
MÜHENDİSLİK FAKÜLTESİ

SİBER GÜVENLİK YÜKSEK LİSANS BÖLÜMÜ

TEZSİZ YÜKSEK LİSANS DÖNEM PROJESİ

# SİBER GÜVENLİKTE YAPAY ZEKÂ



HAZIRLAYAN

NİHAT TUNÇ

DANIŞMAN ÖĞRETİM ÜYESİ
Doç.Dr. Dr. Recep BENZER

2022

## ETİK İLKELERE UYGUNLUK BEYANI

Dönem proje yazma sürecinde bilimsel ve etik ilkelere uyduğumu, yararlandığım tüm kaynakları kaynak gösterme ilkelerine uygun olarak kaynakçada belirttiğimi ve bu bölümler dışındaki tüm ifadelerin şahsıma ait olduğunu beyan ederim.

İmza
Nihat TUNÇ

# SİBER GÜVENLİKTE YAPAY ZEKÂ

**Nihat TUNÇ**

**AHMET YESEVİ ÜNİVERSİTESİ**

**SİBER GÜVENLİK YÜKSEK LİSANS BÖLÜMÜ**

**2022**

## ÖZET

Güncel olarak çok sayıda kurum, oldukça önemli bir yere sahip olan siber güvenliklerini daima geliştirmek ve arttırmak adına yapay zekâ tabanlı siber güvenliğe gereksinim duymaktadır. Teknolojik açıdan yapay zekâ, siber güvenlik için sistemsel savunmayı geliştirirken siber güvenliğin farklı bir tarafı olan saldırı yöntemlerinin de iyileştirilmesi ve süreçlerin giderek kısalmasında oldukça önemli bir yere sahip olmaktadır. Buradaki çalışma; siber güvenliğin sağlanabilmesi için yapay zekanın sunabileceği faydalar ve olanaklar ekseninde ele alınmaktadır. Özel firmalar ile ilgili yapılmış olan araştırmalardan elde edilen sonuçlara bakıldığı zaman, siber güvenlik ve siber saldırının iyileştirilmesi, geliştirilmesi ve arttırılması adına yapay zekaya gereksinim hissetmeye başlandığı gözlemlenmektedir. Çalışmanın esas amacı, devletler adına oldukça büyük öneme sahip, ulusal anlamda güvenlik riski olarak bakılan siber güvenlik hususu için, yapay zekanın sağladığı avantajların tekrar değerlendirilmesidir.

**Anahtar Kelimeler:** Yapay Zekâ, Siber Güvenlik, Siber Saldırı, Sistemsel Savunma.

**Danışman:** Doç. Dr. Recep Benzer

# ARTIFICIAL INTELLIGENCE IN CYBER SECURITY

**Nihat TUNÇ**

**AHMET YESEVI UNIVERSITY**

**CYBER SECURITY**

**2022**

## ABSTRACT

Currently, many institutions need artificial intelligence-based cyber security in order to always improve and increase their cyber security, which has a very important place. In terms of technology, artificial intelligence has a very important place in improving the system defense for cyber security, improving attack methods, which is a different side of cyber security, and shortening the processes. The study here; In order to provide cyber security, the benefits and possibilities that artificial intelligence can offer are discussed. When looking at the results obtained from the researches on private companies, it is observed that artificial intelligence has begun to be felt in order to improve, develop and increase cyber security and cyber attack. The main purpose of the study is to re-evaluate the advantages of artificial intelligence for the issue of cyber security, which is of great importance for states and is considered a national security risk.



**Keywords:** Artificial Intelligence, Cyber Security, Cyber Attack, Systemic Defense.

**Advisor:** Assoc. Prof. Recep BENZER

# İÇİNDEKİLER

## SİMGELER VE KISALTMALAR

**GPS** : Küresel Konumlama Sistemi

**GPU** : Grafik İşlemci Birimi

**LISP** : Liste İşleme

**USDDCS** : ABD Savunma Bakanlığı Siber Stratejisi

**vb.** : ve benzeri

**vd.** : ve diğerleri

# BÖLÜM I

## SİBER GÜVENLİK KAPSAMINDA YAPAY ZEKÂ KULLANIMI

Siber Güvenlik ya da Siber Savunma kavramı, siber tabanlı ortamda kullanıcı, kuruluş ve kurumların varlıklarını güven altında tutmak hedefiyle kullanılan teknolojiler, araçlar, eğitimler, politikalar, kılavuzlar, güvenlik ile ilgili teminatlar, faaliyetler, güvenlik ile ilgili kavramlar ve risk yönetimi için kullanılan görüşlerin tümüdür (Ünver vd., 2009). Siber ortamda yapılan saldırı girişimlerinde risk teşkil eden ve düşman olarak görünen hedefe, karşı saldırıya geçmek, karşı güvenlik savunmasını uygulamaya koymak, hedefte bulunan siber uzay dahilinde istihbarat ile ilgili verileri elde etmek siber savaş ile ilgili uygulamaları oluşturmaktadır.

