlerin Enstitülere Göre Dağılımı

Tezlerin enstitülere göre dağılımı tablo 3.7'de yer almaktadır. Tablo 3.8'de ise tezlerin ilk 3 enstitüye göre dağılımı gösterilmiştir. Şekil 3.5'de ise tezlerin enstitülere göre dağılımı çubuk grafikle gösterilmiştir.

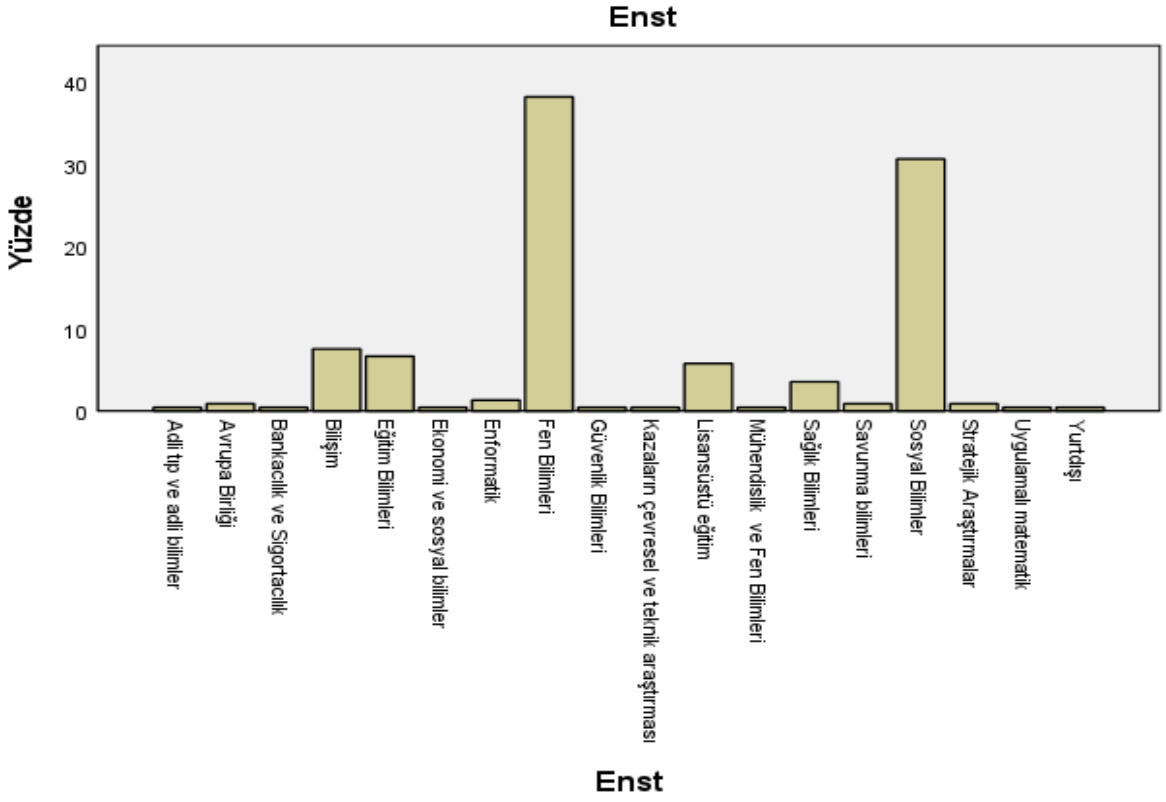
Tablo 3.7. Tezlerin enstitülere göre dağılımı

| Enstitü | N | % (Yüzde) |
|---|---|---|
| Adli tıp ve bilimler | 1 | 0,4 |
| Avrupa Birliği | 2 | 0,9 |
| Bankacılık ve Sigortacılık | 1 | 0,4 |
| Bilişim | 17 | 7,5 |

| | | |
|---|---|---|
| Eğitim Bilimleri | 16 | 6,7 |
| Ekonomi ve sosyal bilimler | 1 | 0,4 |
| Enformatik | 3 | 1,3 |
| Fen Bilimleri | 86 | 38,2 |
| Güvenlik Bilimleri | 1 | 0,4 |
| Kazaların çevresel ve teknik araştırması | 1 | 0,4 |
| Lisansüstü eğitim | 13 | 5,8 |
| Mühendislik ve Fen Bilimleri | 1 | 0,4 |
| Sağlık Bilimleri | 8 | 3,6 |
| Savunma Bilimleri | 2 | 0,9 |
| Sosyal Bilimler | 69 | 30,7 |
| Stratejik Araştırmalar | 2 | 0,9 |
| Uygulamalı matematik | 1 | 0,4 |
| Yurtdışı | 1 | 0,4 |
| **Toplam** | **225** | **100** |

Tablo 3.8. Tezlerin ilk 3 enstitüye göre dağılımı

| **Enstitü** | **N** | **% (Yüzde)** |
|---|---|---|
| Fen Bilimleri | 86 | 38,2 |
| Sosyal Bilimler | 69 | 30,7 |
| Bilişim | 17 | 7,5 |
| **Toplam** | **172** | **76,4** |




**Şekil 3.5. T**ezlerin enstitülere göre dağılımı

## 3.6. Tezlerin Anabilim Dallarına Göre Dağılımı

Tezlerin anabilim dallarına göre dağılımı tablo 3.9'da gösterilmiştir. Tezlerin ilk 3 anabilim dalına göre dağılımı tablo 3.10'da yer almaktadır. Şekil 3.6'da tezlerin anabilim dallarına göre dağılımı çubuk grafikle gösterilmiştir.

Tablo 3.9. Tezlerin anabilim dallarına göre dağılımı

| **Anabilim Dalları** | **N** | **% (Yüzde)** |
|---|---|---|
| Adli Bilişim | 5 | 2,2 |
| Adli tıp | 1 | 0,4 |
| Akıllı sistemler | 1 | 0,4 |
| Amme idaresi | 1 | 0,4 |
| Avrupa Birliği Hukuku | 1 | 0,4 |
| Avrupa Çalışmaları | 1 | 0,4 |
| Bilgi Güvenliği | 6 | 2,7 |

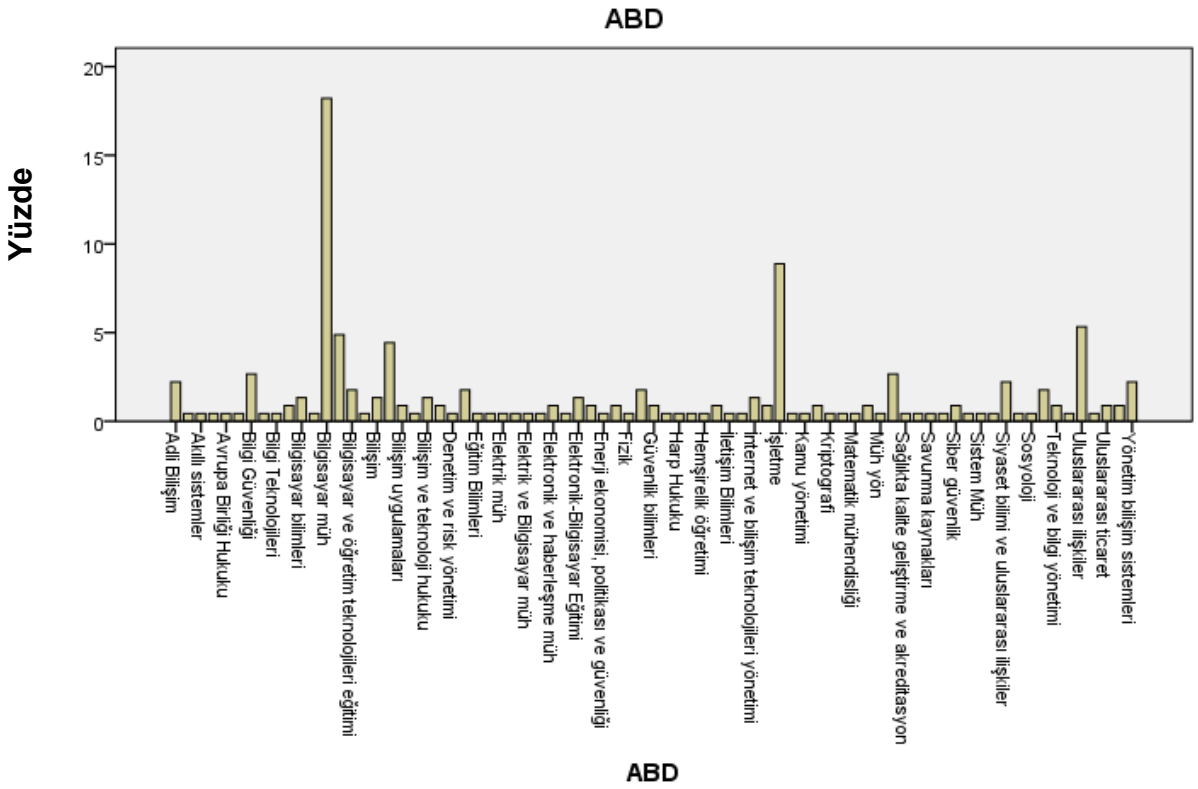
| | | |
|---|---|---|
| Bilgi Teknolojileri | 2 | 0,9 |
| Bilgi ve Belge Yönetimi | 2 | 0,9 |
| Bilgisayar Bilimleri | 4 | 1,7 |
| Bilgisayar Mühendisliği | 41 | 18,2 |
| Bilgisayar ve öğretim teknolojileri | 15 | 6,7 |
| Bilim ve teknoloji politikası çalışmaları | 1 | 0,4 |
| Bilişim | 3 | 1,3 |
| Bilişim Sistemleri | 10 | 4,4 |
| Bilişim Uygulamaları | 2 | 0,9 |
| Bilişim ve Teknoloji Hukuku | 4 | 1,7 |
| ÇEKO | 2 | 0,9 |
| Denetim ve Risk Yönetimi | 1 | 0,4 |
| Deniz Ulaştırma İşletme Mühendisliği | 4 | 1,8 |
| Eğitim Bilimleri | 1 | 0,4 |
| Eğitim Teknolojisi | 1 | 0,4 |
| Elektrik Mühendisliği | 1 | 0,4 |
| Elektrik ve Bilgisayar | 1 | 0,4 |
| Elektrik ve Bilgisayar Mühendisliği | 1 | 0,4 |
| Elektrik-Elektronik Mühendisliği | 1 | 0,4 |
| Elektronik ve Haberleşme Mühendisliği | 3 | 1,3 |
| Elektronik-Bilgisayar Eğitimi | 3 | 1,3 |
| Endüstri Mühendisliği | 2 | 0,9 |
| Enerji ekonomisi, politikası ve güvenliği | 1 | 0,4 |
| Enformatik | 2 | 0,9 |
| Fizik | 1 | 0,4 |
| Gazetecilik | 4 | 1,8 |
| Güvenlik Bilimleri | 2 | 0,9 |

| | | |
|---|---|---|
| Güvenlik stratejileri ve yönetimi | 1 | 0,4 |
| Harp Hukuku | 1 | 0,4 |
| Hastane İşletmeciliği | 1 | 0,4 |
| Hemşirelik Öğretimi | 1 | 0,4 |
| Hukuk | 2 | 0,9 |
| İletişim Bilimleri | 1 | 0,4 |
| İlköğretim Eğitimi | 1 | 0,4 |
| İnternet ve Bilişim Teknolojileri Yönetimi | 3 | 1,3 |
| İstatistik | 2 | 0,9 |
| İşletme | 20 | 8,9 |
| İşletme Bilgi Yönetimi | 1 | 0,4 |
| Kamu Yönetimi | 1 | 0,4 |
| Kazaların çevresel ve teknik araştırması | 2 | 0,9 |
| Kriptografi | 1 | 0,4 |
| Maliye ve Ekonomi | 1 | 0,4 |
| Matematik Mühendisliği | 1 | 0,4 |
| Matematik ve Bilgisayar | 2 | 0,9 |
| Mühendislik Yönetimi | 1 | 0,4 |
| Sağlık Yönetimi | 6 | 2,7 |
| Sağlıkta kalite geliştirme ve akreditasyon | 1 | 0,4 |
| Sağlıkta kalite yönetimi | 1 | 0,4 |
| Savunma kaynakları | 1 | 0,4 |
| Savunma teknolojileri | 1 | 0,4 |
| Siber güvenlik | 2 | 0,9 |
| Sigortacılık | 1 | 0,4 |
| Sistem Mühendisliği | 1 | 0,4 |
| Siyaset Bilimi ve Kamu Yönetimi | 1 | 0,4 |
| Siyaset Bilimi ve Uluslararası İlişkiler | 5 | 2,2 |

| | | |
|---|---|---|
| Siyaset ve Sosyal Bilimler | 1 | 0,4 |
| Sosyoloji | 1 | 0,4 |
| Strateji Bilimi | 4 | 1,8 |
| Teknoloji ve Bilgi Yönetimi | 2 | 0,9 |
| Toplam Kalite Yönetimi | 1 | 0,4 |
| Uluslararası İlişkiler | 13 | 5,7 |
| Uluslararası Ticaret | 2 | 0,9 |
| Yazılım Mühendisliği | 2 | 0,9 |
| Yönetim Bilişim Sistemleri | 5 | 2,2 |
| **Toplam** | **225** | **100** |

Tablo 3.10. Tezlerin ilk 3 anabilim dalına göre dağılımı

| **Anabilim Dalı** | **N** | **%(Yüzde)** |
|---|---|---|
| Bilgisayar Mühendisliği | 41 | 18,2 |
| İşletme | 20 | 8,9 |
| Bilgisayar ve Öğretim Teknolojileri | 15 | 6,7 |
| **Toplam** | **76** | **33,8** |




**Şekil 3.6.** Tezlerin anabilim dallarına göre dağılımı

## 3.7. Tezlerin Bilim Dallarına Göre Dağılımı

Tezlerin bilim dallarına göre dağılımı tablo 3.11'de gösterilmiştir. Tezlerin ilk 3 bilim dalına göre dağılımı tablo 3.12'de yer almaktadır. Şekil 3.7'de tezlerin bilim dallarına göre dağılımı çubuk grafikle gösterilmiştir.

Tablo 3.11. Tezlerin bilim dallarına göre dağılımı

| Anabilim Dalları | N | % (Yüzde) |
|---|---|---|
| Adli Bilişim | 5 | 2,2 |
| Adli tıp | 1 | 0,4 |
| Avrupa Birliği Hukuku | 1 | 0,4 |
| Avrupa Çalışmaları | 1 | 0,4 |
| Bilgi Güvenliği | 7 | 3,1 |
| Bilgi ve Belge Yönetimi | 7 | 3,1 |
| Bilgi ve haberleşme | 1 | 0,4 |
| Bilgisayar Bilimleri | 2 | 0,9 |

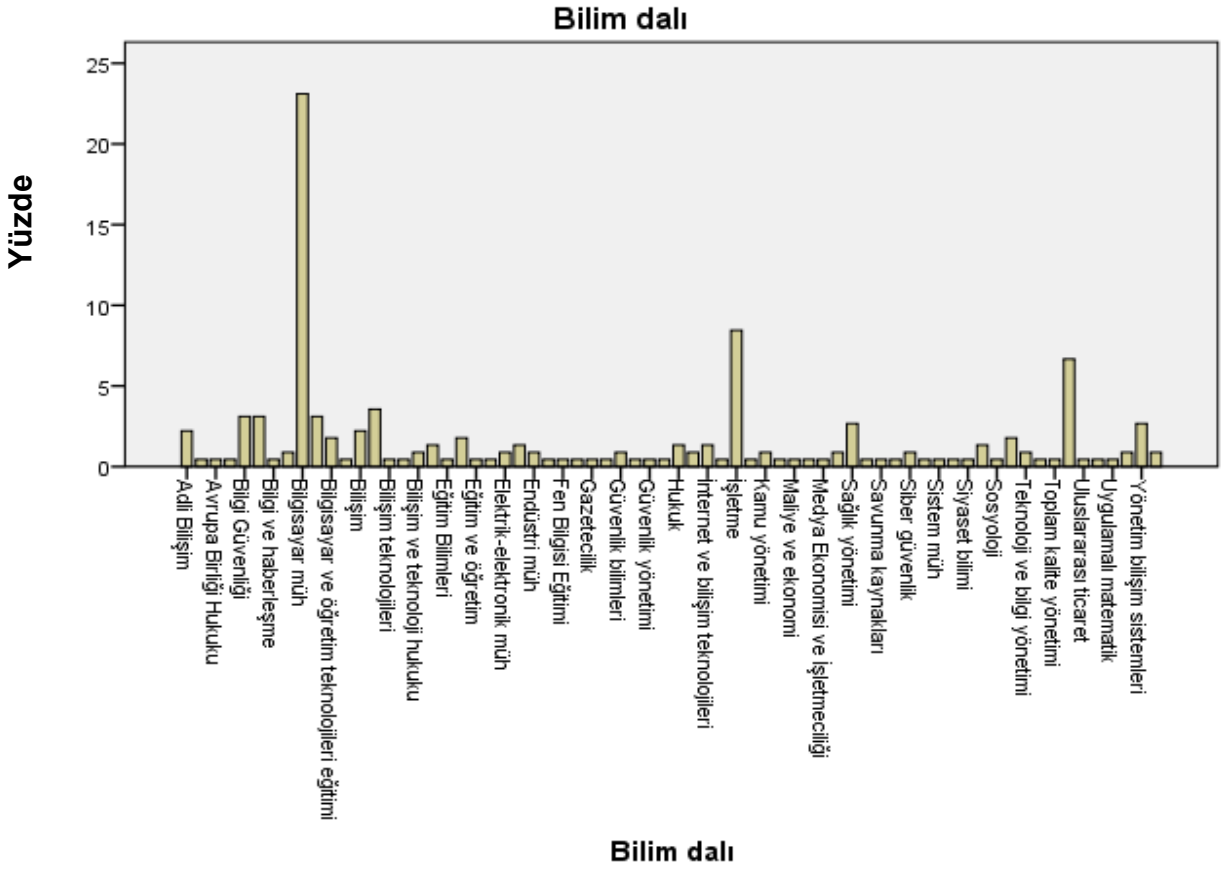
| | | |
|---|---|---|
| Bilgisayar Mühendisliği | 52 | 23,1 |
| Bilgisayar ve öğretim teknolojileri | 7 | 3,1 |
| Bilgisayar ve öğretim teknolojileri eğitimi | 4 | 1,8 |
| Bilim ve teknoloji politikası çalışmaları | 1 | 0,4 |
| Bilişim | 5 | 2,2 |
| Bilişim Sistemleri | 8 | 3,6 |
| Bilişim Teknolojileri | 1 | 0,4 |
| Bilişim Uygulamaları | 1 | 0,4 |
| Bilişim ve Teknoloji Hukuku | 2 | 0,9 |
| Deniz Ulaştırma İşletme Mühendisliği | 3 | 1,3 |
| Eğitim Bilimleri | 1 | 0,4 |
| Eğitim Teknolojisi | 4 | 1,8 |
| Eğitim ve öğretim | 1 | 0,4 |
| Elektrik Mühendisliği | 1 | 0,4 |
| Elektrik-Elektronik Mühendisliği | 2 | 0,9 |
| Elektronik-Bilgisayar Eğitimi | 3 | 1,3 |
| Endüstri Mühendisliği | 2 | 0,9 |
| Enformatik | 1 | 0,4 |
| Fen Bilgisi Eğitimi | 1 | 0,4 |
| Fizik | 1 | 0,4 |
| Gazetecilik | 1 | 0,4 |
| Gemi Mühendisliği | 1 | 0,4 |
| Güvenlik Bilimleri | 2 | 0,9 |
| Güvenlik stratejileri ve yönetimi | 1 | 0,4 |
| Güvenlik Yönetimi | 1 | 0,4 |
| Harp Hukuku | 1 | 0,4 |
| Hukuk | 3 | 1,3 |
| İnsan Kaynakları | 2 | 0,9 |