Siber ortamda gerçekleştirilen savaşların esas amacı; ülkelerin kamusal hizmet, güvenlik, bankacılık, enerji, su, haberleşme ve ulaşım benzeri kritik alanda yer alan sektörlerinin bilgi sisteme dayalı temelleridir. Siber ortamda saldırı; dünya üzerinde herhangi bir bölgede, bilgisayar kontrolü kapsamında yer alan sistemlere, internet aracılığıyla izin olmadan ulaşıp kritik alanda bulunan alt yapıları ele geçirerek, yönetime hâkim olmaya çalışmaktır. Siber ortamdaki saldırıya karşı kullanılacak silahlar ise; temeli internet ortamına dayalı herhangi bilgisayarın tuşları, yazılımlar ve bilgisayarda yer alan tuşları kullanan parmaklardır (Karakuş, 2013).



Etkili özelliklere sahip ağlarda, siber ortamda yapılan saldırı halinde, bütün alt yapı kısa bir zaman içerisinde bozulabilmekte, bu konularla ilgili en kuvvetli ülkeler dahi ilerleyemez duruma gelebilmektedir. Etkin olan ağlarda, aktif biçimde gelişen saldırılardan korunabilmek için klasik ve sabit niteliklere sahip algoritmalar doğrultusunda yazılım oluşturmak zordur. Bahsi geçen durum, ancak öğrenme becerisi sunan ve yazılımsal esnekliği sağlamakta olan yapay zekaya dair tekniklerin faaliyete geçirilmesiyle yürütülebilmektedir (Şenkaya ve Adar, 2014).

Bilgisayar sistemlerinde rastlanılan çok sayıda saldırı çeşidi bulunmaktadır. İçeriğin değiştirilmesi, sistemin kesintiye uğratılması, verilerin bozulmasını sağlama ya da verileri çalma ve erişim kısıtlaması benzeri çok sayıda hedef konarak saldırılar düzenlenmektedir. Hizmette kesintiye uğratma saldırısı, sistemin aşırı talep sonucu yanıt veremeyecek duruma

gelmesine sebep olan saldırılardır. İzinsiz ya da yetkisiz erişim doğrultusunda gerçekleştirilen saldırılar, keylogger ya da parola kırıcılar benzeri araçlar kullanılarak sürdürülen ve bilgiyi açığa çıkaran saldırılardır.

Ağ ya da bilgisayar sistemlerine karşı gerçekleştirilen saldırıları belirleyerek güvenli bir ortamın oluşturulabilmesi adına geliştirilen ve iyileştirilen sistemler, gerçekleştirilen saldırıların genelini belirleyebilme kabiliyetine sahip olsalar dahi, geçmişten şimdiye dek hiç rastlanılmamış olan saldırıların genelinin tespitini yapamamaktadır (Sağıroğlu vd., 2011). Bahsi geçen saldırıların, sistemler üzerinde büyük tahribatlara sebebiyet vermesi, yeni niteliklere sahip saldırı türlerinin belirlenebilmesi, hızlı bir biçimde değişiklik gösteren saldırı çeşitleri için bilgisayar ve bilgi güvenliğinin oluşturulabilmesi hedefiyle sistemlerin geliştirilmesi ve iyileştirilmesinde yapay zekâ tekniklerinin kullanılması amaçlanmaktadır.

Saldırıyı belirlemeye dayalı sistemlerde, gerçekleştirilen saldırının belirlenmesine yönelik iki çeşit teknik kullanılmaktadır. Bu teknikler şu şekildedir (Yıldırım vd., 2014):

1. Kötüye kullanıma yönelik belirleme tekniği.

2. Anormallik durumuna yönelik belirleme tekniği.

Anormallik durumuna yönelik belirleme tekniği; sistem dahilindeki kullanıcıların tutum ve davranışları ile ilgili modelleme yapmaktadır. Kötüye kullanıma yönelik belirleme tekniği ise; Saldırganların tutum ve davranışları ile ilgili modelleme yapmaktadır



Saldırıların bilinmesi ve çok daha önceden belirlenmesi, bunun yanı sıra gerçekleşebilecek saldırılar hakkında ön görülerde bulunarak uyarı alarmı iletmesi yapay zekâ ve veri madenciliğine dayalı teknikler doğrultusunda sağlanabilmektedir. Zeki niteliklere sahip yaklaşımların kullanılmasıyla beraber anormallik durumuna yönelik belirleme tekniği biraz farkla daha öne çıkmış, bu sebeple anormallik durumuna yönelik belirleme tekniğinin yeni nitelikleri barındıran saldırıları ön görebilme ve belirleyebilme becerisi güçlendirilmiştir. Yapay zekâ ile ilgili çalışma yapmakta olan araştırmacıların en başından beri ulaşmayı talep ettiği yer, insana benzer biçimde davranan ve düşünen sistemler oluşturmak ve bu sistemleri geliştirmektir.

Son senelerde, ağ ile ilgili teknolojilerde yaşanmakta olan oldukça önemli gelişmeler, neredeyse tüm işlerin bilgisayar kapsamındaki ağlar sayesinde yapılabilmesini mümkün kılmıştır. Bilgisayar ağları ve bilgisayar sistemlerinin iyileşmesi ve gelişmesi ile uluslararası kapsamda ticaret faaliyeti yapmak, aya insanın gitmesini sağlamak, pilotsuz olan uçakları savaştırmak gibi oldukça güç işler, mümkün ve yapılabilir bir duruma gelmiştir. Ancak tüm bu olanaklara ve avantajlara karşın insanlar, bilgisayar ağ ve sistemlerine tam anlamıyla güvenememektedirler. Güvensizlik durumunun esas sebebinde ise bilgi-işlemin gerçekleştirilebilecek saldırılar karşısında tümüyle başarı gösterememesi bulunmaktadır. Güvenliğin tam anlamıyla sağlanabilmesi, güçlü temellere dayalı ve sağlam bir altyapı ile mühendislik gerektirmektedir (Takcı, 2021).

Ağlar doğrultusunda gelen saldırıların belirlenebilmesi için imza tabanına dayanan saldırı tespit tekniği ve anormal duruma dayanan saldırı tespit tekniği olmak üzere 2 adet esas teknik kullanılmaktadır. İmza tabanına dayanan saldırı tekniğinde; veri tabanında bulunan yani eskiden karşılaşılmış olan saldırılara dair imzalar kullanılmaktadır. Bu teknikteki en önemli sorun; kullanılan imzaların saldırganlar doğrultusunda değiştirilebilmesinin mümkün olmasıdır. Bu sebeple daha önce karşılaşılmış olan saldırıları belirlerken oldukça iyi sonuçlar doğurabilmesine karşın veri tabanında daha önce rastlanılmamış saldırı türlerini belirlemekte yetersiz durumdadır.

Anormal duruma dayanan saldırı tespit tekniği ise; şüpheli ve riskli olan ağ trafiği ile normal durumdaki ağ trafiğini birbirlerinden ayırt edebilecek yöntemlere sahip olmaktadır. İlk adıma hangi ağ trafiğinin normal durumda olduğunun tanımlanması yapılarak başlanır, ardından gelecek olan ağ paketleri daha önceden tanımlananlara göre anormal ya da normal saldırı çeşidi olarak sınıflandırmaktadır (Özen ve Mert, 2018). Buradaki iki adet yaklaşım da en az daha önceden bilinmekte olan saldırıların belirlenmesi kadar bilinmeyenleri de belirleyebilmektedir. Bu durumdan dolayı, ağ trafiğinde gerçekleşen saldırıların belirlenebilmesi için anormal durumları saptamak için makine öğrenmesi temelli sistemlerin daha sık kullanılması günümüzde oldukça büyük bir öneme sahip olmuştur.



### 1.1. Problem

İlkçağlardan beri insanların en temel ihtiyaçlarından biri güvenlik ihtiyacı olmuştur. Nitekim tarihsel süreç içerisinde bu ihtiyacın karşılanması hususu sürekli olarak revize edilmiştir.

Günümüzde kullanılmakta olan teknolojik imkanlar ile gerçek ve sanal birbirine karışmış; soyut ile somut arasındaki algısal farklılık giderek azalmıştır. Siber güvenlik kavramı güncel teknolojik gelişmelerden kaynaklı olarak meydana gelmekte olan tehlikeleri bertaraf etme amacıyla kurgulanmaktadır. Siber güvenlik için gerekli olan en önemli husus verilerin doğru ve etkili bir biçimde tasnif edilmesi, verilerin birbirleriyle olan ilişkilerinin sistematik bir şekilde kurulması; aynı zamanda da minimum risk ile depolanmasıdır. Bundan dolayı da yapay zekanın siber güvenlik ağlarında kullanılmaya başlanması söz konusu olmuştur. Bu bağlamda gerçekleşmekte olan çalışmanın problemi yapay zekâ ve siber güvenlik arasındaki ilişkilerin geçmişten günümüze nasıl şekillendiği esasına dayandırılmaktadır.