| | | |
|---|---|---|
| İnternet ve Bilişim Teknolojileri Yönetimi | 3 | 1,3 |
| İstatistik | 1 | 0,4 |
| İşletme | 19 | 8,4 |
| İşletme Bilgi Yönetimi | 1 | 0,4 |
| Kamu Yönetimi | 2 | 0,9 |
| Kazaların çevresel ve teknik araştırması | 1 | 0,4 |
| Maliye ve Ekonomi | 1 | 0,4 |
| Matematik Mühendisliği | 1 | 0,4 |
| Medya Ekonomisi ve İşletmeciliği | 1 | 0,4 |
| Mühendislik Bilimleri | 2 | 0,9 |
| Sağlık Yönetimi | 6 | 2,7 |
| Sağlıkta kalite yönetimi | 1 | 0,4 |
| Savunma kaynakları | 1 | 0,4 |
| Savunma teknolojileri | 1 | 0,4 |
| Siber güvenlik | 2 | 0,9 |
| Sigortacılık | 1 | 0,4 |
| Sistem Mühendisliği | 1 | 0,4 |
| Siyasal Bilimler | 1 | 0,4 |
| Siyaset Bilimi | 1 | 0,4 |
| Siyaset Bilimi ve Uluslararası İlişkiler | 3 | 1,3 |
| Sosyoloji | 1 | 0,4 |
| Strateji Bilimi | 4 | 1,8 |
| Teknoloji ve Bilgi Yönetimi | 2 | 0,9 |
| Telekomünikasyon Mühendisliği | 1 | 0,4 |
| Toplam Kalite Yönetimi | 1 | 0,4 |
| Uluslararası İlişkiler | 15 | 6,7 |
| Uluslararası Ticaret | 1 | 0,4 |
| Uluslararası Ticaret ve Pazarlama | 1 | 0,4 |

| | | |
|---|---|---|
| Uygulamalı Matematik | 1 | 0,4 |
| Yazılım Mühendisliği | 2 | 0,9 |
| Yönetim Bilişim Sistemleri | 6 | 2,7 |
| Yönetim ve Organizasyon | 2 | 0,9 |
| **Toplam** | **225** | **100** |

Tablo 3.12. Tezlerin ilk 3 bilim dalına göre dağılımı

| **Bilim Dalları** | **N** | **% (Yüzde)** |
|---|---|---|
| Bilgisayar Mühendisliği | 52 | 23,1 |
| İşletme | 19 | 8,4 |
| Uluslararası İlişkiler | 15 | 6,7 |
| **Toplam** | **86** | **38,2** |



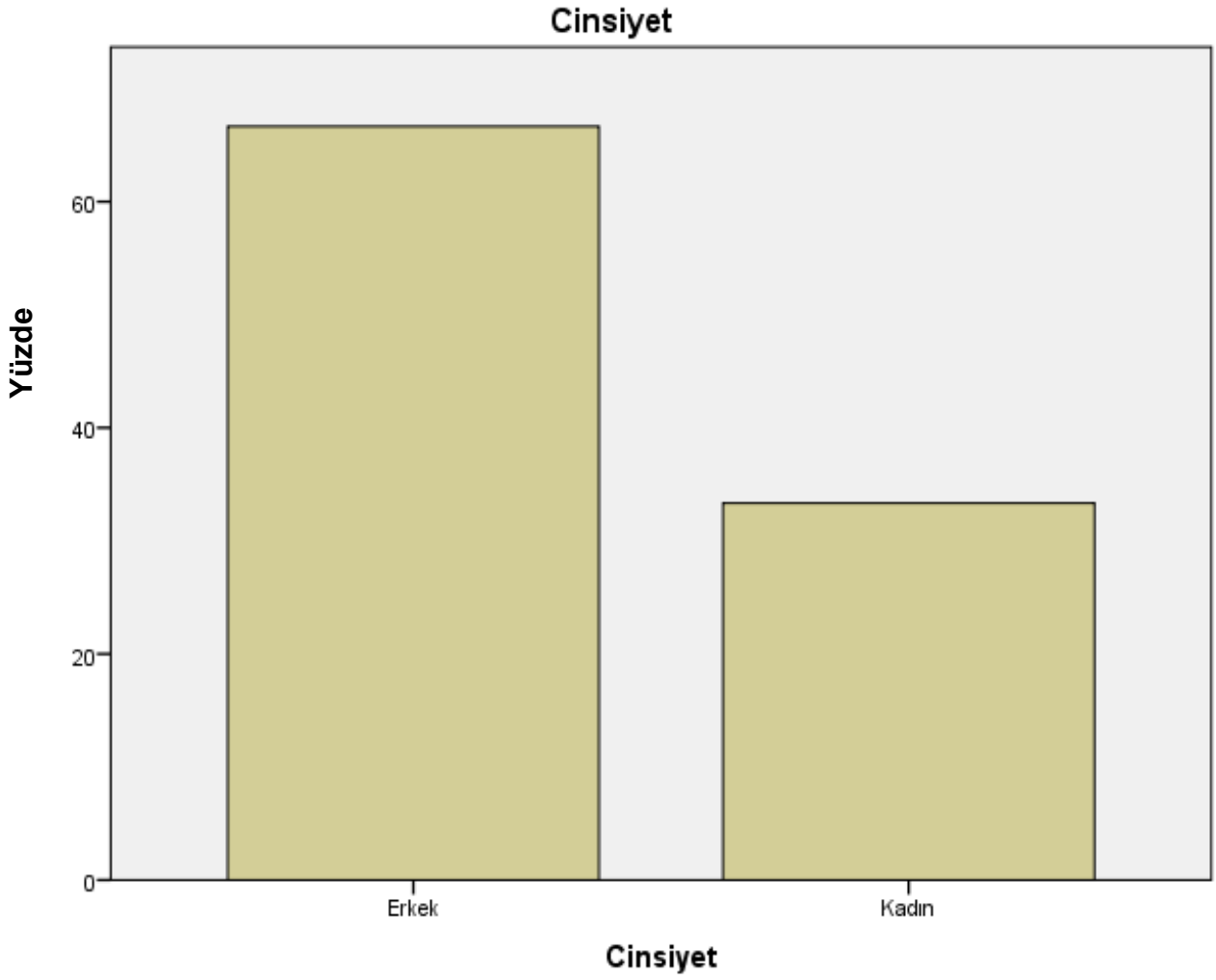

**Şekil 3.7.** Tezlerin bilim dallarına göre dağılımı

## 3.8. Tezlerin Cinsiyete Göre Dağılımı

Tezlerin cinsiyete göre dağılımı tablo 3.13'de gösterilmiştir. Şekil 3.8'de ise tezlerin cinsiyete göre dağılımı çubuk grafikle gösterilmiştir. Buna göre kadın öğrencilerin çalışmaları erkek öğrencilerin yarısı kadardır ve oldukça azdır.

Tablo 3.13. Tezlerin cinsiyete göre dağılımı

| **Cinsiyet** | **N** | **% (Yüzde)** |
|---|---|---|
| Kadın | 75 | 33,3 |
| Erkek | 150 | 66,7 |
| **Toplam** | **225** | **100** |



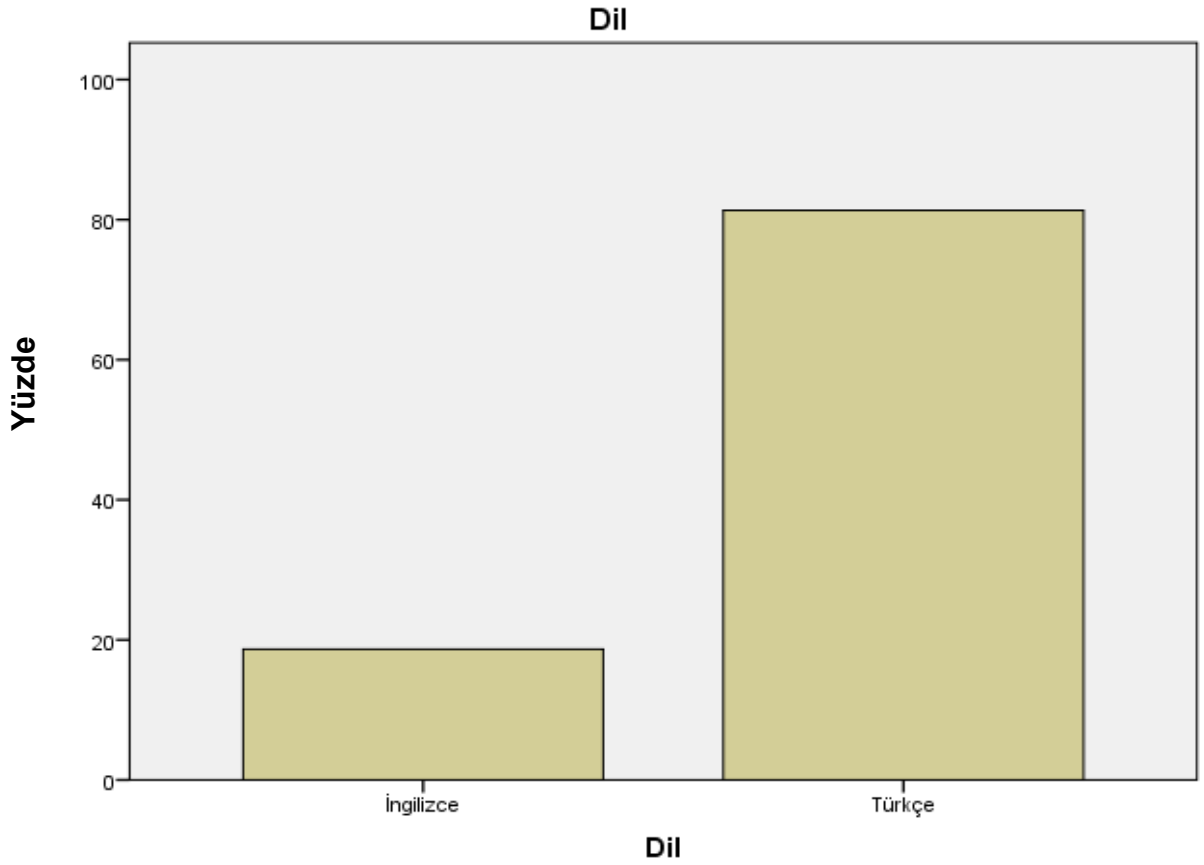

**Şekil 3.8.** Tezlerin cinsiyete göre dağılımı

## 3.9. Tezlerin Yazım Dillerine Göre Dağılımı

Tezlerin yazım dillerine göre dağılımı tablo 3.14'de gösterilmiştir. Şekil 3.9'da ise tezlerin yazım dillerine göre dağılımı çubuk grafikle gösterilmiştir. Buna göre tezlerin çoğunluğu Türkçe dilinde yazılmıştır.

Tablo 3.14. Tezlerin yazım dillerine göre dağılımı

| Cinsiyet | N | % (Yüzde) |
|---|---|---|
| İngilizce | 42 | 18,7 |
| Türkçe | 183 | 81,3 |
| **Toplam** | **225** | **100** |



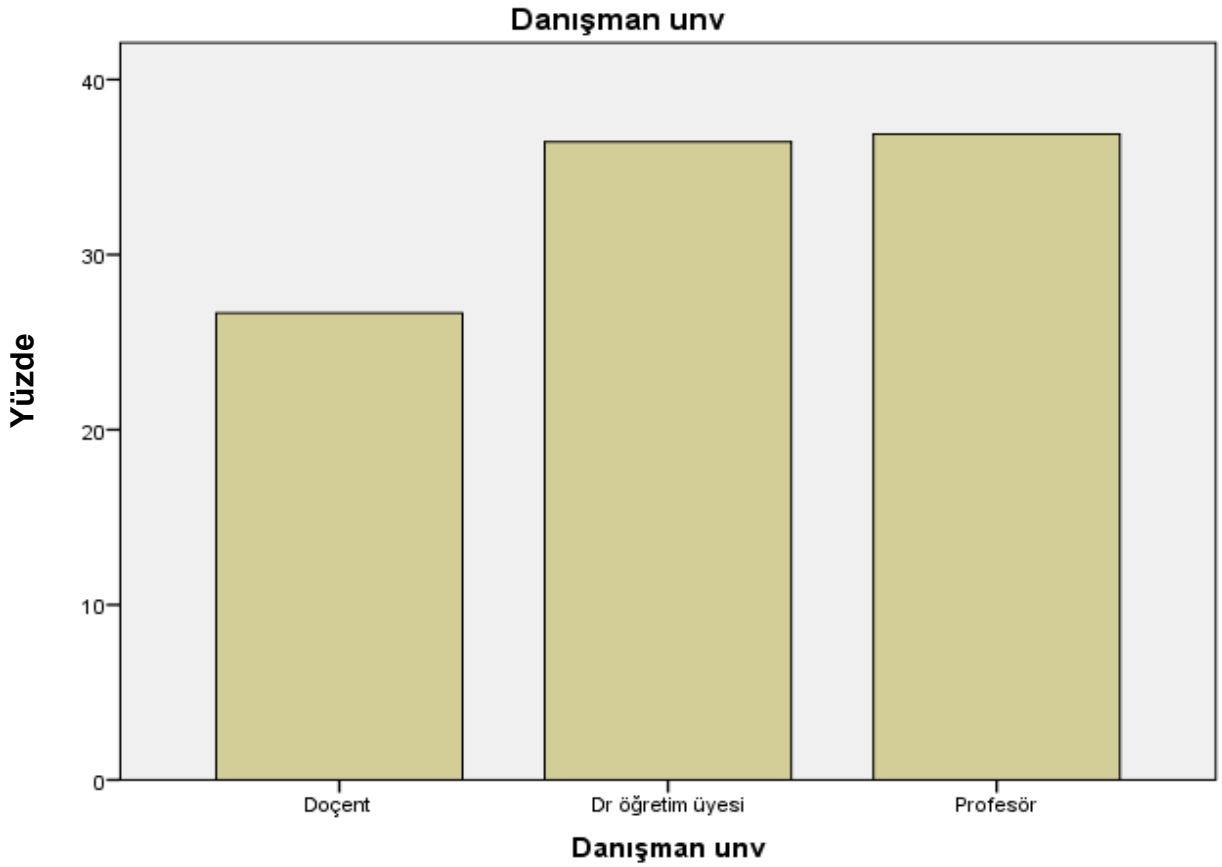

**Şekil 3.9.** Tezlerin yazım dillerine göre dağılımı

## 3.10. Tezlerin Danışman Unvanlarına Göre Dağılımı

Tezlerin danışman unvanlarına göre dağılımı Tablo 3.15'de gösterilmiştir. Şekil 3.10'da ise tezlerin danışman unvanlarına göre dağılımı çubuk grafikle gösterilmiştir.

Tablo 3.15. Tezlerin danışman unvanlarına göre dağılımı

| Danışman unvanı | N | %(Yüzde) |
|---|---|---|
| Doçent | 60 | 26,7 |
| Dr. öğretim üyesi | 82 | 36,4 |
| Profesör | 83 | 36,9 |
| **Toplam** | **225** | **100** |




**Şekil 3.10.** Tezlerin danışman unvanlarına göre dağılımı

Elde edilen sonuçlara göre doktor öğretim üyesi ve profesör unvanlarıyla görev yapmakta olan akademisyenler bu alanda en fazla tez danışmanı olarak yer alanlar olmuştur. Doçent unvanıyla görev yapmakta olan akademisyenler ise onların gerisinde kalmışlardır.

## 3.11. Tezlerin Sayfa Sayısına Göre Dağılımı

Tablo 3.16'da tezlerin sayfa sayısına göre dağılımı yer almaktadır. Şekil 3.11'de ise tezlerin sayfa sayısına göre dağılımı çubuk grafikle gösterilmiştir.

Elde edilen sonuçlara göre bu alandaki tez çalışmalarının sayfa sayısı en fazla 80 – 120 sayfa aralığındadır. Dolayısıyla çalışmaların genellikle 80-120 sayfa arasında olduğu sonucuna varılabilir.