### 1.2 Araştırmanın Amacı

Bu çalışmanın amacı; siber güvenlik alanında oldukça etkin bir rolü olan yapay zekanın sistem içerisindeki yerinin ve ilişkisinin sistematik bir şekilde birincil kaynaklara dayandırılarak açıklanması, tarihsel gelişimlerinin irdelenerek gelecek kurgusuna zemin oluşturulması olarak açıklanabilmektedir.

### 1.3. Araştırmanın Önemi

Bu çalışma güncel teknolojik gelişmelere kavramsal bir temel oluşturması bakımından önem arz etmektedir. Çalışmanın sistematiği ekseninde kavramlar arası ilişkilerin kurulması ve bu bağlamda kavramlar arası bütünlüğün alan yazına kazandırılması bakımından da önemli bir yere sahiptir.



### 1.4. Sayıltılar

Bu çalışmada; gerçekleştirilmekte olan alan yazını analizlerinin tam olarak doğru sonuç verdiği ve kullanılan kaynakların objektif aynı zamanda şeffaf bilgiler sunmakta olduğu varsayımı ile hareket edilmiştir.

### 1.5. Sınırlılıklar

Bu çalışmadaki sınırlılıklar;

- Referans erişimi sürecinde üyelik istemekte olan e-arşivlerin çalışma dışında bırakılması,
- Bir adet veri toplama aracı (sistematik tesadüfi örnekleme) kullanılması,

olarak ifade edilebilmektedir.

### 1.6. Tanımlar

*Güvenlik:* Bireylerin ve bireylerden oluşan toplumların kazalardan ve tehlikelerden korunması anlamına gelmektedir.

*Siber Güvenlik:* Kişisel ya da toplumsal olması fark etmeksizin elektronik bilgi akışının ve depolanmasının belirli yasal çerçeve dahilinde korumasıdır.

*Zekâ:* Düşünme, gerçekleri sezme, algılama, yargılama ve bir sonuca bağlama noktasında sergilenmekte olan kabiliyetlerin bütününe zekâ denmektedir.

*Yapay Zekâ:* içerisinde kodlanmış olan görevleri ifa edebilmek için insan zihnini taklit eden bir sistemdir.

# BÖLÜM II
# KAVRAMSAL OLARAK SİBER GÜVENLİK VE YAPAY ZEKÂ

Bu bölüm içerisinde siber güvenlik ve yapay zekâ tanımları ekseninde tarihsel gelişimlere ve kavram özelliklerine yer verilmiştir**.**

## 2.1. Siber Güvenlik Kavramının Tanımı

Siber güvenlik, betimlemesi fazlaca değişken bir kavramdır. Genel olarak öznel özelliklere sahiptir. Bazı durumlarda bilgilendirici bir işlev taşımamakla birlikte, yaygın bir biçimde kullanılmaktadır. Siber güvenlik kavramının geniş yelpazesini kapsayan, ayrıntılı boyutlara değinen, özlü ve benimsenebilir herhangi bir betimlemesini yapabilmek oldukça güçtür. Bu durum, siber güvenlik kavramının yoğun olarak yöntemsel tarafını kuvvetlendirirken, eş zamanlı olarak teknolojik bağlamda siber güvenlik ile ilgili güçlükleri çözebilmek adına beraber adım atılması gereken disiplinleri birbirinden ayırmaktadır (Akyeşilmen, 2018).

Yine betimlemesinin kısıtlı kalması durumu, siber güvenlik ekseninde gelişen bilimsel ve teknolojik açıdan ilerleme adımlarına da engel olmaktadır. Siber güvenlik ile alakalı yapılmış olan çalışmalar; sosyoloji, bilgisayar bilimi, eğitim, mühendislik, yönetim, siyasi çalışmalar, güvenlik çalışmaları ve psikoloji benzeri çok sayıda akademik disiplini de kapsayan oldukça geniş boyutlara sahip bir kaynak yelpazesinde yerini almıştır.



Ancak, Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020)'e göre; siber uzayı ortaya çıkaran bilişim sistemlerinin, herhangi bir gerçekleşebilecek saldırıdan korunmasını, buradaki alanda işlenen verinin ya da bilginin erişebilirliği, gizliliği ve bütünlüğünün koruma altına alınmasını, siber olayların ve saldırıların belirlenmesini, yapılan belirlemeler için tepki mekanizmalarının aktifleştirilmesini, daha sonra da sistemlerin gerçekleştirilen siber saldırıdan hemen önceki pozisyonlarına döndürülmesini sağlayan uygulamaların tümüne "siber güvenlik" denmektedir.

Siber güvenlik kapsamında birbiriyle ilişkili pek çok söylem yer almaktadır. Siber güvenliğin tekrar yapılandırılması, yaşanan tartışmaların bazen "*siber*" bazen de "*güvenlik*" dahilinde konumlandırılmasına yarar sağlayacaktır. "*Siber*" kelimesi eskiden ortaya çıkışı, betimlemesi yapılmış olan siber uzay kavramını, bağlantılı terimlerle bir bütün haline

getirmektedir. Güvenlik kavramının yeni niteliklere sahip betimlemesinin önüne siber ortamı yansıtan siber kelimesi getirilerek, bahsi geçen iki alanda da problem ve yenilikleri bütün haline getiren bir terim özelliği taşıyan siber güvenlik mefhumu ortaya çıkmıştır (Craigen vd., 2014).

### 2.1.1. Siber Tehditler Ekseninde Siber Güvenlik Kullanımı

İletişimin ve internetin imkanlarının çoğalmasıyla beraber saldırganlar için saldırılabilecek çok daha fazla sistem var olmuştur. Bahsi geçen saldırıların oldukça büyük bir kısmı kullanılmakta olan sistemin eksiklikleri ya da kusurlarından yararlanılarak yapılmaktadır. Bu tarz saldırı hareketlerini engelleyebilmenin 2 tane yolu bulunmaktadır. Bu yollardan birincisi; tam anlamıyla güvenli bir ortam ya da bir sistem yaratmaktır. İkincisi ise; gerçekleştirilebilecek saldırıları belirleyip gerekli olan önlemleri önceden almaktır. Bahsi geçen yöntemlerden birincisi pratik bakımdan pek de mümkün değildir. Bu durumun sebepleri ise (Sundaram, 1996);

- Kullanılmakta olan işletim sisteminde bulunan açık, kusur ve hataları genelde öncelikle saldırganların fark etmesi ve bu açık, kusur ve hatalarla ilgili önlemler alınana dek kullanılmaya devam edilebilmeleri,

- Verilerin iletimi amacıyla kullanılmakta olan protokollerin temelinde bulunan kimi kuralların saldırı gerçekleştirebilme hedefiyle kullanılabilmesi,

- Kriptografik özelliklere sahip yöntemlerin ve bu yöntemlerin anahtarlarının kırılabilmesi,

- Aktif olan kullanıcıların parolalarını unutabilmesi,

- Oluşturulmuş olan kripto-sistemin ele geçirilebilmesi ve bu sebeple yüksek düzeyde güvenli ortamların oluşturulamaması,

- Dış güçlere karşı güvenlik sistemi oluşturulan düzenin, iç ortamlardan bozularak güvenli ortamın etkisiz hale getirilmesi,

- Güvenliği sağlayabilme hedefiyle aktif kullanıcı yetkilerinin en alt seviyeye indirgenmesi neticesinde aktif kullanıcıların verimliliğinin azalması olarak sıralanabilmektedir.

Sistemlerini güvenli bir ortam dahilinde korumak isteyenler, genellikle herhangi bir saldırı gerçekleşene dek bekleme halinde kalmak, bahsi geçen saldırı gerçekleştirildiğinde ise oldukça hızlı bir biçimde tespitini yapmak istemektedir. Bu durum siber güvenliğin kapsamına ait bir iş olmaktadır. Herhangi bir siber saldırının hangi porttan ya da hangi adresten yapıldığını bulmadan, bu saldırıya engel olabilmek mümkün olmamaktadır. Siber güvenliğe ait yöntemler doğrultusunda gerçekleştirilen saldırıların tespiti yapılırken bahsi geçen bilgilere de ulaşılmaktadır.

Yapay zekâ doğrultusunda oluşturulmuş olan siber güvenlik yöntemleri, ayrıntılı bir biçimde ulaştığı ve depolamış olduğu bilgilerden faydalanarak, gerçekleşen saldırıları oldukça çabuk belirleyebilme niteliğine sahiptir. Elde edilmiş olan aynı bilgilerin analiz edilmesi doğrultusunda geçmişten bu yana hiç rastlanılmamış herhangi bir saldırı girişimini dahi belirleyebilmektedir (İftikhar ve Alghamdi, 2009).

Uluslararası ilişkiler alanının temelinde süregelen tartışma konularından biri güvenliktir. Çok sayıda görüş ve kapsam açısından güvenlik kavramına verilen manalar değişiklik göstermektedir. Siber uzayın gün geçtikçe hızlı bir biçimde büyümesi ve gelişmesiyle birlikte, güvenlikle ilgili yapılan tartışmalara, yeni niteliklere sahip bir anlam kazandırılmıştır. Uluslararası kapsamdaki politika unsurlarına, siber uzay tarafından, klasik yaklaşımlardan oldukça farklı, daha değişken ve daha hızlı tehditler, fırsatlar ve avantajlar sunulmaktadır.