Tablo 3.16. Tezlerin sayfa sayısına göre dağılımı

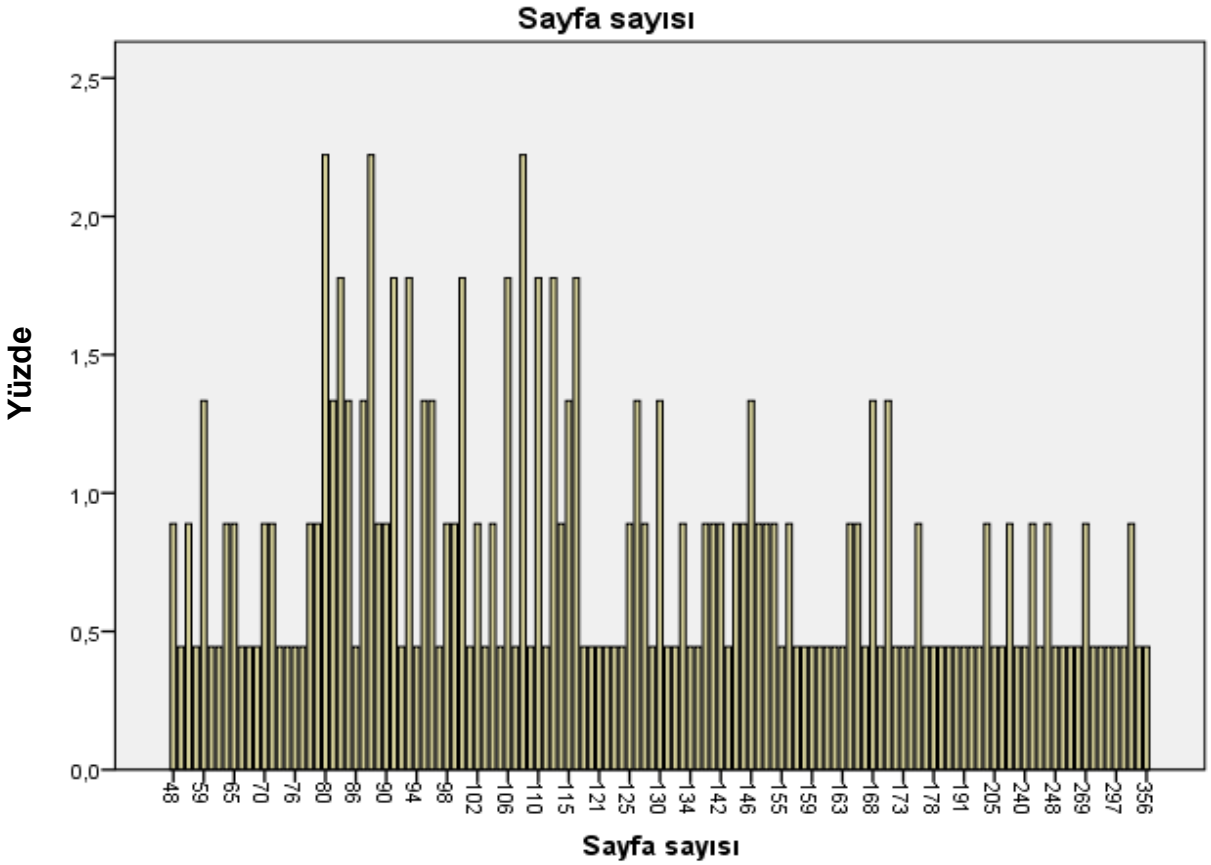
| **Sayfa sayısı** | **N** | **% (Yüzde)** |
|---|---|---|
| 48 | 2 | 0,9 |
| 52 | 1 | 0,4 |
| 56 | 2 | 0,9 |
| 57 | 1 | 0,4 |
| 59 | 3 | 1,3 |
| 60 | 1 | 0,4 |
| 62 | 1 | 0,4 |
| 64 | 2 | 0,9 |
| 65 | 2 | 0,9 |
| 67 | 1 | 0,4 |
| 68 | 1 | 0,4 |
| 69 | 1 | 0,4 |
| 70 | 2 | 0,9 |
| 71 | 2 | 0,9 |
| 73 | 1 | 0,4 |
| 75 | 1 | 0,4 |
| 76 | 1 | 0,4 |
| 77 | 1 | 0,4 |
| 78 | 2 | 0,9 |
| 79 | 2 | 0,9 |
| 80 | 5 | 2,2 |
| 82 | 3 | 1,3 |
| 84 | 4 | 1,8 |

| | | |
|---|---|---|
| 85 | 3 | 1,3 |
| 86 | 1 | 0,4 |
| 87 | 3 | 1,3 |
| 88 | 5 | 2,2 |
| 89 | 2 | 0,9 |
| 90 | 2 | 0,9 |
| 91 | 4 | 1,8 |
| 92 | 1 | 0,4 |
| 93 | 4 | 1,8 |
| 94 | 1 | 0,4 |
| 95 | 3 | 1,3 |
| 96 | 3 | 1,3 |
| 97 | 1 | 0,4 |
| 98 | 2 | 0,9 |
| 99 | 2 | 0,9 |
| 100 | 4 | 1,8 |
| 101 | 1 | 0,4 |
| 102 | 2 | 0,9 |
| 103 | 1 | 0,4 |
| 104 | 2 | 0,9 |
| 105 | 1 | 0,4 |
| 106 | 4 | 1,8 |
| 107 | 1 | 0,4 |
| 108 | 5 | 2,2 |
| 109 | 1 | 0,4 |
| 110 | 4 | 1,8 |
| 111 | 1 | 0,4 |
| 112 | 4 | 1,8 |

| | | |
|---|---|---|
| 113 | 2 | 0,9 |
| 115 | 3 | 1,3 |
| 117 | 4 | 1,8 |
| 118 | 1 | 0,4 |
| 119 | 1 | 0,4 |
| 121 | 1 | 0,4 |
| 122 | 1 | 0,4 |
| 123 | 1 | 0,4 |
| 124 | 1 | 0,4 |
| 125 | 2 | 0,9 |
| 126 | 3 | 1,3 |
| 128 | 2 | 0,9 |
| 129 | 1 | 0,4 |
| 130 | 3 | 1,3 |
| 131 | 1 | 0,4 |
| 132 | 1 | 0,4 |
| 133 | 2 | 0,9 |
| 134 | 1 | 0,4 |
| 136 | 1 | 0,4 |
| 137 | 2 | 0,9 |
| 139 | 2 | 0,9 |
| 142 | 2 | 0,9 |
| 143 | 1 | 0,4 |
| 144 | 2 | 0,9 |
| 145 | 2 | 0,9 |
| 146 | 3 | 1,3 |
| 148 | 2 | 0,9 |
| 152 | 2 | 0,9 |

| | | |
|---|---|---|
| 154 | 2 | 0,9 |
| 155 | 1 | 0,4 |
| 156 | 2 | 0,9 |
| 157 | 1 | 0,4 |
| 158 | 1 | 0,4 |
| 159 | 1 | 0,4 |
| 160 | 1 | 0,4 |
| 161 | 1 | 0,4 |
| 162 | 1 | 0,4 |
| 163 | 1 | 0,4 |
| 164 | 2 | 0,9 |
| 165 | 2 | 0,9 |
| 166 | 1 | 0,4 |
| 168 | 3 | 1,3 |
| 169 | 1 | 0,4 |
| 171 | 3 | 1,3 |
| 172 | 1 | 0,4 |
| 173 | 1 | 0,4 |
| 174 | 1 | 0,4 |
| 176 | 2 | 0,9 |
| 177 | 1 | 0,4 |
| 178 | 1 | 0,4 |
| 179 | 1 | 0,4 |
| 180 | 1 | 0,4 |
| 181 | 1 | 0,4 |
| 191 | 1 | 0,4 |
| 192 | 1 | 0,4 |
| 200 | 1 | 0,4 |

| | | |
|---|---|---|
| 202 | 2 | 0,9 |
| 205 | 1 | 0,4 |
| 214 | 1 | 0,4 |
| 218 | 2 | 0,9 |
| 228 | 1 | 0,4 |
| 240 | 1 | 0,4 |
| 241 | 2 | 0,9 |
| 246 | 1 | 0,4 |
| 247 | 2 | 0,9 |
| 248 | 1 | 0,4 |
| 251 | 1 | 0,4 |
| 265 | 1 | 0,4 |
| 268 | 1 | 0,4 |
| 269 | 2 | 0,9 |
| 271 | 1 | 0,4 |
| 276 | 1 | 0,4 |
| 290 | 1 | 0,4 |
| 297 | 1 | 0,4 |
| 340 | 1 | 0,4 |
| 345 | 2 | 0,9 |
| 355 | 1 | 0,4 |
| 356 | 1 | 0,4 |
| **Toplam** | **225** | **100** |




**Şekil 3.11.** Tezlerin sayfa sayısına göre dağılımı

## 3.12. Tezlerin Konulara Göre Dağılımı

Tablo 3.17'de tezlerin konulara göre dağılımı yer almaktadır. Şekil 3.12'de ise tezlerin konulara göre dağılımı çubuk grafikle gösterilmiştir. Tablo 3.18'de ise tezlerin ilk 3 konuya göre dağılımı yer almaktadır. Buna göre en fazla çalışma bilgisayar mühendisliği konusunda yapılmıştır, ardından işletme ve uluslararası ilişkiler gelmektedir.

Tablo 3.17. Tezlerin konulara göre dağılımı

| Konular | N | % (Yüzde) |
|---|---|---|
| Adli Bilişim | 4 | 1,8 |
| Adli tıp | 1 | 0,4 |
| Avrupa Birliği Hukuku | 1 | 0,4 |
| Bilgi Güvenliği | 6 | 2,7 |
| Bilgi ve Belge Yönetimi | 12 | 5,3 |
| Bilgisayar Mühendisliği | 55 | 24,4 |

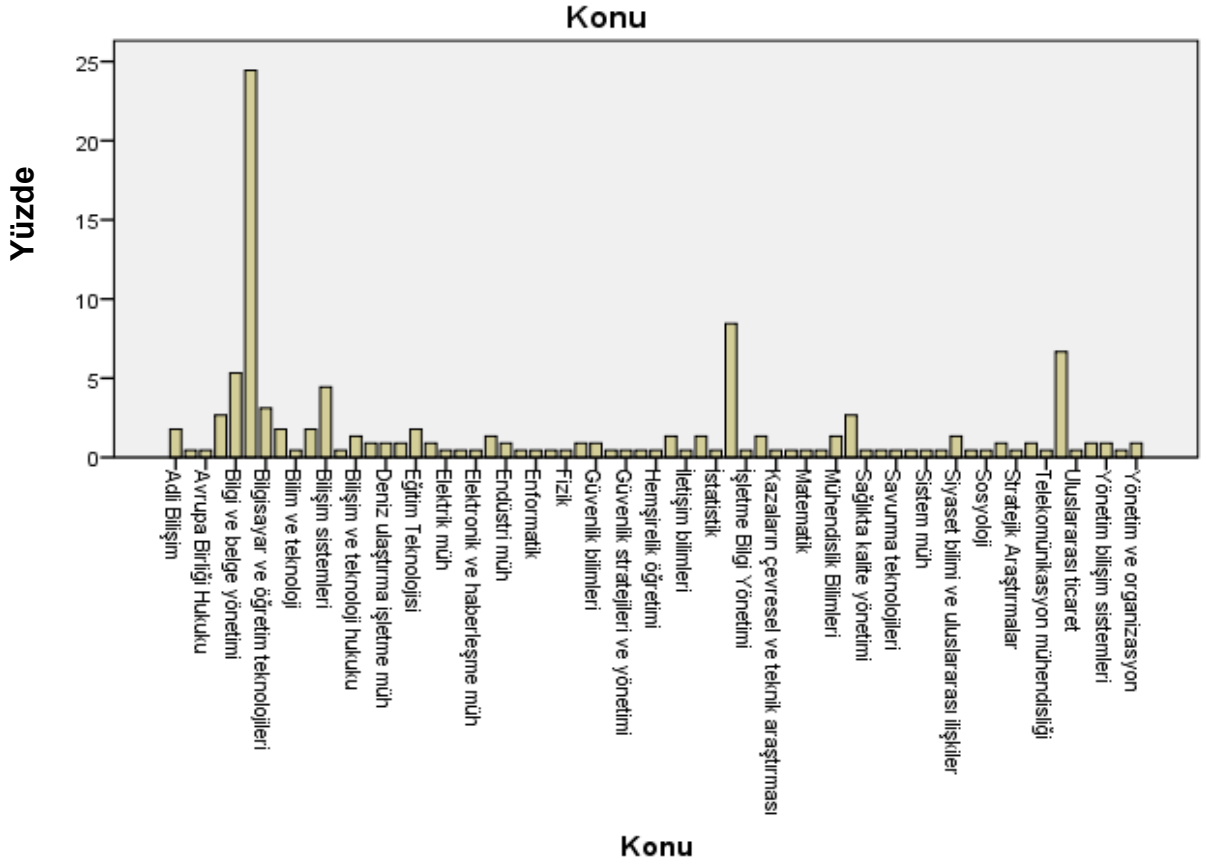
| | | |
|---|---|---|
| Bilgisayar ve Öğretim Teknolojileri | 7 | 3,1 |
| Bilgisayar ve Öğretim Teknolojileri Eğitimi | 4 | 1,8 |
| Bilim ve Teknoloji | 1 | 0,4 |
| Bilişim | 4 | 1,8 |
| Bilişim Sistemleri | 10 | 4,4 |
| Bilişim Uygulamaları | 1 | 0,4 |
| Bilişim ve Teknoloji Hukuku | 3 | 1,3 |
| ÇEKO | 2 | 0,9 |
| Deniz Ulaştırma İşletme Mühendisliği | 2 | 0,9 |
| Denizcilik | 2 | 0,9 |
| Eğitim Teknolojisi | 4 | 1,8 |
| Eğitim ve Öğretim | 2 | 0,9 |
| Elektrik Mühendisliği | 1 | 0,4 |
| Elektrik ve Elektronik Mühendisliği | 1 | 0,4 |
| Elektronik ve Haberleşme Mühendisliği | 1 | 0,4 |
| Elektronik-Bilgisayar Eğitimi | 3 | 1,3 |
| Endüstri Mühendisliği | 2 | 0,9 |
| Enerji | 1 | 0,4 |
| Enformatik | 1 | 0,4 |
| Fen Bilgisi Eğitimi | 1 | 0,4 |
| Fizik | 1 | 0,4 |
| Gazetecilik | 2 | 0,9 |
| Güvenlik Bilimleri | 2 | 0,9 |
| Güvenlik Politikaları | 1 | 0,4 |
| Güvenlik Stratejileri ve Yönetimi | 1 | 0,4 |
| Güvenlik Yönetimi | 1 | 0,4 |
| Hemşirelik Öğretimi | 1 | 0,4 |
| Hukuk | 3 | 1,3 |

| | | |
|---|---|---|
| İletişim Bilimleri | 1 | 0,4 |
| İnternet ve Bilişim Teknolojileri Yönetimi | 3 | 1,3 |
| İstatistik | 1 | 0,4 |
| İşletme | 19 | 8,4 |
| İşletme Bilgi Yönetimi | 1 | 0,4 |
| Kamu Yönetimi | 3 | 1,3 |
| Kazaların Çevresel ve Teknik Araştırması | 1 | 0,4 |
| Maliye ve Ekonomi | 1 | 0,4 |
| Matematik | 1 | 0,4 |
| Matematik Mühendisliği | 1 | 0,4 |
| Mühendislik Bilimleri | 3 | 1,3 |
| Sağlık Yönetimi | 6 | 2,7 |
| Sağlıkta Kalite Yönetimi | 1 | 0,4 |
| Savunma Kaynakları | 1 | 0,4 |
| Savunma Teknolojileri | 1 | 0,4 |
| Sigortacılık | 1 | 0,4 |
| Sistem Mühendisliği | 1 | 0,4 |
| Siyasal Bilimler | 1 | 0,4 |
| Siyaset Bilimi ve Uluslararası İlişkiler | 3 | 1,3 |
| Siyaset ve Sosyal Bilimler | 1 | 0,4 |
| Sosyoloji | 1 | 0,4 |
| Strateji Bilimi | 2 | 0,9 |
| Stratejik Araştırmalar | 1 | 0,4 |
| Teknoloji ve Bilgi Yönetimi | 2 | 0,9 |
| Telekomünikasyon Mühendisliği | 1 | 0,4 |
| Uluslararası İlişkiler | 15 | 6,7 |
| Uluslararası Ticaret | 1 | 0,4 |
| Yazılım Mühendisliği | 2 | 0,9 |

| | | |
|---|---|---|
| Yönetim Bilişim Sistemleri | 2 | 0,9 |
| Yönetim ve Bilişim Sistemleri | 1 | 0,4 |
| Yönetim ve Organizasyon | 2 | 0,9 |
| **Toplam** | **225** | **100** |

Tablo 3.18. Tezlerin ilk 3 konuya göre dağılımı

| **Konular** | **N** | **% (Yüzde)** |
|---|---|---|
| Bilgisayar Mühendisliği | 55 | 24,4 |
| İşletme | 19 | 8,4 |
| Uluslararası İlişkiler | 15 | 6,7 |
| **Toplam** | **89** | **39,5** |




**Şekil 3.12.** Tezlerin konulara göre dağılımı

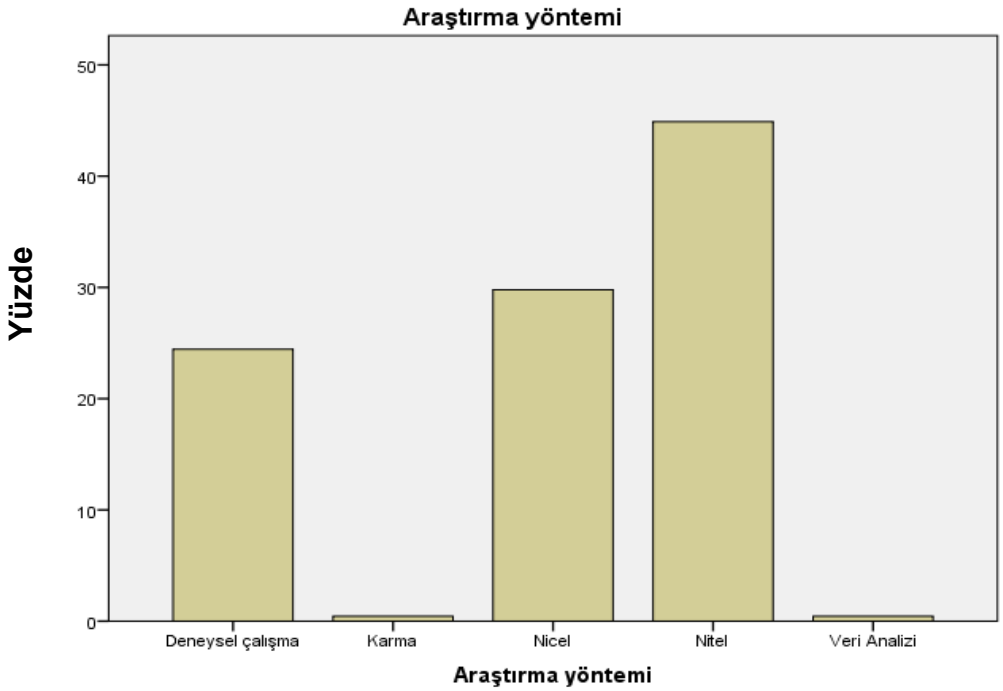
## 3.13. Tezlerin Araştırma Yöntemlerine Göre Dağılımı

Tablo 3.19'da tezlerin araştırma yöntemlerine göre dağılımı yer almaktadır. Şekil 3.13'de ise tezlerin araştırma yöntemlerine göre dağılımı çubuk grafikle gösterilmiştir.