Genellikle siber uzay, internete dayalı ve birbirlerine bağlı bilgisayar sistemleri ile buradaki sistemler dahilinde depolanan, aktarılan ve kullanılan bilgilerin güvenliğini içeren bir kavramdır (Kramer, 2009). Bu özelliği doğrultusunda bir anlamda internet kabloları, ağları ve bilgisayar benzeri donanımsal eksende ulaşımın sağlanabildiği sanal nitelikli bir ortam ya da gerçeklik olduğu söylenebilmektedir. Bahsi geçen sanal gerçeklik ortamı, yeni bilinen bir kavram değildir. 20. yüzyılın başlarında yürütülen çalışmalar genellikle devletlerin savaş ile ilgili stratejileri ve askeri istihbaratlarıyla bağlantılıdır.

20. yüzyılın sonlarına doğru ise internet ağlarına bağlanan kullanıcıların artışı, şahsi olan bilgisayarların piyasaya çıkarılmasıyla birlikte internetin yaygınlık kazanması, özel sektör ekseninde oldukça önem gösteren bir pazar sahası oluşturmuştur. Güncel olarak ise siber uzay, genellikle özel sektör firmalarının etkisi altında gelişimini sürdürürken devletler adına da egemenliğin hâkim olduğu bir ortam olarak görülmektedir. Bundan dolayı siber güvenlik ile alakalı çalışmalar, devletlerin kimi zaman ulusal kapsamlı güvenlik hususları kimi zaman da egemenlik hususları adına kritik bir öneme sahiptir (Horowitz vd., 2018).

Siber ortamda çok çeşitli saldırılar gerçekleştirilebilmektedir. Bu saldırılar özetle şu şekilde sıralanabilmektedir (Akdağ, 2021):

1. Zararlı özellikler içeren yazılımlar,

2. İnternet sitelerinde ya da uygulamalarda bulunan açıklık, eksiklik ve kusurlara yönelik gerçekleştirilen saldırılar,

3. Kimlik avı ve oltalamaya yönelik saldırılar,

4. Servis dışı durumda bırakmaya yönelik saldırılar,

5. Veri hırsızlığına yönelik saldırılar.

Siber ortamda çok çeşitli saldırıların gerçekleştirilebildiği gibi bu saldırıları gerçekleştiren ya da gerçekleştirmeye yönelik risk oluşturan yani siber tehdide sebep olan aktörler de bulunmaktadır. Siber tehdide sebep olan aktörleri ise şu şekilde sıralamak mümkündür (Akdağ, 2021):

- Ulus devlet özelliğine sahip olanlar,

- Daha önce siber ortamda suç işlemiş olanlar,

- Hacktivist bireyler,

- Siber ortamda bulunan teröristler,

- İleri düzeyde bilgiye sahip hacker grupları,

- Kurum içerisindeki tehditler.

### 2.1.2. Siber Savunma ve Siber Güvenlik Ölçüleri

Oluşturulacak herhangi bir siber savunmaya yönelik sistem, siber güvenliği minimum 3 ölçüde sağlamalıdır. İlk ölçü, kimlik doğrulama ve kimlik, erişim kontrolü, kriptografik koruma, ağ filtreleme, denetim benzeri klasik boyutlu statik özellikli siber savunma yöntemlerini kapsamaktadır. İkinci ölçü; güvenlik ile ilgili değerlendirme, saldırı durumu, bilgi elde etme, ağ durumunu gözlemleme benzeri proaktif özellikli siber savunma yöntemlerini kapsamaktadır. Üçüncü ölçü; optimal ya da uygun savunma yöntemlerinin belirlenmesini, ağ durumunun tümüyle analiz edilmesini, uygun ya da optimal savunma yöntemlerinin adaptasyonunun sağlanmasını sağlayan yöntemleri kapsamaktadır (Kotenko, 2007).

Bahsi geçen siber güvenlik ölçülerinin sağlanması için bünyesinde, yapay zekaya dayalı teknolojik sistemleri de barındıran saldırı önleme, saldırı tespit ve erken uyarı sistemleri oldukça önemli bir yere sahiptir. Ciddi öneme sahip siber saldırılara karşı verimli ve olabildiğince etkin, karşı siber savunma oluşturabilmek için saldırı önleme ve saldırı tespit etme sisteminin belirli niteliklere sahip olması gerekmektedir. Buradaki nitelikler şu şekilde sıralanabilmektedir (Patel vd., 2010);



- Gerçekleştirilen siber saldırı sürerken ya da bu siber saldırının hemen ardından gerçek zamanla eş biçimde saldırıya yönelik tespit oluşturabilmek,

- Yanlış uyarı alarmlarını en aza indirgemek,

- İnsan elinden yapılan gözetimi en aza indirgemek ve operasyonların devamlılığını sağlamak,

- Gerçekleşen saldırılardan kaynaklanan ya da kazara olan, sistem dahilinde oluşabilecek herhangi bir zarara karşı sistemin yeniden kurtarılabilirliğini sağlamak,

- Saldırıyı yapan saldırganların sistem içerisinde değişiklik yapmaya yönelik girişimlerinin belirlenebilmesi adına, kendini denetleme becerisine sahip olmak,

- Kullanılan sistemin güvenlik ile ilgili politikalarına uyum sağlamak,

- Zamanla gelişen kullanıcı davranışlarına ve sistemsel değişikliklere uyum sağlayabilmek.