Elde edilen sonuçlara göre çalışmaların çoğunluğu nitel araştırma yöntemi kullanılarak yazılmıştır. Bunun ardından nicel araştırma ve deneysel çalışma yöntemi gelmektedir. Deneysel çalışma kapsamında siber güvenlik alanında gerçekleştirilen sızma testleri, ilgili simülasyonlar ve uygulamalı çalışmalar yer almaktadır.

Tablo 3.19. Tezlerin araştırma yöntemlerine göre dağılımı

| **Araştırma yöntemi** | **N** | **% (Yüzde)** |
|---|---|---|
| Karma | 1 | 0,4 |
| Veri Analizi | 1 | 0,4 |
| Deneysel Çalışma | 55 | 24,4 |
| Nicel | 67 | 29,8 |
| Nitel | 101 | 44,9 |
| **Toplam** | **225** | **100** |



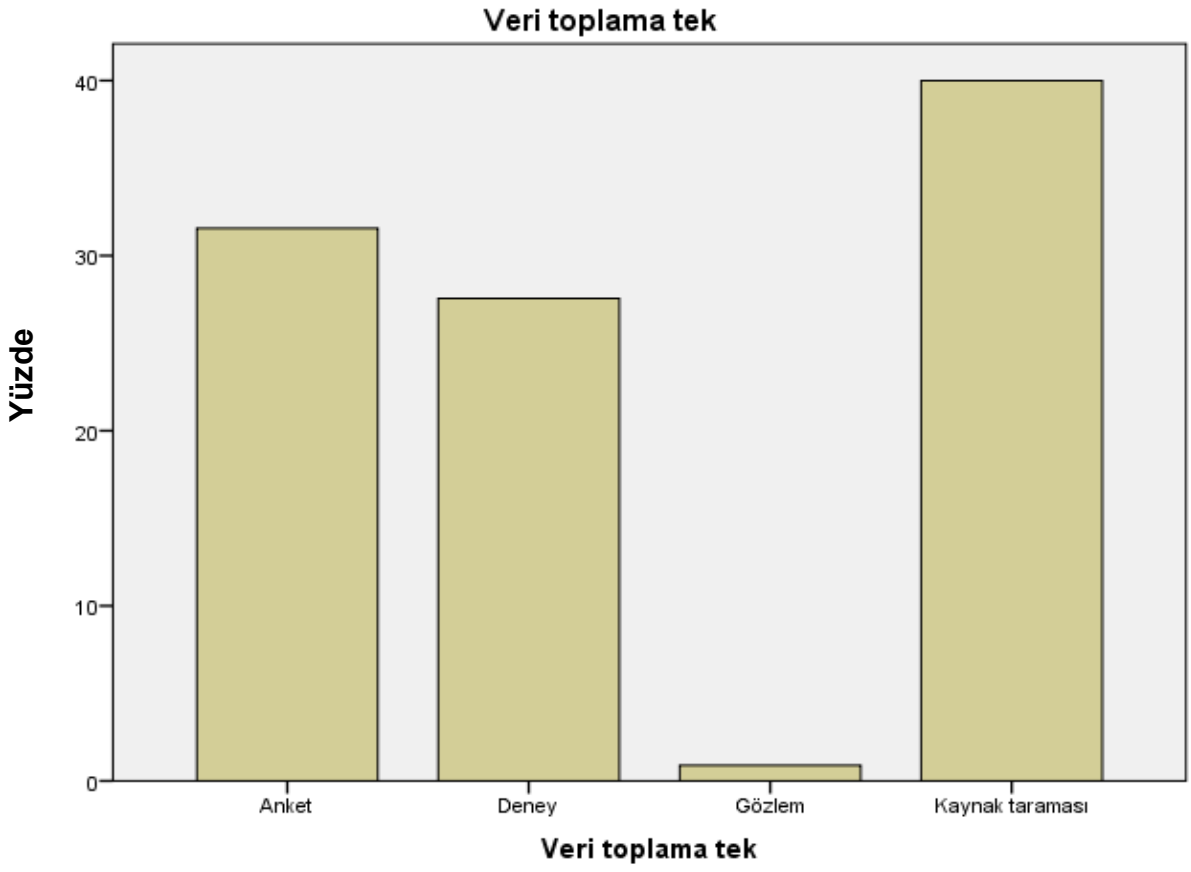

**Şekil 3.13.** Tezlerin araştırma yöntemlerine göre dağılımı

## 3.14. Tezlerin Veri Toplama Tekniklerine Göre Dağılımı

Tablo 3.20'de tezlerin veri toplama tekniklerine göre dağılımı yer almaktadır. Şekil 3.14'de ise tezlerin veri toplama tekniklerine göre dağılımı çubuk grafikle gösterilmiştir.

Tablo 3.20. Tezlerin veri toplama tekniklerine göre dağılımı

| Veri toplama tekniği | N | % (Yüzde) |
|---|---|---|
| Gözlem | 2 | 0,9 |
| Deney | 62 | 27,6 |
| Anket | 71 | 31,6 |
| Kaynak Taraması | 90 | 40,0 |
| **Toplam** | **225** | **100** |




**Şekil 3.14.** Tezlerin veri toplama tekniklerine göre dağılımı

Elde edilen sonuçlara göre siber güvenlik alanında yayımlanmış olunan tezlerin çoğunluğu kaynak taraması yöntemiyle veri toplanarak yazılmıştır. Bunun ardından anket yöntemi ve deney yöntemi yer almaktadır. En son sırada ise gözlem yöntemi yer alır.

# BÖLÜM 4

# 4. TARTIŞMA, SONUÇLAR VE ÖNERİLER

Bu bölümde, bir önceki bölümde açıklanan bulgulara dayalı olarak ulaşılan sonuçlar ve bu sonuçlar doğrultusunda geliştirilen öneriler yer almaktadır

## 4.1. Tartışma ve Sonuçlar

Geçmişten günümüze insanoğlu sürekli değişim içinde bulunmakta, farklılaşmakta ve değişim süreci içinde yeni nitelikler kazanmaktadır. Teknoloji bu değişimin yapı taşı olmuştur. Toplumsal değişim sürecinde teknoloji bulunduğu toplumdan bağımsız gelişmemiş aksine toplumsal yapının belirleyicisi olmuştur. Gelişen teknoloji ile kültürde bir dönüşüm yaşanmakta, teknolojinin toplumda oluşturduğu dönüşüm ile teknoloji kültürü şekillenmektedir. Hayatımızı kolaylaştıran ve vazgeçilmezi olan teknolojiyi reddetmek imkânsız olmuşken, reddeden kişiler de bir süre sonra kendilerini geride görmektedirler (Bayraktutan, 2004).

Günümüzde bilgi ve iletişim teknolojilerinde yaşanan gelişmeler sebebiyle günlük yaşam değişmektedir. Teknoloji günlük alışkanlıkları değiştirmeye başlamıştır. Bunun yanı sıra teknoloji hayatlarımızı kolaylaştırmaktadır. Ancak madalyonun öteki tarafında ise teknolojinin getirmiş olduğu riskler yer almaktadır. Dijital ortamlarda üretilen ve saklanan bilgide yaşanan artış sebebiyle bilgi güvenliğine ilişkin çeşitli tehdit ve riskler ortaya çıkmaktadır (Yılmaz, Şahin, & Akbulut, 2016).

İnternet eğitim-öğretim süreçlerinde aktif rol almaya başladıktan sonra bilgi sınıf ortamından çıkıp tüm dünyaya yayılmıştır. (Akkoyunlu, 2002). Eğitim ortamlarında aktarım ve iletişim teknolojilerinin kullanımının yaygınlaşması ve öğretmenlerin öğrenme ortamlarında kullandıkları teknolojik cihazlarının sayısındaki artış bilgi güvenliği konusundaki endişeleri arttırmaktadır. Teknolojide yaşanan gelişmeler öğretmenlerin teknoloji alanında kendilerini geliştirmelerini gerektirmektedir (Arslan & Şendurur, 2017).

Veri; araştırma ya da inceleme neticesinde elde edilen, işlenmemiş ve ham durumda olan bilgiler bütününe denir. Böylelikle farklı kullanıcılar tarafından üzerine yorum yapılır (Yıldız, 2006). Dijital veri ise internet ya da bilişim sistemleri aracılığıyla oluşturulmuş olunan bilgi paketleridir (Şengül, Atsan, & Bostan, 2014). Dijital veriler, çeşitli avantajlara sahiptirler. Veriyi üreten kişi tarafından uzaktan erişime açılmaları söz konusudur. Farklı formatlarda

kaydedilebilirler. Dijital verilerin avantajları sayesinde birçok uygulama ve hizmetler dijital platformlara taşınmaktadır (Schroeder, Steinmetz, Pereira, & Espindola, 2016).

Siber güvenlik bilişim dünyasının güvenliğini ifade eden bir kavram olarak karşımıza çıkar. Siber güvenlik, siber ortamda yer alan sistemlerin güvenliğini sağlamak amacıyla alınmış olunan tedbirler, faaliyetler ve bu amaçlarla belirlenmiş tüm standart, politika ve kurallar bütünüdür (Çiftçi, 2013). Burada güvenlik kavramı gizlilik, bütünlük ve erişilebilirliği kapsamaktadır. Teknolojinin hızlı ilerlemesi ile birlikte insanlar her geçen gün siber güvenlik açısından da çeşitli tehditlere maruz kalmaktadır. Siber suçlular geliştirdikleri yöntem ve tekniklerle kişisel verileri, banka hesapları ve hassas şirket verileri gibi bilgileri ele geçirmeyi hedeflemektedirler. Siber suçlar, bilişim sistemlerinin güvenlik açıklıklarını ve açıklıklara bağlı olarak kullanıcı verilerini hedef edinmiş suçlardır (EGM, 2022). Siber saldırılar "bilgisayar korsanlarının bilgisayar sistemini veya ağını yok etme, zarar verme veya fidye talep etme girişimleri" olarak tanımlanmaktadır. Tanımlamalar siber saldırı sayıları her geçen gün artıkça değişebilmektedir (Cengiz,2021).

Araştırma konusuyla ilgili kapsamlı bir bilimsel çalışma ortaya koyabilmek için araştırmacının ilk yapması gereken, araştırılacak konu ile ilgili alanyazında yapılmış bilimsel çalışmaları incelemektir. Araştırmacı kendisinden önce akademik hayata katkı sağlayan bilimsel çalışmaların ışığında, enerjisini verimli bir şekilde çalışmasına aktarabilecektir. Bundan dolayı, bibliyografik çalışmalar araştırmacılar için her zaman oldukça önemli bir işlevselliğe sahip olmuşlardır (Tığlı, 2021).

Bu çalışmada siber güvenliğe yönelik tezlerde yöntemsel açıdan ne tür çalışmaların yapıldığı incelenmeye çalışılmıştır. Bu bağlamda çalışma Türkiye'de siber güvenlik ile ilgili alanda herhangi bir çalışma yapmadan, ilgili literatürün durumunu ortaya koymak amacıyla yapılmıştır.

Bu amaç doğrultusunda Türkiye'de siber güvenlik alanında yapılan tezleri:

- Yıllara
- Üniversitelere
- Üniversitelerin illerine
- Üniversitelerin türüne
- İlgili enstitülere

- Anabilim dallarına
- Bilim dallarına
- Yazarlarının cinsiyetlerine
- Yazım dillerine
- Danışman unvanına
- Sayfa sayılarına
- Konularına
- Araştırma yöntemlerine
- Veri toplama teknikleri

Belirlenen değişkenler doğrultusunda incelenerek değerlendirme sonucuna ulaşılmıştır. Yayımlanan tezlerin sayılarına bakıldığında dalgalanmalar görülmektedir. En yüksek sayıda tez yayımlanan yıl 2019'dur. Tezlerin %19,1'i 2019 yılında yayımlanmıştır. En düşük sayıda tez yayımlanan yıllar 2003 ve 2008'dir. Tezlerin %0,4'ü bu yıllarda yayımlanmıştır. İncelenen toplam çalışma sayısı 225'dir. Çalışma sayılarına bakıldığında son yıllardaki artış doğru oranlı olarak teknoloji kullanım alanının son zamanlarda çok hızlı genişlemesi ve hayatın her alanında teknolojinin kullanılması ile beraberinde güvenlik risk ve sonuçlarını getirmesidir. Çalışma sonucunda gelecek yıllarda teknoloji kullanımının artması ile siber güvenlik, veri güvenliği ve bilgi güvenliği alanında yapılacak çalışmaların artış göstereceği öngörülmektedir.

Elde edilen sonuçlara göre en yüksek sayıda tez Gazi Üniversitesi bünyesinde yayımlanmıştır. 25 tez yayımlanmıştır ve tüm tezlerin yüzde 11,1'ini oluşturmaktadır. Elde edilen bulgulara göre ilk sırada İstanbul yer almaktadır. İkinci sırada Ankara yer almaktadır ve sadece 1 tez farkla ikinci sırayı almıştır. Üçüncü sırada ise Konya yer almaktadır. Söz konusu 3 ilden çalışmaların toplamda %65,8'i yayımlanmıştır. Yükseköğretim kurumlarının sayıca fazla olduğu illerde ve siber güvenlik alanında önde gelen üniversitelerde yapılan çalışmalar, doğru orantılı olarak yüksek çıkmıştır.

Genellikle tez çalışmalarında en fazla yayımlanan tez İstanbul'dan olmaktadır ve İstanbul tez sayısı açısından ilk sıradadır. Ankara'nın sadece 1 tez farkla ikinci sırada olması savunma sanayinin ağırlıklı olarak Ankara'da olmasından kaynaklandığı söylenebilir. Dolayısıyla savunma sanayinin etkisi olarak yorumlanabilir.

Tezlerin %78,2'si devlet üniversitelerinde yayımlanmıştır. Dolayısıyla siber güvenlik alanında devlet üniversitelerine kayıtlı öğrenciler tarafından daha fazla tez yazılmıştır. Yayımlanmış olunan tezlerin enstitülere göre dağılımı incelendiğinde en fazla çalışmanın fen bilimleri enstitüleri bünyesinde yapılmış olduğu görülmektedir. Ana bilim dalları ve bilim dallarına göre elde edilen sonuçlara göre en fazla bilgisayar mühendisliği anabilim dalında ve bilgisayar mühendisliği bilim dalında çalışma yapılmıştır.

Çalışmaların cinsiyete göre dağılımı sonuçlarına göre kadın öğrencilerin çalışmaları erkek öğrencilerin yarısı kadardır ve oldukça azdır. Tezlerin çoğunluğu Türkçe dilinde yazılmıştır. Doktor öğretim üyesi ve profesör unvanlarıyla görev yapmakta olan akademisyenler bu alanda en fazla tez danışmanı olarak yer alanlar olmuştur. Doçent unvanıyla görev yapmakta olan akademisyenler ise onların gerisinde kalmışlardır. Bu alandaki tez çalışmalarının sayfa sayısı en fazla 80-120 sayfa aralığındadır. Dolayısıyla çalışmaların genellikle 80-120 sayfa arasında olduğu sonucuna varılabilir. En fazla çalışma bilgisayar mühendisliği konusunda yapılmıştır, ardından işletme ve uluslararası ilişkiler gelmektedir.

Elde edilen sonuçlara göre çalışmaların çoğunluğu nitel araştırma yöntemi kullanılarak yazılmıştır. Bunun ardından nicel araştırma ve deneysel çalışma yöntemi gelmektedir. Deneysel çalışma kapsamında siber güvenlik alanında gerçekleştirilen sızma testleri, ilgili simülasyonlar ve uygulamalı çalışmalar yer almaktadır. Siber güvenlik alanında yayımlanmış olunan tezlerin çoğunluğu kaynak taraması yöntemiyle veri toplanarak yazılmıştır. Bunun ardından anket yöntemi ve deney yöntemi yer almaktadır. En son sırada ise gözlem yöntemi yer almıştır.

Bu çalışma Türkiye'de siber güvenlik ile ilgili alanda herhangi bir çalışma yapmadan, ilgili literatürün durumunu ortaya koymak amacıyla yapılmıştır. Geleceğe dönük çalışmalar için öneriler şu şekildedir;

1. Çalışmanın kapsamı daraltılarak belirli anabilim dalları için literatürün durumu hakkında daha detaylı analiz yapılabilir.
2. Bu çalışma yurt dışında gerçekleştirilen çalışmalar için gerçekleştirilebilir.
3. Bu çalışma uluslararası yayınlar ve Türkiye için karşılaştırmalı çalışma yapılabilir. Spesifik ülkeler ele alınabilir.
4. Çalışma kapsamında yer alan alanlar arasından az yayın yapılan konularda yayın yapılması literatüre katkı sağlayacaktır. Örneğin adli bilişim alanında yayın oldukça azdır.
5. Değişkenler farklılaştırılabilir.

Bu çalışma yüksek lisans ve doktora tezleri için gerçekleştirilerek karşılaştırma yapılabilir.