## 2.2. Yapay Zekâ Kavramı

Yapay zekâ kavramı dendiği zaman, insanlarda ilk olarak oluşan düşünce; insana benzer şekilde fikir yürütebilen, insanı direkt taklit yeteneğine sahip olan ya da bir insan beyninin klonlanmasıdır. Bilgisayarların şahsileştirilmesi anlamı da ilk olarak akla gelenlerdendir. Oysa yapay zekâ, türlü sorunları çözerken faydalandığı algoritma bileşenini herhangi bir insanın sorunlara çözüm bulabilme mantığına dayandırmaktadır. Özetle yapay zekâ; herhangi bir bilgisayarın veya bilgisayara bağlı denetimi bulunan herhangi bir makinenin, çoğunlukla insana ait özellikler olarak görülen anlam çıkartabilme, fikir yürütebilme, tecrübe edinilmiş olaylardan öğrenim kazanma ve genelleme benzeri yüksek zihinsel kapsamlarla alakalı verilen görevleri, istenen şekilde yerine getirebilme becerisi şeklinde betimlenebilmektedir (Kalaycı, 2018).

Yapay zekada en çok önem barındıran unsur bilgidir. Elde edilen bilgilerden bir sonuca varılması ve varılan sonucun bir sebebe dayandırılması ise yapay zekanın düşünebilmesine verilebilecek bir örnektir. Bunların gerçekleştirilmesini sağlarken, sorumlu olduğu konuda maksimum seviyede bilgiye ulaşması beklenmektedir. Elde etmiş olduğu bilgileri birleştirir, değerlendirir, sonuca ulaşır ve ulaşılan sonucu da belli bir sebebe bağlamaktadır. Yapay zekanın tarihi de modern nitelikteki bilgisayar bilimine dek eskidir. Yapay zekanın düşünce sahibi, "*makineler de düşünme yetisine sahip olabilir mi?*" sorusunu oluşturan Alan Mathison Turing'dir. Makinelerde de zekâ bulunabileceği konusunu tartışmaya açmıştır (Klein vd., 2010).

Yapay zekâ sisteminin insana benzer şekilde düşünebilmesine verilebilecek en uyumlu misal; Rusya'da düzenlenmiş olan satranç şampiyonasındaki şampiyon olan Kasparov'u yenilgiye uğratan yapay zekânın yaratılmış olmasıdır. Herhangi bir yapay zekâ sisteminin satranç oyununu mantıklı bir şekilde oynayarak, daha önce dünya şampiyonu olan kişiyi

yenilgiye uğratacak olması aslında imkânsız sanılmaktadır. Oysaki bu durum tam anlamıyla gerçekleşmiştir. Bu durumun üç tane temel sebebi bulunmaktadır. Bunlar (Şenkaya ve Adar, 2014):

- Artırılmış ve geliştirilmiş olan bilgisayar gücü,

- Çok iyi düzenlenmiş ve sistemleştirilmiş bir algoritma,

- Olası bütün satranç bilgisine sahip olan çok iyi planlanarak düzenlenmiş bilgi kaynaklarının bulunmasıdır.

### 2.2.1. Yapay Zekâ Kavramının Tarihsel Gelişimi

Walter Pitts ile Warren McCulloch tarafından 1943 senesinde kaleme alınmış yapay zekâ ile alakalı eser, bu konu hakkında tarihte bilinen ilk eser özelliği taşımaktadır. Walter Pitts ile McCulloch kaleme almış oldukları eserlerinde, beyinsel nöronlar ekseninde bir model olarak bulunan yapay nitelikli sinir ağlarına değinmektedirler (McCulloch ve Pitts, 1943). Bahsi geçen gelişmeyle alakalı McCulloch, yapay nitelikli sinir ağı modellemesiyle beraber beyni de modelleyebilmek adına kimi zaman deneysel kimi zaman ise teorik çalışmalar yürütmüş fakat çok da başarı gösterememiştir.