Bilgi teknolojileri kullanılmaya başlanıldığından bu yana toplumlar, şahıslar ve kültürlerde büyük etkiler bırakmıştır. İnsanlar yaşamları boyunca teknolojiyi her alanda kullanırken siber güvenliğin ve bilgi güvenliğinin ne kadar önemli olduğunu yaşanan kayıplar ile acı bir şekilde öğrenmektedirler. Çalışmada, siber güvenlik, bilgi güvenliği ve veri güvenliği alanında yapılmış lisans üstü akademik çalışmaların çeşitli değişkenler ile sonuçları belirlenmeye çalışılmıştır. Akademik çalışmalar değişkenler ile ele alındığında;

- Akademik çalışma sayılarının son yılarda artması, teknolojinin artan yoğunlukta kullanılması ile beraberinde bilgi hırsızlığı, yetkisiz erişim, fidye yazılımları ile işlenen suçlarının artması ve kimlik hırsızlığı vb. olayların sayılarındaki yükselmedir. Siber güvenliğe yönelik işlenen suçlar paralelinde güvenlik sistemlerinin önemini de getirmiştir. Akademik olarak elde edilen bulgular ve alan yazının taranması neticesinde alınması gereken önlemler konusunda hassas olmamız gerektiği sonucunu çıkarmaktadır. Yapılan çalışmada yıllara sari elde edilen bulgular incelendiğinde bilgisayar mühendisliği ve adli bilişim mühendisliği ana bilim dallarında son yıllardaki artışın diğer ana bilim dallarına göre hızlı olduğu görülmektedir. Bunun sebebinin, siber güvenlik ve bilgi güvenliği alanının ve alt uzmanlıklarına yönelik bölümlerin üniversitelerde oluşması olarak değerlendirilebilir.

- Yapılan çalışmalar enstitüler bakımından incelendiğinde, sosyal bilimlerde enstitülerindeki sayıca artışın nedeninin kamu yönetimi, uluslararası ilişkiler, bilişim yönetim sistemleri, bilişim sistemleri ve hukuk bölümlerinin yer alması olarak değerlendirilebilir.

- Yine çalışma sayılarına göre üniversiteler ele alındığında sıralamanın Gazi Üniversitesi, Marmara Üniversitesi ve Fırat Üniversitesi olduğu görülmüştür. Fırat Üniversitesinin üçüncü sırada yer alması Adli Bilişim Mühendisliği bölümün var olması ile açıklanabilir. Adli bilişim, içerdiği konular gereği bilişim güvenliği, bilişim suçları, yetkisiz erişim, zararlı yazılım ve kripto analiz gibi siber güvenliği içeren konulardan oluşması oluşmaktadır. Sanal gerçeklik ve Web 3.0 kavramlarının yoğun gündem olduğu günümüzde siber güvenlik, bilgi güvenliği ve veri güvenliği temel çizgileri oluşturmaktadır.

- Çalışmaların yapıldığı iller incelendiğinde sırasıyla, İstanbul, Ankara ve Konya gelmektedir. İl nüfus sayıları ve gelişmişlik düzeyleri ele alındığında üçüncü sırada İzmir ilinin olması beklenirken, Konya ilindeki üniversitelerde, bilişim bölümlerinin mazisinin geçmiş yıllara dayanması bu sıralamadaki etmen olduğu düşünülmektedir.

- Siber güvenlik, bilgi güvenliği ve veri güvenliği alanında yapılmış akademik çalışmalar incelendiğinde, bilişim teknolojileri bölümlerinin yanı sıra birçok alanda bu kavramlar üzerine çalışma yapıldığı görülmüştür. Bunun temel sebebinin teknolojinin hayatın her alanında var olması ve beraberinde bu risk kavramlarını getirmesidir. İlerleyen süreçlerde birçok alanın bu konular üzerine kendilerine yönelik olan kısımlarda akademik çalışmaların artarak yapılacağı öngörülmektedir.

Eğitim alanında teknoloji kullanımının her geçen gün tüm disiplinlerde artarak ilerlemesi beraberinde teknolojinin yanlış kullanımını veya yanlış kişilerce farklı amaçlar için kullanılma riskini de taşımaktadır. Bu bağlamda eğitim ve öğretim alanında teknolojinin sağlıklı ve verimli kullanılması için çeşitli anabilim dallarında çalışmalar yapılmaktadır. Eğitim ve öğretim sürecinde öğretmenlere siber güvenlik farkındalığının artırılması adına büyük görevler düşmektedir. Öncelikle öğretmenlerin siber güvenlik farkındalık düzeylerinin yüksek olması beklenmektedir. İmren'in (2021) çalışmasında öğretmenlerin siber güvenlik farkındalığının artırılması için vermiş oldukları cevaplarda; kişisel verilerin korunmasına yönelik yasal yaptırımların artırılması, kişisel verilerin yer aldığı teknoloji araçlarının daha güvenli hale getirilmesi, üniversiteler ve halk eğitim kurları gibi eğitim ortamlarında siber güvenlik eğitimlerinin verilmesi önerileri belirtilmiştir. Özbek'in (2019) çalışmasında, öğretmen adaylarının kişisel siber güvenlik farkındalıkları orta düzeyde bulunmuş ve erkek adayların farkındalık düzeyi kadın öğretmen adaylarından daha yüksek çıkmıştır. Solmaz'ın (2020) çalışmasında ise eğitim fakültelerinde eğitim gören öğretmen adaylarının siber bilgi güvenliği farkındalıkları ortalamanın üstünde bulunmuştur. Hedef düzeye uygun seminerler, yaşanılabilecek sorunlara yönelik alınması gereken önlemler konusunda simülasyon ortamları ve eğitimler ile bilinçlendirme sağlanmalıdır.

Öğretmenlerin bilgi güvenliği farkındalığı kadar öğrencilerin de farkındalıkları önem arz etmektedir. Özellikle lise düzeyinde teknoloji kullanımının daha yaygın olması, telefon, bilgisayar, tablet veya internet erişiminin olduğu herhangi bir cihazdan internete çıkabilen

öğrenciler siber tehdit, saldırı ve zorbalığa maruz kalabilmektedir. Dönmez'in (2019) çalışmasında, lise öğrencilerinin bilgi güvenliği farkındalıklarının iyi durumda olduğu bulunmuştur.

Hacımustafaoğlu'nun (2019) çalışmasında orta öğretim düzeyindeki öğrencilerin bilgi güvenliği farkındalık düzeyleri yüksek, internet kullanım sürelerine bağlı olarak siber mağduriyete maruz kalma düzeyleri düşük olarak bulunmuştur.

Gelişen teknoloji ile birlikte interaktif ve çevrimiçi eğitim ortamları hızla yaygınlaşmakta ve siber güvenlik konulu birçok eğitime internet ortamında erişilebilmektedir. Bu ortamların her geçen gün sayısının artması farkındalığı artırmakla beraber tasarım ilkelerine uygun olmayan içeriklerin oluşmasına da neden olmuştur. Tasarım ilkelerine uygun olmayan eğitimlerde verimliliği düşürmektedir. Güneş'in (2020) çalışmasında çevrimiçi ders platformlarından Udemy'de bulunan siber güvenlik eğitimleri incelenmiş, siber güvenlik eğitimlerinin çeşitli ilkelere uygun olarak hazırlanmadığı ve eksiklikler sonucuna varılmıştır.

Siber güvenlik, bilgi güvenliği ve veri güvenliği farkındalığının oluşmasında eğitim öğretim ortamlarının fiziksel durumları, yaşanılan bölge, öğrencilerin cinsiyeti ve öğretim kademelerine göre farklılık göstermektedir. Nitekim Yerlikaya'nın (2019) çalışmasında, özel okulda öğrenim gören öğrencilerin devlet okullarında öğrenim gören öğrencilere göre bilgi güvenliği farkındalık düzeylerinin daha yüksek olduğu sonucuna ulaşmıştır. Yine bilgi güvenliği farkındalığı cinsiyete göre incelendiğinde erkek öğrencilerin farkındalık düzeyleri daha yüksek çıkmıştır.

Siber güvenlik farkındalığına internet kullanım süresi önemli ölçüde etki etmektedir. İnternette geçirilen süre arttıkça yaşanılan tecrübeler ile farkındalık düzeyleri de artmaktadır. Kapanoğlu'nun (2016) çalışmasında, öğretmenlerin internet kullanım süreleri bilgi güvenliği farkındalığına anlamlı olarak etki ettiği bulunmuştur.

Bilgisayar ve öğretim teknolojileri anabilim dalında siber güvenlik, bilgi güvenliği ve veri güvenliği konularında çeşitli çalışmalar yapılmakta olup, farklı fakülte ve enstitülerdeki bilgisayar öğretmenliği öğretmen adayları ve öğretmenlerinin farkındalığı artmaktadır. Bilgisayar öğretmenlerinin siber güvenlik farkındalığının oluşması bu konularda alınacak önlemler, verilecek eğitim ve yetiştirilecek nesil açısından önem arz etmektedir. Bilgisayar ve öğretim teknolojileri bölümünün ders müfredatı içeriği siber güvenlik, bilgi güvenliği ve veri

güvenliği konularını içerdiğinden bu alanda yazılmış tez sayısı çalışmada analiz edilen tezlerin önemli bir kısmını oluşturmaktadır.

Çalışmada bilgisayar ve öğretim teknolojileri anabilim dalında 15 adet tez ele alınmıştır. Bu sayı incelenen 225 adet tezin %6,7'sini oluşturmaktadır. Eğitim bilimleri enstitüsü bilgisayar ve öğretim teknolojileri bilim dalında ise çalışmaya konu 8 adet tez incelenmiştir. Tüm çalışmanın %3,6'sını oluşturmaktadır. Tezlerin 2016 yılı ve sonrasında hazırlandığı, tamamında veri toplama yöntemi olarak anket kullanıldığı ve araştırmalarının %75'i nicel %25'i ise nitel yöntemler kullanılarak hazırlandığı verileri elde edilmiştir.

Bilgisayar ve öğretim teknolojileri bilim dalında çalışmaya konu siber güvenlik konulu tezlerin cinsiyete göre dağılımında %75'i kadın %25'i erkek öğrenciler tarafından hazırlandığı ortaya çıkmıştır. Çalışmanın geneline bakıldığın ise 225 adet çalışmanın cinsiyet dağılımında %33,3 kadın %66,7 erkek öğrenciler tarafından hazırlandığı elde edilmiştir. Bu sonuçlar gösteriyor ki eğitim bilimleri enstitüsü bilgisayar ve öğretim teknolojileri bilim dalında, kadın öğrenciler erkek öğrencilere göre iki katından fazla tez çalışması hazırlamışlardır.

Tezlerin sayfa sayılarına bakıldığında genel aralığın 80-120 sayfa aralığında olduğu ancak bilgisayar ve öğretim teknolojileri bilim dalındaki çalışmaların %50'sinin 120 sayfa üstü olduğu sonucu çıkmıştır.

## 4.2. Öneriler

Araştırma sonucunda elde edilen bulgulara dayanılarak akademik çalışmalarda siber güvenlik, bilgi güvenliği ve veri güvenliği konulu çalışmalardan elde edilen bilgiler açısından aşağıdaki öneriler sunulmuştur; Bireylerde siber güvenlik, siber suç olgusu, siber zorbalık, bilgi güvenliği, zararlı yazılımların bıraktığı hasarlar ve güvenli internet kullanımı farkındalığı yaratmak için bireylere eğitim, farkındalık etkinlikleri ve bilgilendirici sosyal mesajlar verilmelidir.

Tüm dünyada olduğu gibi ülkemizde de teknoloji kullanımı hızlı bir ivme ile artmaktadır. Teknolojik ürünlerin bilinçsiz kullanılması tahmin edilemeyecek büyüklükteki hasarları oluşturabilmektedir. Bu sebeple siber güvenlik kavramına belli başlı günler veya haftalardan ziyada her an dikkat çekilmeli ve bu farkındalığın artırılmasına yönelik kamu ile özel sektör iş birliği içinde olmalıdır. Eğitim faaliyetleri çeşitli yöntemlerle gerçekleştirilebilmektedir. İnternet siteleri oluşturulması, seminerler düzenlenmesi, bilgi güvenliğine ilişkin kampanyalar düzenlenmesi, bilgisayar ve internet kullanıcılarının güvenlikle ilgili gelişmeler, kötücül yazılım

ve kişisel verilerin korunması gibi konularda bilgilendirilmesi başlıca eğitim faaliyetleridir. TV, radyo ve internet gibi kitle iletişim araçları da farkındalığın oluşturulmasında önemli göreve sahiptir. Farkındalık oluşturulması adına İçişleri Bakanlığı Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı tarafından yürütülen Siberay projesi kapsamında ilk ve ortaöğretim kademelerinde bilgilendirici seminer ve eğitimler verilmektedir. Bu bilgilendirici faaliyetlerin sadece ilk ve ortaöğretim ile sınırlı kalmayarak lise, lisans, akademik hayat ve iş dünyasına aktarılması sağlanmalıdır. Siberay gibi sosyal sorumluluk projeleri sadece devlet eliyle yapılmamalı, özel sektör ve sivil toplum kuruluşları da siber güvenlik farkındalığı oluşturma adına bilgi güvenliği ve siber güvenlik alanında projeler yapmalıdır. Teknolojik gelişmeler yakından takip edilmelidir. Kullanılacak yazılım, donanım ve teknolojiler önceden uzmanlar tarafından test edilmelidir.

Siber güvenlik uzmanlarınca hazırlan raporlar dikkate alınarak öngörülen zafiyetler giderilmelidir. Ülkemizde ne yazık ki siber güvenlik ihlali sonrasında siber güvenlik kavramı önem kazanmakta bu durumda maddi manevi kayıp oluşturmaktadır. Kurumların siber güvenlik birimi uzmanları da dünya genelindeki güncelleri yakından takip etmeli ve yönetilen sistemlerde çok hızlı reaksiyon göstermelidir. Özellikle çok kullanıcılı kurumlarda son kullanıcılar bilinçlendirilmeli ve gereksiz yetki verilmemeli ve kullanılan parola değerleri karmaşık desenler kullanılarak belirli periyotlarla değiştirilmelidir. Çok kullanıcılı yapılarda yetki yönetimi çok dikkat edilmesi gereken bir husus olmakla beraber kullanıcının görev tanımı dışında tanımlanmış yetkileri tehdit olarak görülmelidir. Güvenlikte en zayıf halkanın insan olduğu unutulmamalıdır. Zararlı yazılım barındıran USB, mail ekinde yer alan zararlı kod, bilinmeyen URL adreslerine girilerek zararlı dosya indirilmesi gibi senaryolar son kullanıcı tarafından bilinçsizce tetiklenmektedir. Güvenlik bu sebeplerden dolayı teknoloji kullanımının en üst seviyelerde olduğu günümüzde önem arz etmektedir.

Bilgi güvenliği, siber güvenlik ve veri güvenliği alanında yapılan farkındalık programlarına katılımcılar sadece dinleyici olarak katılmamalı program içerisinde gerektiğinde oyuncu olarak interaktif katılım ile tam öğrenme sağlanmalıdır.

Güvenlik amaçlı kullanılan sistemler, üreticiden geldiği gibi kullanılmamalı kurumun politikaları doğrultusunda özelleştirilmelidir. Güvenlik duvarlarının kuralları genel ayarlar şeklinde kalmamalı kurumun yapısına uygun kurallar yazılarak sıkılaştırma yapılmalıdır. Ayrıca güvenlik cihazları ve diğer kullanılan cihazların güncelleştirme işlemleri takip edilerek yazılımların güncel olması sağlanmalıdır. Güvenlik duvarlarının yanı sıra kurum ağında anlık

davranış analizi yapabilen mekanizmaların kurulması ayrı bir güvenlik önlemidir. Hizmet durdurma saldırıları gibi çok farklı hedeften tek bir hedefe yönelik yapılan saldırılar fark edilerek önceden hazırlanmış sunuculara yönlendirilerek hizmet durması engellenmelidir. Yapay zekanın da önemli yer aldığı günümüzde güvenlik sistemleri, oluşabilecek tüm kötü senaryolara yönelik öncesinde test edilmelidir.

İlerde yapılacak araştırmalara yönelik öneriler aşağıda verilmiştir;

1. Bu araştırmada 225 çalışma analiz edilerek oluşturulmuştur. Sonraki çalışmalarda daha fazla çalışma kullanılarak yapılacak araştırmalar bu araştırma ile karşılaştırılabilir.

2. Bu araştırma, siber güvenlik, bilgi güvenliği ve veri güvenliği konulu akademik çalışmalar incelenmiştir. Başka bir çalışmada nitel araştırma yöntemleri kullanılarak bilişim kültürü seviyeleri ve bilgi güvenliği farkındalıkları belirlenebilir.

## KAYNAKLAR


Adams, S., Brokx, M., Dalla Corte, L., Galič, M., Kala, K., Koops, B., . . . Skorvánek, I. (2015). The Governance of Cybersecurity (s. 15-16). Netherlands: Tilburg University.

Ağaoğlu, E., Ceylan, M., Kesim, E., Madden, T., & Altınkurt, Y. (2005). Okul Yönetimi ile İlgili Lisansüstü Tezlerin İncelenmesi. II.Lisansüstü Eğitim Sempozyumu. İstanbul: Marmara Üniversitesi.

Akkoyunlu, B. (2002). Öğretmenlerin İnternet Kullanımı ve Bu Konudaki Öğretmen Görüşleri. Hacettepe Üniversitesi Eğitim Fakültesi Dergisi, 1-8.

Al, U., & Tonta, Y. (2004). Atıf Analizi: Hacettepe Üniversitesi Kütüphanecilik Bölümü Tezlerinde Atıf Yapılan Kaynaklar. Bilgi Dünyası, 19-47.

Alkan, C. (2011). Eğitim Teknolojisi. içinde Ankara: Anı Yayıncılık.

Altıner, İ. (2021). Öğretmenlerin Kişisel Siber Güvenlik Farkındalık Düzeylerinin Farklı Değişkenlere Göre Değerlendirilmesi. Yüksek Lisans Tezi. Ankara: Ankara Üniversitesi.

Arslan, S., & Şendurur, P. (2017). Eğitimde Teknoloji Entegrasyonunu Etkileyen Faktörlerdeki Değişim. Mehmet Akif Ersoy Üniversitesi Eğitim Fakültesi Dergisi, 25-50.

Aslan, Ö., Samet, R., & Tanrıöver, Ö. Ö. (2020). Using a Subtractive Center Behavioral Model to Detect Malware. Security and Communication Networks.

Aslay, F. (2017). Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi. International Journal of Multidisciplinary Studies and Innovative Technologies, 24 - 28.



Aslay, F. (2017). Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi. International Journal of Multidisciplinary Studies and Innovative Technologies, 24 - 28.



Aydeniz, M. (2021, 3 12). Eğitim Sistemimiz ve 21. Yüzyıl Hayalimiz: 2045 Hedeflerine İlerlerken, Türkiye İçin STEM Odaklı Ekonomik Bir Yol Haritası. Tennessee Research and Creative Exchange (TRACE):

https://trace.tennessee.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1019&context=utk_theopubs adresinden alındı

Bacanak, A., Karamustafaoğlu, O., Köse, S. (2003) Yeni Bir Bakış: Eğitimde Teknoloji Okuryazarlığı. Pamukkale Üniversitesi Eğitim Fakültesi Dergisi, 14, 191-196.

Barış, Ö. (2021). Etkin Siber Güvenlik Stratejilerinde Yönetim Bilişim Sistemlerinin Yaklaşımları. Yüksek Lisans Tezi. Ankara: Ufuk Üniversitesi.

Bayraktutan, Y., 2004. Bilgi, İktisadi Gelişme Evreleri ve Maldan Sanala Paranın Evrimi, Türkiye Günlüğü Dergisi. Sayı 78, s 12-14.

Bayram Nuran. Sosyal bilimlerde SPSS ile veri analizi. Ezgi Kitabevi.

Bıçakçı, S., Ergun, D., & Çelikpala, M. (2019). Türkiye'de Siber Güvenlik. Türkiye'de Siber Güvenlik ve Nükleer Enerji, 28 - 73.

Büyüköztürk Şener. Sosyal Bilimler için veri analizi el kitabı. Pegem Akademi Yayıncılık.

Canbek, G., & Sağıroğlu, Ş. (2006). Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme. Journal of Polytechnic, 165-174.

Cebeloğlu, S. (2020). Endüstri 4.0 Sistemlerinde Yapay Zeka Tabanlı Siber Güvenlik Yaklaşımlarının Geliştirilmesi. Yüksek Lisans Tezi. Elazığ: Fırat Üniversitesi.

Cengiz, G. (2021). Siber Suçlar, Sosyal Medya ve Siber Etik. İletişim Çalışmaları Dergisi, 7(3), 407-424.

Chalmers , I., Hedges, L., & Cooper, H. (2002). A brief history of research synthesis. Evaluation & the Health Professions, 12-37.

Clarke, R. A., & Knake, R. K. (2011). Siber Savaş : Ulusal Güvenliğe Yönelik Yeni Tehdit (s. 44). içinde İstanbul: İstanbul Kültür Üniversitesi Yayınevi.

Çiftçi, H. (2013). Her Yönüyle Siber Savaş. TÜBİTAK Yayınları.

Demirel, Ö. (2003). Eğitim Sözlüğü Dictionary of Education (2. b.). Ankara: Pegem A Yayıncılık.

Demirel, Ö., & Altun, E. (2009). Eğitim, Öğretim Teknolojisi ve İletişim, Öğretim Teknolojileri ve Materyal Tasarımı (s. 1-127). içinde Ankara: Pegem Akademi.

Dönmez, G. (2019). Lise Öğrencilerinin Bilgi Güvenliği Farkındalığı İle Dijital Okuryazarlığı Arasındaki İlişkinin İncelenmesi. Yüksek Lisans Tezi. Ankara: Hacettepe Üniversitesi.

Durmuş, Ö. (2021). Siber Güvenlik Önlemlerinin Analizi ve Modellenmesi. Yüksek Lisans Tezi. Elazığ: Fırat Üniversitesi.

EGM. (2022). Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı. https://www.egm.gov.tr/siber/sibersucnedir adresinden alınmıştır. Erişim tarihi: 03.12.2022

Erkuş, A. (2009). A. Erkuş içinde, Davranış Bilimleri İçin Bilimsel Araştırma Süreci (İkinci Baskı b.). Ankara: Seçkin Yayıncılık.

Ersöz Filiz, Ersöz Taner. IBM SPSS ile İstatistiksel Veri Analizi. Elit kültür yayınevi.

Ertürk, S. (1984). S. Ertürk içinde, Eğitimde 'Program' Geliştirme (s. 12). Ankara: Yelkentepe Yayınları.

Güleç, Ö. (2021). Uluslararası İlişkilerde Siber Güvenlik Kavramı ve Uygulamaları. Yüksek Lisans Tezi. Elazığ: Fırat Üniversitesi.

Güneş, F. (2020). Kitlesel Açık Çevrimiçi Ders Platformlarında Yayınlanan Siber Güvenlik İçeriklerinin Çoklu Ortam Tasarım İlkeleri Açısından İncelenmesi. Yüksek Lisans Tezi. Ankara: Gazi Üniversitesi.

Güngör, N. (2021). İç Denetimde Bilgi Teknolojileri ve Siber Güvenlik: Borsa İstanbul Şirketlerinde Bir İnceleme. Doktora Tezi. İstanbul: İstanbul Üniversitesi.

Hacımustafaoğlu, R. (2019). Ortaöğretim Öğrencilerinin Bilgi Güvenliği Farkındalık Düzeylerinin Siber Mağdur Olma Durumlarına Etkisinin İncelenmesi (Üsküdar Örneği). Yüksek Lisans Tezi. Sakarya: Sakarya Üniversitesi.

Hakan AYDIN, Mehmet Ali Barışkan, Ali Çetinkaya- Siber Güvenlik Kapsamında Enerji Sistemleri Güvenliğinin Değerlendirilmesi- Güvenlik Bilimleri Dergisi, Mayıs 2021, Cilt:10 Sayı:1, 151-174.

Hekim, H. (2013). Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları. Uluslararası Güvenlik ve Terörizm Dergis, 133 - 158.

Işık, Z. E. (2019). Siber Güvenlik Ekosisteminin Geliştirilmesi. Yüksek Lisans Tezi. Ankara: Gazi Üniversitesi.

Kapanoğlu, G. (2016). Öğretmenlerin Bilgi Güvenliği Farkındalığının İncelenmesi. Yüksek Lisans Tezi. Ankara: Gazi Üniversitesi.

Kara, İ. (2019). Dijital Verilerin İmha Süreçlerinin Tanımlanması ve Uygulama Yönünden Değerlendirilmesi. Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi, 52-58.

Karaarslan, E., & Akbaş, M. F. (2017). Blokzinciri Tabanlı Siber Güvenlik Sistemleri. Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, 16 - 21.

Karabacak, B. (2011). Kritik Altyapılara Yönelik Siber Tehditler ve Türkiye İçin Siber Güvenlik Önerileri. Siber Güvenlik Çalıştayı , 1 - 11.

Karabulut, B. (2021). Büyük Ölçekli Ağlarda Gerçek Zamanlı Hibrit Honeypot Sistemi: Türk Siber Güvenlik Sektöründe. Yüksek Lisans Tezi. İstanbul: İstanbul Ticaret Üniversitesi.

Karacı, A., Akyüz, H. İ., & Bilgici, G. (2017). Üniversite Öğrencilerinin Siber Güvenlik Davranışlarının İncelenmesi. Kastamonu Eğitim Dergisi, 2079 - 2094.

Kolaç, E. (2008). İlk Okuma Yazma Alanında Yapılan Lisansüstü Tezlerin Değerlendirilmesi. VII. Ulusal Sınıf Öğretmenliği Eğitimi Sempozyumu (s. 1-21). Çanakkkale: Çanakkale Onsekiz Mart Üniversitesi.

Lorcu Fatma. Örneklerle veri analizi. Ezgi Kitabevi.

McAfee. (2021, Haziran 19). Haziran 19, 2021 tarihinde https://www.mcafee.com: https://www.mcafee.com/tr-tr/antivirus/malware.html adresinden alındı

McCumber J.R. (1991) Information systems security: A comprehensive model. InProc. 14thNIST-NCSC National Computer Security Conference, 1-4 October, Washington D.C., 328-337.

Mehmet Emin Arslan, Gazi Üniversitesi Sağlık Bilişim Enstitüsü- Siber Güvenlik ve Siber Saldırı Türleri.

Önel, D., & Dinçkan, A. (2007). Bilgi Güvenliği Yönetim Sistemi Kurulumu. TÜBİTAK UEKAE (Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü), 6.

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

Sağıroğlu Ş., Alkan M., Samet R., ve ark. (2018) Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık, Grafiker Yayınları, Ankara, Türkiye

Sarı, O. (2013). Uluslararası Hukuk ve Türk Ceza Hukuku Bağlamında Siber Güvenlik ve Bilişim Sistemine Yönelik Suçlar. Harp Akademileri Stratejik Araştırmalar Enstitüsü.

Schroeder, G. N., Steinmetz, C., Pereira, C. E., & Espindola, D. B. (2016). Digital Twin Data Modeling with AutomationML and a Communication Methodology for Data Exchange. IFAC-PapersOnLine, 12-17.

Solmaz, M. (2020). Öğretmen Adaylarının Siber Bilgi Güvenliği Farkındalıklarının ve Dijital Vatandaşlık Düzeylerinin Farklı Değişkenler Açısından İncelenmesi. Yüksek Lisans Tezi. Mersin: Mersin Üniversitesi.

Şengül, G., Atsan, F. K., & Bostan, A. (2014). Adli Bilişim Alanındaki Mevcut Problemler, Çözüm Önerileri ve Gelecek Öngörüleri. 7. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, (s. 17-18).

Şenol, Ş. (2008). Tanımlayıcı İstatistik (s. 52-53). içinde İstanbul: Nobel Yayınları.

Tığlı, İ. (2021). Türk Jandarma Literatürünün Bibliyografik Analizi (1928-2021). Yüksek Lisans Tezi. Ankara: T.C. İçişleri Bakanlığı Jandarma Ve Sahil Güvenlik Akademisi Güvenlik Bilimleri Enstitüsü.

Türkiye Bilişim Sanayicileri Derneği, (TUBISAD), Türkiye'nin Siber Güvenlik Stratejisine Yönelik Değerlendirmeler,

Ulaştırma Denizcilik ve Haberleşme Bakanlığı, (UDHB), 2016-2019 Ulusal Siber Güvenlik Stratejisi, https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf Erişim tarihi: 30.11.2020

Ünver M., Canbay C., (2010). Ulusal ve Uluslararası Boyutlarıyla Siber Güvenlik. Elektrik Mühendisliği, 438, 94-103.ç

Yerlikaya, A.C. (2019). Bilgi Güvenliğine Yönelik Öğrenci, Öğretmen, Veli ve Okul Yöneticilerinin Farkındalıklarının İncelenmesi. Yüksek Lisans Tezi. İzmir: Ege Üniversitesi.

Yıldırım, A., & Şimşek, H. (2011). Sosyal Bilimlerde Nitel Araştırma Yöntemleri (s. 39). içinde Ankara: Seçkin Yayıncılık.

Yıldırım, C. (1966). Eğitimde Araştırma Metotları (s. 67). içinde Ankara: Ayyıldız Matbaası.

Yıldız, A. K. (2006). Dijital Belge Yönetimi: Dijital Belgelerin Üretimi, Yönetimi ve Korunması için Rehber. Bilgi Dünyası.

Yılmaz, E., Şahin, Y. L., & Akbulut, Y. (2016). Öğretmenlerin Dijital Veri Güvenliği Farkındalığı. Sakarya University Journal of Education, 26-45.

Zupic, I., & Cater, T. (2015). Bibliometric Methods in Management and Organization. Organizational Research Methods, 429-472.

http://www.tubisad.org.tr/tr/images/pdf/dtp_siber_guvenlik_raporu_4_0.pdf Erişim tarihi: 10.12.2020

https://en.wikipedia.org/wiki/Bibliography Erişim tarihi: 10.12.2021

https://en.wikipedia.org/wiki/Bibliometrics Erişim tarihi: 10.12.2021

https://www.btkakademi.gov.tr/portal/blog/remote-access-trojan-rat-nedir-1550 Erişim tarihi: 02.02.2022

# EKLER

## EK 1 Araştırmada İncelenen Araştırmalar

## EK 1 Araştırmada İncelenen Araştırmalar

| SIRA | TEZ NO | YAZAR | YIL | TEZ ADI | TEZ TÜRÜ |
|---|---|---|---|---|---|
| **1** | 134325 | BİLGE KARABACAK | 2003 | Bilgi güvenliği risk analizi (BİGRA) metodu | YL |
| **2** | 146162 | FAİK BAŞHAN | 2004 | İşletmelerin ağ-bilgi sistemlerinde bilgi güvenliğinin yönetimi ve bir uygulama | YL |
| **3** | 184322 | ÖZLEM ÖZKAN | 2004 | Veri güvenliğinde saldırı ve savunma yöntemleri | YL |
| **4** | 199160 | AHMET ERKAN | 2006 | An automated tool for information security management system | YL |
| **5** | 186015 | PELİN ÖĞÜT | 2006 | Küreselleşen dünyada bilgi güvenliğine yönelik politikalar: Sayısal imza teknolojisi ve Türkiye | YL |
| **6** | 219994 | ŞENER MAVZER | 2006 | Milli olan yazılımların ve milli olmayan yazılımların bilgi güvenliğine etkileri: Karşılaştırmalı bir çalışma | YL |
| **7** | 210683 | BÜNYAMİN YILDIZ | 2007 | Bilgi güvenliği ve e-devlet kapsamında kamu kurumlarında bilgi güvenliği yönetimi standartlarının uygulanması | YL |
| **8** | 220815 | GÖKHAN ERGEN | 2007 | Developing an information security management framework: Case studies on registration office and computer center of a state university | YL |
| **9** | 214814 | İSMAİL ÖZLER | 2007 | Bilgi güvenliği ve elektronik imza kavramları: Ekonomik boyutlarının incelenmesi ve elektronik imza uygulamaları | YL |
| **10** | 212815 | YILMAZ VURAL | 2007 | Kurumsal bilgi güvenliği ve sızma (penetrasyon) testleri | YL |
| **11** | 237127 | MEHTAP ÇETİNKAYA | 2008 | Bilgi güvenliği yönetim sistemi alt yapısının değerlendirilmesi için bir test aracı geliştirilmesi | YL |
| **12** | 240309 | CENGİZHAN CANLI | 2009 | Saldırı tesbit sistemlerinin incelemesi ve bu bağlamda bilgi güvenliği | YL |
| **13** | 259635 | ERHAN KUMAŞ | 2009 | Bilgi güvenliğinin sağlanmasında risk yönetimi: E-devlet kapısı uygulaması | YL |
| **14** | 278365 | NECLA VARDAL | 2009 | Yükseköğretimde bilgi güvenliği: Bilgi güvenlik yönetim sistemi için bir model önerisi ve uygulaması | DR |
| **15** | 246397 | BİLAL ÖZCAN | 2009 | Kurumsal bilgi güvenliği ve cobıt | YL |
| **16** | 239879 | ÇİĞDEM YILDIZ | 2009 | Telekomünikasyon sektöründe firma içindeki bilgi güvenliğini etkileyen faktörler ve bu faktörlerin çalışanlar üzerine etkileri | YL |
| **17** | 238229 | YAŞAR ARSLAN | 2009 | Web tabanlı uzaktan eğitim sistemlerinde bilgi güvenliğinin sağlanması | YL |

| SIRA | TEZ NO | YAZAR | YIL | TEZ ADI | TEZ TÜRÜ |
|---|---|---|---|---|---|
| **18** | 238690 | FATMA ÖZDEN AKTAŞ | 2009 | Bilgi güvenliği risk yönetiminde en uygun ve objektif yöntemin belirlenmesi | YL |
| **19** | 258223 | KEREM ASLANDAĞ | 2010 | Bilgi güvenliği kavramı ve bilgi güvenliği yönetim sistemleri ile şirket performansı ilişkisine dair bir uygulama | YL |
| **20** | 291855 | EMEL AYDOĞMUŞ | 2010 | Assessment of information security maturity levels and ISO/IEC 27001:2005 compliance of organizations in turkey | YL |
| **21** | 273018 | UFUK BİNGÖL | 2010 | ISO 27001 bilgi güvenliği yönetim sistemi otomasyonu | YL |
| **22** | 271494 | HAKKI TOK | 2010 | Kamu kurumları için bilgi güvenliği yönetişim modeli | YL |
| **23** | 269257 | ENDER ŞAHİNASLAN | 2010 | Standartlara dayalı bilgi güvenliği risk analiz ve ölçümleme metodolojisinin bankacılık sektörüne özgü modellenmesi ve uygulama yazılımının geliştirilmesi | DR |
| **24** | 273108 | HAKAN METE | 2010 | ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi'nin bilgi işlem merkezlerinde uygulanması | YL |
| **25** | 287481 | CEMAL GEMCİ | 2010 | Uzman sistem temelli bilgi güvenliği yönetim sistemi yaklaşımı | DR |
| **26** | 295662 | MUSTAFA GÜLMÜŞ | 2010 | Kurumsal bilgi güvenliği yönetim sistemleri ve güvenliği | YL |
| **27** | 262493 | ÖZLEM TOĞUZ | 2010 | Data protection and intellectual property in the EU and Turkey | YL |
| **28** | 273520 | ARİF YILDIRIM | 2010 | Bilişim sistemlerinde veri güvenliği yaklaşımı ve şifreleme algoritmaları: DNA algoritması önerisi | DR |
| **29** | 312774 | ÖZNUR ESMER | 2011 | RFID teknolojisinde veri güvenliğinin sağlanması için melez şifreleme algoritmasının uygulanması | YL |
| **30** | 300205 | METE EMİNAĞAOĞLU | 2011 | Özdevimli öğrenme yaklaşımı ile bilgi güvenliği risklerinin nitel değerlendirilmesine yönelik bir model | DR |
| **31** | 287054 | TÜRKER TUNCER | 2011 | Resimler için veri gizleme tabanlı bilgi güvenliği uygulamaları | YL |
| **32** | 315146 | ERKAN BAYAR | 2012 | Modern kriptosistemlerle şifrelemenin modellenmesi ile veri güvenliğinin sağlanması | YL |
| **33** | 304658 | OĞUZ ATA | 2012 | Kablosuz duyarga ağlarda azami veri güvenliğini sağlamak için mimari tasarım | DR |
| **34** | 330848 | TUĞBA HAKLI | 2012 | Bilgi güvenliği standartları ve kamu kurumları bilgi güvenliği için bir model önerisi. | YL |
| **35** | 331292 | BAŞAK GERÇEKER | 2012 | Sağlık kuruluşlarında örgüt iklimi ve bilgi güvenliğinin ilişkisi | YL |

| SIRA | TEZ NO | YAZAR | YIL | TEZ ADI | TEZ TÜRÜ |
|---|---|---|---|---|---|
| **36** | 323863 | FÜRKAN ELİBOL | 2012 | Monitörlerin elektromanyetik yayınımlarının bilgi güvenliği açısından incelenmesi ve yazılımsal korunma yöntemi geliştirilmesi | YL |
| **37** | 302368 | NECATİ ALASULU | 2012 | Bilgi güvenliği ve kalite yönetim sistemleri arasındaki ilişkinin incelenmesi ve bir uygulama | YL |
| **38** | 318088 | İNCİ MART | 2012 | Bilişim kültüründe bilgi güvenliği farkındalığı | YL |
| **39** | 322107 | MEHMET SALİH GÖK | 2012 | 5651 sayılı Kanun ve bilgi güvenliği ilişkisi | YL |
| **40** | 386061 | FARUK AYDIN | 2012 | Cyber security in the national protection of Turkey | YL |
| **41** | 348942 | ONUR SARI | 2013 | Uluslararası Hukuk ve Türk Ceza Hukuku bağlamında siber güvenlik ve bilişim sistemine yönelik suçlar | YL |
| **42** | 332057 | SÜLEYMAN FİLİZ | 2013 | Siber güvenlikte biyometrik sistemler ve yüz tanıma | YL |
| **43** | 353566 | MUHAMMED ALPARSLAN AKYILDIZ | 2013 | Siber güvenlik açısından sızma testlerinin uygulamalar ile değerlendirilmesi | YL |
| **44** | 335475 | MELTEM KOCAMUSTAFAOĞULLARI | 2013 | A prototype for assessment of information security awareness and implementation level | YL |
| **45** | 346626 | OTGONJARGAL GANBAT | 2013 | Bilgi güvenliği yönetim sistemi ISO/IEC 27001 ve bilgi güvenliği risk yönetimi ISO/IEC 27005 standartlarının uygulanması | YL |
| **46** | 344372 | FATİH AKYOL | 2013 | COBIT (Bilgi ve ilgili teknolojiler için kontrol hedefleri) uygulayan şirketlerdeki bilgi güvenliği politikalarının şirket, personel ve süreçlere etkileri | YL |
| **47** | 337116 | GÖKHAN MUHARREMOĞLU | 2013 | Kurumsal bilgi güvenliğinde zafiyet, saldırı ve savunma öğelerinin incelenmesi | YL |
| **48** | 327359 | BİLGEN YILMAZ | 2013 | E-dönüşüm sistemlerinin bilgi güvenliği açısından incelenmesi e-devlet kullanıcıları üzerine bir araştırma | YL |
| **49** | 335284 | ESRA ŞATIR | 2013 | Bilgi güvenliği için metin steganografisinde yeni bir yaklaşım | DR |
| **50** | 354864 | HASAN DEMİRTAŞ | 2013 | Bilgi güvenliği yönetiminin gerekleri ve başarı dayanakları:Bir uygulama örneği | YL |
| **51** | 355576 | ARZU ÖZ | 2013 | Bulut bilişim veri güvenliği | YL |
| **52** | 382296 | ANAS MU'AZU KADEMİ | 2014 | National cyber security strategy: A model for Nigeria | YL |
| **53** | 368390 | İSMAYİL GÖKHAN AKAY | 2014 | Bilgi güvenliği yönetim sistemleri: Bilgi güvenliği uygulama mülakatları | YL |
| **54** | 389081 | TURAN TOLGAY KIZILELMA | 2014 | An analysis of the relationships among information security | DR |

| SIRA | TEZ NO | YAZAR | YIL | TEZ ADI | TEZ TÜRÜ |
|---|---|---|---|---|---|
| | | | | management systems, patient safety, and quality | |
| **55** | 374418 | MURAT OĞUZ | 2014 | Managing the human factors in information security through computational intelligence methods | YL |
| **56** | 657002 | BANU ERDEM | 2014 | Analyse des donnees de securite de systemes d'information | YL |
| **57** | 392876 | İZZET ATIL GÜRCAN | 2014 | Assessing information security management requirements for finance sector using an ISO 27001 based approach | YL |
| **58** | 372501 | AHMET DURMUŞ | 2014 | The observation of information security awareness in Turkey | YL |
| **59** | 361360 | PINAR KILIÇ AKSU | 2014 | Hastane bilgi yönetim sisteminin bilgi güvenliği açısından değerlendirilmesi | DR |
| **60** | 363034 | RAMAZAN ALTUN | 2014 | Belirli kısıtlara göre bilgi güvenliği ihlallerinin tespiti | YL |
| **61** | 365729 | VOLKAN YILMAZ | 2014 | Veri güvenliği esaslı 'Kendi Cihazını Getir' sistem tasarımı | YL |
| **62** | 409164 | ADEM TOSUN | 2015 | A survey about the integration of social engineering attacks and cyber security policies exploiting Turkish vulnerabilities in Turkey | YL |
| **63** | 417580 | YASEMEN ÖZFINDIK KOİK | 2015 | Uluslararası ilişkilerde siber güvenlik algısı ve ulus devletin değişen stratejisi | YL |
| **64** | 398413 | MUSTAFA MERAL | 2015 | Siber güvenlik kapsamında kritik altyapıların korunmasının önemi | YL |
| **65** | 392800 | AKIN AYTEKİN | 2015 | Türkiye'nin siber güvenlik stratejisi ve eylem planının değerlendirilmesi | YL |
| **66** | 385867 | MEHMET ERCAN | 2015 | Kritik altyapıların korunmasına ilişkin belirlenen siber güvenlik stratejileri | YL |
| **67** | 384780 | NURCAN TATAR | 2015 | The comparison of information security standards by using analytic hierarchy process | YL |
| **68** | 398691 | ÖZGÜR TAŞDEMİR | 2015 | Implementing PCI DSS v3.0 information security standards | YL |
| **69** | 379857 | BAHADIR GÖKHAN SARIKOZ | 2015 | An information security framework for web services in enterprise networks | YL |
| **70** | 396156 | CAN GÜLDÜREN | 2015 | Yükseköğretim kurumlarındaki öğretim elemanlarının bilgi güvenliği farkındalık düzeylerinin değerlendirilmesi | DR |
| **71** | 398539 | KEREM GENCER | 2015 | ISO 27001 kapsamında kurumsal bilgi güvenliğine dinamik bir yaklaşım | YL |
| **72** | 380076 | TÜRKAY HENKOĞLU | 2015 | Hassas bilgi varlıklarının ve kişisel verilerin hukuksal düzenlemeler ile korunması ve bu kapsamda üniversiteler için bilgi güvenliği politikasının geliştirilmesi | DR |

| SIRA | TEZ NO | YAZAR | YIL | TEZ ADI | TEZ TÜRÜ |
|---|---|---|---|---|---|
| **73** | 396689 | OĞUZHAN GÜNEY | 2015 | Uluslararası yeni güvenlik yaklaşımları kavramsalında bilgi güvenliğinin önemi | YL |
| **74** | 428221 | ERKAN AĞIRALAN | 2015 | Bilgi güvenliği, kişisel verilerin korunması ve mahremiyet etki değerlendirmesi | YL |
| **75** | 395184 | ERAY YILMAZ | 2015 | Öğretmenlerin dijital veri güvenliği farkındalığı | DR |
| **76** | 439049 | DUYGU KÜÇÜKAYDIN | 2016 | National and international cybersecurity strategies of the United States: A securitization attempt | YL |
| **77** | 435138 | DENİZ ZERİN | 2016 | Governing Turkey's internet: Cyber security as a strategy of power | YL |
| **78** | 449489 | SALİH ERDEM EROL | 2016 | Siber güvenlik farkındalığı için yetenek tabanlı dinamik model | YL |
| **79** | 450056 | VAHİT GÜNTAY | 2016 | Uluslararası ilişkiler temelinde siber güvenlik: Mikro siber ittifak teorisi (Micro-CAT) | DR |
| **80** | 447934 | MEHMET EREN | 2016 | Avrupa Birliği'nin siber güvenlik politikası | YL |
| **81** | 448102 | İBRAHİM KURNAZ | 2016 | 21. yüzyılda ortodoks güvenlik paradigmasının aşınımı: Uluslararası ilişkilerde siber güvenlik | YL |
| **82** | 429510 | BARIŞ ÇELİKTAŞ | 2016 | Siber güvenlik kavramının gelişimi ve Türkiye özelinde bir değerlendirme | YL |
| **83** | 457635 | YASİN KARAPINAR | 2016 | Developing a search tool for information security management systems standards | YL |
| **84** | 460829 | OĞUZHAN ŞEREFLİŞAN | 2016 | Quantitive management of information security in organizations | YL |
| **85** | 425884 | ŞEHNAZ HİLAL MOĞOL | 2016 | Importance of information security awareness | YL |
| **86** | 424182 | İSMAİL KARADOĞAN | 2016 | Ağ iletişiminde veri gizleme tabanlı bilgi güvenliği uygulamaları | YL |
| **87** | 457958 | EMRE DEMİROK | 2016 | Kurumsal bilgi güvenliği yönetim sistemi; vakıf üniversitesi örneği | YL |
| **88** | 458010 | ABDULKADİR BİLEN | 2016 | Bir kurumun bilgi güvenliği farkındalığının incelenmesi | YL |
| **89** | 450078 | GÜLSÜM KAPANOĞLU | 2016 | Öğretmenlerin bilgi güvenliği farkındalığının incelenmesi | YL |
| **90** | 432136 | ÖZGE ALTINPULLUK | 2016 | Iso 27001:2013 Bilgi Güvenliği Yönetim Sistemi kurumsal risk yönetimi | YL |
| **91** | 424173 | ERSAN YAZAN | 2016 | Veri güvenliği için gizlilik paylaşımı temelli bir uygulama | YL |
| **92** | 490282 | MAHA SAMEER ABDULADHEEM | 2017 | A comparative study of common cyber security policies for different enterprises | YL |
| **93** | 487335 | ALİ BURAK DARICILI | 2017 | Amerika Birleşik Devletleri ve Rusya Federasyonu'nun siber | DR |

| SIRA | TEZ NO | YAZAR | YIL | TEZ ADI | TEZ TÜRÜ |
|---|---|---|---|---|---|
| | | | | güvenlik stratejilerinin karşılaştırmalı analizi | |
| **94** | 476751 | MERT MELİH ÖZÇELİK | 2017 | Kablosuz algılayıcı ağların siber güvenlik açısından incelenmesi ve özgün bir saldırı tespit sisteminin önerilmesi | YL |
| **95** | 472522 | MEHMET ALİ BARIŞKAN | 2017 | Türkiye'deki siber güvenlik bilinci ve sosyal mühendislik ataklarına karşı savunma önlemlerinin geliştirilmesi | YL |
| **96** | 465384 | NAZLI BAŞDİNKÇİ | 2017 | Sağlık kurumlarında bilgi güvenliği risk değerlendirilmesi ve kullanıcıların bilgi güvenliği farkındalık düzeyinin ölçülmesi | YL |
| **97** | 496021 | ERAY ÇEK | 2017 | Kurumsal bilgi güvenliği yönetişimi ve bilgi güvenliği için insan faktörünün önemi | YL |
| **98** | 481831 | NABİ KOÇ | 2017 | İşletmelerde bilgi güvenliği için web tabanlı bir uygulamanın geliştirilmesi | YL |
| **99** | 472920 | ATILGAN ERDOĞMUŞ | 2017 | Üniversite öğrencilerinin bilgi güvenliği kazanımlarının, farkındalıkları üzerindeki etkilerinin analizi: Afyon Kocatepe Üniversitesi örneği | YL |
| **100** | 479816 | İSMET ÇUHADAR | 2017 | İnsansız hava aracı sistemlerinde bilgi güvenliği ve risk tabanlı çok kriterli karar verme modeli ile değerlendirilmesi | DR |
| **101** | 488754 | ÇİĞDEM ÇELİK ÇÖP | 2017 | Kalite yönetim direktörlerinin bilgi güvenliği farkındalığı:İstanbul ili örneği | YL |
| **102** | 492929 | BERRİN ASLAN ÖZTEZCAN | 2017 | Bilgi güvenliği farkındalığı üzerine bir araştırma : Marmara Üniversitesi örneği | YL |
| **103** | 488060 | GÖKSU HAZAR ERDİNÇ | 2017 | Bilgi güvenliği, kişisel verilerin korunması ve biyometrik verilerin işlenmesine ilişkin öneriler | YL |
| **104** | 467467 | BATMUNKH GANBAT | 2017 | Steganografi ile bilgi güvenliği | YL |
| **105** | 467466 | ABUBAKR RAKHIMOV | 2017 | Biyometrik sistemlerin bilgi güvenliği | YL |
| **106** | 476744 | ERTUĞRUL AKTAN | 2017 | Örgüt kültürünün bilgi güvenliği algısı üzerine etkisi: Türkiye'deki devlet üniversitelerinde bir araştırma | DR |
| **107** | 472964 | ÖMER FARUK KAYA | 2017 | Kurumsal işletmelerde bilgi ve veri güvenliği | YL |
| **108** | 488430 | SAYED ZAKARIYA HABIB | 2018 | Investigation of Afghanistan network infrastructure for cyber security | YL |
| **109** | 510056 | MEVLÜT BÜYÜKKILIÇ | 2018 | Cybersecurity framework for small and medium size enterprises | YL |
| **110** | 498778 | AHMET BOZGEYİK | 2018 | Gaziantep'te faaliyet gösteren orta ve büyük ölçekli işletmelerin siber güvenlik yönetim yaklaşımlarının analizi | DR |

| SIRA | TEZ NO | YAZAR | YIL | TEZ ADI | TEZ TÜRÜ |
|---|---|---|---|---|---|
| **111** | 492344 | VOLKAN GÖÇOĞLU | 2018 | Türkiye'nin siber güvenlik politikalarının kamu politikası analizi çerçevesinde değerlendirilmesi | DR |
| **112** | 508020 | ÖZGÜR ALP | 2018 | Akıllı şehirlerde siber güvenlik | YL |
| **113** | 532351 | GİZEM SOMUNCU | 2018 | NATO'nun güvenlik alanında yeni bir boyut: Siber güvenlik | YL |
| **114** | 517572 | KAMİL TARHAN | 2018 | Uluslararası güvenliğin bir bileşeni olarak siber güvenlik | YL |
| **115** | 493020 | ABDULLAH TOKDAŞ | 2018 | Siber güvenlik ve uluslararası ilişkiler | YL |
| **116** | 530411 | DİLAVER GEDİK | 2018 | Siber güvenlik ve terörizmin evrilişi: Türkiye üzerine etkileri | YL |
| **117** | 496262 | MEHMET ADA | 2018 | NATO üyesi ülkelerin siber güvenlik stratejileri açısından incelenmesi | YL |
| **118** | 509880 | MUSTAFA TURAN | 2018 | A systematic review of 6698-Law on the Protection of Personal Data in Turkey according to the information security practices and applicability of law perspective | YL |
| **119** | 507626 | NUR SENA TANRIVERDİ | 2018 | The effect of employees' information security familiarity on their security incident awareness | YL |
| **120** | 543945 | EMRE TANER | 2018 | Güvenlik güçlerinin bilgi güvenliği farkındalığına yönelik bir betimleme | YL |
| **121** | 525418 | HALİL ERBİ | 2018 | Bilgi güvenliği stres faktörlerinin iş tatminin üzerindeki etkileri: AR-GE merkezi olan işletmeler üzerine bir araştırma | YL |
| **122** | 515405 | HANİFE GÜLİZ YAYLA | 2018 | Fatih projesi uygulanan ve uygulanmayan okullardaki öğretmenlerin bilgi güvenliği farkındalığının incelenmesi | YL |
| **123** | 507785 | OLDOUZ KARİMİ | 2018 | İnsan faktörünü içeren bilgi güvenliği çerçevesi için kavramsal bir model oluşturmak | DR |
| **124** | 493378 | ESRA SEVİMLİ | 2018 | Sağlık yönetiminin gelecekteki paydaşlarından bilgisayar mühendisliği öğrencilerinin sağlık bilgi sistemlerini bilgi güvenliği ve hasta mahremiyeti açısından değerlendirmesi | YL |
| **125** | 495144 | YUSUF ALACA | 2018 | Yapay bağışıklık sistemleri ile bilgi güvenliği ve olay yönetimi geliştirilmesi | YL |
| **126** | 498775 | CÜNEYT ÇATUK | 2018 | Siber riskler karşısında KOBİ'lerin bilgi güvenliği farkındalıklarını ölçen bir ölçek geliştirme: Gaziantep örneklemi | DR |
| **127** | 529299 | MUSTAFA YILMAZ | 2018 | İşletmelerde bilgi güvenliği uygulama sorunları ve çözüm önerileri; Konya örneği | YL |
| **128** | 511289 | SERKAN GÖNEN | 2018 | PLC ile kontrol edilen mikro tip akıllı şebeke sistemlerde bilgi güvenliğinin sağlanması | DR |

| SIRA | TEZ NO | YAZAR | YIL | TEZ ADI | TEZ TÜRÜ |
|---|---|---|---|---|---|
| **129** | 518074 | ASNDAR WAINAKH | 2018 | Homomorphic encryption for data security in cloud computing | YL |
| **130** | 518075 | BERNA ILGAZ | 2018 | Küçük ve orta büyüklükteki işletmeler için veri güvenliği ve standartları | YL |
| **131** | 485011 | SEYİT BÖGE | 2018 | Sanal özel ağlarda veri güvenliği | YL |
| **132** | 552715 | GİZEM YÜKSEL | 2019 | Antecedents and consequences of cyber security awareness: A case study for maritime sector | YL |
| **133** | 548678 | BURAK AYDIN | 2019 | Identifying critical cybersecurity controls at country level | YL |
| **134** | 550720 | HASAN ÇİFCİ | 2019 | Technology foresight and modeling: Turkish cybersecurity foresight 2040 | DR |
| **135** | 607225 | BÜNYAMİN GÜNEŞ | 2019 | Siber fiziksel sistemler üzerinde bütünleşik siber güvenlik risk değerlendirmesi: Bir konteyner limanı uygulaması | YL |
| **136** | 572168 | ARİF EMRE ADIR | 2019 | Kurumlar için siber güvenlik laboratuvarı altyapısının oluşturulması | YL |
| **137** | 594353 | YASEMİN GÜRYUVA | 2019 | Uluslararası siber güvenlik ve siber ortamdaki tehditlerin fiziksel bir savaşa dönüşme olasılığı | YL |
| **138** | 576469 | HÜSNÜ TAVLAŞ | 2019 | Ortaöğretim kurumlarında uygulanan uygulanan siber güvenlik farkındalık eğitiminin öğrenciler üzerindeki etkisi | YL |
| **139** | 600278 | EMRE GÜL | 2019 | Log yönetimi ile siber güvenlik araçlarının geliştirilmesi | YL |
| **140** | 562140 | GÜLCİHAN AYDANER | 2019 | Genç tüketicilerin sosyal mühendislik ile siber güvenlik farkındalıklarının online alışveriş niyetleri üzerindeki etkisinin ölçülmesi | YL |
| **141** | 582563 | SU DİLARA ALİOĞLU | 2019 | Siber saldırılar ve ülkelerin siber güvenlik politikaları | YL |
| **142** | 561930 | CİHAN ATAÇ | 2019 | Ulusal siber güvenlik stratejisi oluşturma sürecine bir bakış | YL |
| **143** | 575731 | SEZER YILDIZ | 2019 | Yerel alan ağlarının siber güvenlik yönünden incelenmesi ve değerlendirilmesi | YL |
| **144** | 545623 | İBRAHİM YALÇIN | 2019 | Soğuk savaş sonrası NATO ve Türkiye'de siber güvenlik | YL |
| **145** | 564312 | AYCAN RAMAZAN GÜNDÜZHEV | 2019 | Siber güvenlik yönetim modelleri ve etkilerinin araştırılması | YL |
| **146** | 569578 | YASEMİN ÖZBEK | 2019 | Öğretmen adaylarının siber güvenlik farkındalıklarının incelenmesi | YL |
| **147** | 589528 | ZEYNEP EBRU IŞIK | 2019 | Siber güvenlik ekosisteminin geliştirilmesi | YL |
| **148** | 593168 | AYFER EKİZ | 2019 | Information security management system and information security risk management methodology development | YL |
| **149** | 607327 | BERKER KILIÇ | 2019 | ISO/IEC 27001 bilgi güvenliği yönetim sistemi açısından türkiye' | YL |

| SIRA | TEZ NO | YAZAR | YIL | TEZ ADI | TEZ TÜRÜ |
|---|---|---|---|---|---|
| | | | | de hukuk bürolarında bilgi güvenliği yönetimi | |
| **150** | 547705 | EVRİM AKMAN KADIOĞLU | 2019 | Design, development and implementation of an information security and cyberethics course for pre-service teachers: A design-based research | DR |
| **151** | 586556 | ERCAN BUĞRA TOKDEMİR | 2019 | An information security management system approach and technical security best practices for the enterprise companies | YL |
| **152** | 592917 | MESUT ÖZHAN | 2019 | The effects of information security domains on reputation of financial institutions | YL |
| **153** | 592932 | SEVİLAY BEKEN | 2019 | An information security risk assessment model based on Bayesian networks and fuzzy inference system | YL |
| **154** | 612885 | EZEL TEKER | 2019 | Öğretmenlerin ve lise öğrencilerinin bilgi güvenliği farkındalık düzeylerinin değerlendirilmesi | YL |
| **155** | 581788 | FATİH YILMAZ AKAN | 2019 | Havacılık sektöründe bilgi teknolojileri uygulamaları ve bilgi güvenliği inceleme detayı: Yer hizmetleri (Ground handling) | YL |
| **156** | 605851 | GÖKHAN ÖZASLAN | 2019 | Bilgi güvenliği ve mahremiyetin korunmasına yönelik eğitimin etkilerinin değerlendirilmesi: Bir özel hastane uygulaması | YL |
| **157** | 586385 | RAHİME HACIMUSTAFAOĞLU | 2019 | Ortaöğretim öğrencilerinin bilgi güvenliği farkındalık düzeylerinin siber mağdur olma durumlarına etkisinin incelenmesi (Üsküdar örneği) | YL |
| **158** | 588095 | MERVE ÜNVER | 2019 | Türkiye'de insan kaynakları yönetiminde bilgi güvenliği uygulamaları | YL |
| **159** | 557979 | HACER ÖZGE KURT | 2019 | Kurumlarda bilgi güvenliği yönetimi: Hastane bilgi sistemleri üzerine bir araştırma | YL |
| **160** | 607246 | AYŞE ÖZDEMİR | 2019 | Kamu kurum ve kuruluşlarında bilgi güvenliği farkındalığı | YL |
| **161** | 566816 | SULTAN GÜLER KURT | 2019 | Bilgi güvenliğinin bilgi işlem çalışanları tarafından değerlendirilmesi – Sağlık sektöründe bir çalışma | YL |
| **162** | 584130 | CAN GENÇ | 2019 | Kişisel verilerin korunması kapsamında bilgi güvenliği farkındalığı analizi ve e-devlet yapısının incelenmesi | YL |
| **163** | 556960 | TÜLAY GÜRSEL | 2019 | Sigorta şirketlerinde bilgi güvenliği yönetim sistemi denetimi | YL |
| **164** | 597346 | MEHMET TUYGUN | 2019 | ISO27001 bilgi güvenliği yönetim sistemi standardının kamu | YL |

| SIRA | TEZ NO | YAZAR | YIL | TEZ ADI | TEZ TÜRÜ |
|---|---|---|---|---|---|
| | | | | kurumlarına uygulanabilirliğinin araştırılması: Ankara ili örneği | |
| **165** | 622530 | ZEYNEP ASLAN | 2019 | Hemşire akademisyenlerin bilgi güvenliği farkındalık düzeylerinin ve etkileyen faktörlerin belirlenmesi | YL |
| **166** | 586587 | CANSU ALTUNSABAN YERLİKAYA | 2019 | Bilgi güvenliğine yönelik öğrenci, öğretmen, veli ve okul yöneticilerinin farkındalıklarının incelenmesi | YL |
| **167** | 586342 | NURHAN KARAYÜCEL EFE | 2019 | Ondokuz Mayıs Üniversitesi öğretmen adaylarının bilgi güvenliği farkındalıklarının bazı değişkenler açısından incelenmesi | YL |
| **168** | 569451 | SELMA BARAN | 2019 | Örgütsel bilgi paylaşımının bilgi güvenliği üzerine etkisinin incelenmesi | YL |
| **169** | 591903 | İLKNUR TUNCER | 2019 | Bilgi güvenliği açısından bir değerlendirme: E-devlet uygulamaları | YL |
| **170** | 584383 | GÜLHAN DÖNMEZ | 2019 | Lise öğrencilerinin bilgi güvenliği farkındalığı ile dijital okuryazarlığı arasındaki ilişkinin incelenmesi | YL |
| **171** | 607137 | HALİME CEYLAN | 2019 | Türkiye'de bilgi güvenliği algısının istatistiksel analizi | YL |
| **172** | 598695 | KÜBRA ASLAN | 2019 | Performance evaluation of iot data security on cloud computing | YL |
| **173** | 592784 | AHMET GÜÇLÜ | 2019 | Sosyal ağ platformlarında kullanıcı sözleşmelerinin veri güvenliği açısından incelenmesi:Facebook ve Google örneği | YL |
| **174** | 564017 | HATİCE KÜBRA KOÇ | 2019 | Biyometrik tanı yöntemlerinde kişisel veri güvenliği arttırılmış sistem tasarımı | YL |
| **175** | 650102 | SAYED OSMAN SAYEDI | 2020 | Ulusal siber güvenlik stratejisi oluşturma süreç analizi ve Türkiye ile Afganistan'ın ulusal siber güvenlik stratejisinin değerlendirilmesi | YL |
| **176** | 653929 | EFE DÜVEROĞLU | 2020 | A comparative analysis of critical infrastructure cyber security policies: Best practices from the US, EU and Turkey | YL |
| **177** | 619071 | AYBARS ORUÇ | 2020 | Cybersecurity risk assessment for tankers and defence methods | YL |
| **178** | 636553 | ENGİN SAVÇIN | 2020 | Devletlerin siber güvenlik politikalarının şekillendirilmesi sürecinde kamu-özel sektör işbirliğinin artan önemi: İsrail ve Yeni Zelanda örnekleri | YL |
| **179** | 647487 | MUSTAFA ŞENOL | 2020 | Türkiye'nin ulusal siber güvenlik strateji ve politikalarının oluşturulması çerçevesinde caydırıcılık | DR |

| SIRA | TEZ NO | YAZAR | YIL | TEZ ADI | TEZ TÜRÜ |
|---|---|---|---|---|---|
| **180** | 612990 | GÜLÜZAR CANSU ERGÜR | 2020 | Uluslararası marka bilinirliği açısından uluslararası pazarlama stratejileri: Bilişim sektörü (siber güvenlik) firmaları üzerine bir araştırma | YL |
| **181** | 609359 | SEMİH POLAT | 2020 | Milli güvenlik açısından siber güvenlik | YL |
| **182** | 648535 | FİRDEVS SÜMEYYE CEBELOĞLU | 2020 | Endüstri 4.0 sistemlerinde yapay zekâ tabanli siber güvenlik yaklaşimlarinin geliştirilmesi | YL |
| **183** | 653998 | CEMAL ARAALAN | 2020 | Teknik ve hukuki boyutlarıyla elektronik ödeme sistemlerinde siber güvenlik | YL |
| **184** | 637272 | GÖKHAN ALGAÇ | 2020 | Siber güvenlik alanında düzenlenen uygulamalı öğretici CTF yarışmalarında kullanılan programlara genel bir bakış | YL |
| **185** | 626390 | İDRİS YIKICI | 2020 | Siber teknolojilere dayalı yeni uluslararası güvenlik konsepti bağlamında Türkiye'nin siber güvenlik stratejisi | YL |
| **186** | 633219 | ONUR TOPAL | 2020 | Denizcilikte siber güvenlik: Türk gemi işletmecileri üzerine bir inceleme | YL |
| **187** | 626407 | ORHAN MURATOĞLU | 2020 | Akıllı araçlar için bulanık mantık temelli siber güvenlik risk modeli | DR |
| **188** | 635938 | BUĞRAHAN EMİR | 2020 | Uluslararası ilişkilerin kuramsal çerçevesi ve siber güvenlik kavramının analizi | YL |
| **189** | 659129 | FİKRİ GÜNEŞ | 2020 | Kitlesel açık çevrimiçi ders platformlarında yayınlanan siber güvenlik içeriklerinin çoklu ortam tasarım ilkeleri açısından incelenmesi | YL |
| **190** | 629320 | MERVE ÇETİN | 2020 | Nükleer tedarik zincirinde en iyi siber güvenlik sistemine sahip ülkenin seçilmesi | YL |
| **191** | 656240 | AHMET KORKUSUZ | 2020 | Kurumlarda siber güvenlik ve siber riskler | YL |
| **192** | 628021 | SUNA ATILGAN | 2020 | Hastanelerde hasta mahremiyetine yönelik hasta veri güvenliği uygulamalarının sağlık çalışanlarının bakış açısıyla değerlendirilmesi | YL |
| **193** | 654097 | ÇİĞDEM BAKIR | 2020 | Dağıtık veritabanı sistemlerinde gerçek zamanlı veri güvenliği: Bilgi akış denetimi | DR |
| **194** | 608772 | KEMAL HAKAN | 2020 | İstemci taraflı şifreleme ve dağıtık depolama ile kişisel veri güvenliğinin arttırılmasına yönelik bulut tabanlı uygulamanın geliştirilmesi | YL |
| **195** | 672684 | MURAT SAMİ BAYKIZ | 2020 | Elektronik finans kullanan küçük ve orta büyüklükteki işletmelerde (kobi) bilgi güvenliği risklerine karşı alınabilecek tedbirler üzerine bir öneri: Bilgi güvenliği odaklı iç | DR |

| SIRA | TEZ NO | YAZAR | YIL | TEZ ADI | TEZ TÜRÜ |
|---|---|---|---|---|---|
| | | | | kontrol ve risk profiline uygun kontrol seçimi | |
| **196** | 632526 | KÜBRA AKTAŞ | 2020 | Iso 27001 bilgi güvenliği yönetim sistemi: Erişim kontrol politikası üzerine bir inceleme | YL |
| **197** | 639263 | TÜLİN FİLİK | 2020 | Tıbbi sekreterlerde bilgi güvenliği farkındalık düzeyinin elektronik sağlık kayıtlarının güvenlik ve mahremiyet uygulamalarına etkisinin değerlendirilmesi | YL |
| **198** | 650063 | AYKUT ALEMDAROĞLU | 2020 | Çalışanların bilgi güvenliği farkındalığına ilişkin algıları: Bankacılık sektöründe bir araştırma | YL |
| **199** | 667787 | CEVDET ÖZMEN | 2020 | Sosyal mühendislik bağlamında bilgi güvenliğinin endüstri 4.0 tabanlı sistemlere uyarlanması | DR |
| **200** | 629345 | MURAT SOLMAZ | 2020 | Öğretmen adaylarının siber bilgi güvenliği farkındalığı ve dijital vatandaşlık düzeylerinin çeşitli değişkenler açısından incelenmesi | YL |
| **201** | 617829 | SEYDA EMİR ERDOĞAN | 2020 | Bilgi güvenliği yönetim sisteminin oluşturulması, IEC/ ISO 27001 standartının bir sivil havacılık kurumunda hayata geçirilmesi | YL |
| **202** | 620913 | DİLAN ŞERİFE ŞİŞKİN | 2020 | Üniversite kütüphanelerinde bilgi güvenliği ve kişisel verilerin korunması: Ankara'daki üniversite kütüphanelerinin değerlendirilmesi | YL |
| **203** | 687543 | EYLÜL AYDIN | 2021 | Study of the cyber security measures: Comparative work of the United States and Turkey | YL |
| **204** | 680362 | ARTRIM KJAMILJI | 2021 | Blockchain driven secure and private machine learning algorithms for post quantum 5G/6G enabled industrial IoT with applications to cybersecurity and health | DR |
| **205** | 672467 | MOHAMMED HASAN HADI AL MAAWI | 2021 | Cybersecurity breaches and the role of ethical hackers in securing the online system of the organisation | YL |
| **206** | 668885 | BERKCAN KARABULUT | 2021 | Büyük ölçekli ağlarda gerçek zamanlı hibrit honeypot sistemi: Türk siber güvenlik sektöründe | YL |
| **207** | 683647 | MUHAMMET OĞUZ | 2021 | Stratejiden Yasaya: Avrupa Birliği Siber Güvenlik Politikası | YL |
| **208** | 676107 | ÖMER BARIŞ | 2021 | Etkin siber güvenlik stratejilerinde yönetim bilişim sistemlerinin yaklaşımları | YL |
| **209** | 692755 | ALEXANDER SEZAİ GÜVEN | 2021 | Türkiye ile Avrupa Birliği'nin siber güvenlik stratejilerinin karşılaştırılması | YL |
| **210** | 655980 | ÖMER DURMUŞ | 2021 | Siber güvenlik önlemlerinin analizi ve modellenmesi | YL |

| SIRA | TEZ NO | YAZAR | YIL | TEZ ADI | TEZ TÜRÜ |
|---|---|---|---|---|---|
| **211** | 669929 | KADİR SEVİNÇ | 2021 | Siber güvenlik ölçeği geliştirme: Geçerlik ve güvenirlik çalışması | YL |
| **212** | 679596 | ÖZGE GÜLEÇ | 2021 | Uluslararası ilişkilerde siber güvenlik kavramı ve uygulamaları | YL |
| **213** | 662447 | ALI MOHAMMED IDAN | 2021 | Ulusal ve uluslararası güvenliğin bileşeni olarak siber güvenlik: Irak örneği | DR |
| **214** | 675185 | OZAN ZEKİ KİRAZ | 2021 | Siber güvenlik bağlamında yeni tehdit algılamalarının Türkiye'nin güvenlik politikalarına etkileri | YL |
| **215** | 668938 | NEVZAT GÜNGÖR | 2021 | İç denetimde bilgi teknolojileri ve siber güvenlik: Borsa İstanbul şirketlerinde bir inceleme | DR |
| **216** | 678929 | BERNA TOZLU | 2021 | Siber güvenlikte sosyal mühendisliğe karşı bir model geliştirilerek test edilmesi | YL |
| **217** | 670567 | HÜSEYİN SİNAN OCAK | 2021 | İç denetimin gelişen ve değişen dünyasında: Siber güvenlik ve denetim | YL |
| **218** | 680187 | İBRAHİM AKDAĞ | 2021 | Siber güvenlik ve Türkiye: Örgütsel yapı, uygulamalar ve gelecek | DR |
| **219** | 697620 | İMREN ALTINER | 2021 | Öğretmenlerin kişisel siber güvenlik farkındalık düzeylerinin farklı değişkenlere göre değerlendirilmesi | YL |
| **220** | 688474 | ABDUL MUNAM ALHAMEED | 2021 | Data security and protection in electronic commerce management | YL |
| **221** | 669281 | ONUR KORUCU | 2021 | Veri güvenliğinin iyileştirilmesi sürecinde risk tabanlı küresel standart, çerçeve ve en iyi uygulama yaklaşımları | YL |
| **222** | 675610 | ASMAA EL KHATIB | 2021 | The outbreak of COVID-19: A wakeup call to explore information security policies, training and awareness from teleworkers' perspective in the context of Saudi Arabia | YL |
| **223** | 689656 | TUĞBA ÇELİK | 2021 | Bilgi güvenliği yönetim sistemlerinin belgelendirilmesi: Batı Karadeniz'de bir alan araştırması | YL |
| **224** | 692223 | ALİ EREN | 2021 | Bilgi güvenliği yönetim sisteminin yükseköğretim kurumlarında sürdürülebilirliğinin incelenmesi | YL |
| **225** | 679722 | BAŞAK ÖZEN SERTER | 2021 | Ortaokul öğrencilerinin bilgi güvenliği farkındalık düzeyinin belirlenmesi | YL |