McCulloch bu çalışmasında yapay nitelikli sinir ağlarının yapı taşını ortaya koyduğundan Alan Turing'in ardından yapay zekanın kurulmasında rol oynayan ikinci kişi olarak görülmektedir. Yapay nitelikteki sinir ağları konusu 1970'li senelerde tecrübe etmiş olduğu düşüşten sonra 1980'li senelerin sonlarına doğru tekrar ilgi odağı olarak yükselmeye yüz tutmuştur.

Yapay zekâ kavramının 3. kurucusu olarak sayılabilecek diğer isim ise aynı zamanda Alan Turing ile aynı mesleğe sahip olan ve Alan Turing'in arkadaş çevresinden John Von Neumann'dır. Bununla birlikte Neumann, 1951 senesinde tarihte yapay nitelikli sinir ağına dair özelliklere sahip bilgisayarı yapan Dean Edmonds ve Marvin Minsky'i bu yollarında destekleyerek teşvik etmiştir.

Claude Shannon ise 1950 yılında kaleme aldığı, satranç oyunu oynayabilen zeki niteliklere sahip makinelerle alakalı makalesinde, bu oyun dahilinde bulunan ihtimaller ve mevcut haldeki makinelerle satranç oyununun zamanlarını ölçerek, sezgisel özellikli taramaların uygulamaya konması gerektiğini ifade etmiştir. Yapay zekâ mefhumunu ilk defa kullanmış olan John McCarthy, çabalarıyla birlikte 1956 yılında Dartmouth College bünyesinde bir çalıştay planlayarak, otomat teorisi, yapay nitelikli sinir ağları ve makine zekâsıyla yakından ilgilenen araştırmacıları toplamıştır. Sadece 10 kişinin katılım gösterdiği bu çalıştay doğrultusunda yapay zekâ isminde yeni niteliklere sahip bir bilim oluşmuştur (Stanford, 2019).

Yapay zekanın ilk dönemleri, oldukça büyük bir heyecana ve coşkuya neden olmuştur. Bu bilimle ilgilenen araştırmacılar, birkaç sene öncesine dek, monoton sayısal hesaplamalar yapabilme yetisi olan bilgisayarların, bu yetiden çok daha öteye gidebileceklerini düşünmüşlerdir. Bu düşünceler ise bir hayli yüksek beklentiler içerisine girmeye sebep olmuştur.

Yapay zekâ kavramına isim veren kişi olan John McCarthy, eş zamanlı olarak günümüzde hala kullanılmaya devam eden ve oldukça eski bir programlama diline sahip olan yüksek düzey LISP dilini uzun uğraşlar sonucunda 1958 senesinde geliştirmiştir (Stanford, 2019). Yapay zekâ ekseninde, oldukça büyük beklentilere girilen dönem içerisinde yapay niteliklere sahip sinir ağları ve zeki niteliklere sahip bilgisayarlarla alakalı çalışmalar sürdürülmüş, öğrenme teknikleri ve algoritmaları geliştirilmiştir.



Herbert Simon ve Allen Newell tarafından oluşturulan ve dönemsel açıdan en cesur çalışmalar içerisinde yer alan “Genel Problem Çözücü” isimli proje geliştirilmiştir. GPS, esasen insanların yaşadığı problemleri çözmeye yönelik teknik ve yöntemlerin zeki niteliklere sahip bir makine doğrultusunda simule edilebilmesini hedeflemiştir. Fakat GPS çalışması, karmaşık problemleri çözebilme sürecinde yaşamış olduğu başarısızlık, gereksinim duyduğu bellek boyutu ve bilgi işlem zamanı sebebiyle sona erdirilmiştir (Nilsson, 2019).

Genellikle 1960’lı seneler, sözcüklerle hesaplama, öğrenme algoritmaları, yapay zekâ, sinirsel hesaplama, yapay nitelikli sinir ağları benzeri yeni oluşmuş alanlarda pek çok ışık saçan düşünceye sahip bilim insanlarının, karışık problemleri çözebilmek adına karışık fikir

sistemlerinin simule edilebilmesiyle alakalı genel teknikler ortaya koydukları bir süreç olarak devam etmiştir. Fakat bahsi geçen dönemde yapılmış olan çalışmalar Lotfi Zadeh tarafından kaleme alınan "*Bulanık Kümeler*" isimli makalenin yayına konmasıyla (Zadeh, 1965), bulanık mantığın bulunmasına benzer şekilde faydalarını 20 sene sonra göstermeye başlayacaktır. Yapılmış olan bu çalışma doğrultusunda yol izleyen araştırmacılar, çok sayıda makine ve akıllı sistem geliştirebilmişlerdir.

1970'li senelere dek süregelen dönem içerisinde, düşüncelerin büyük fakat hali hazırdaki bilgisayar teknolojisi özelliklerinin bu düşünceleri uygulamaya koyabilecek kadar iyileşmiş ve gelişmiş olamamaları durumu, yapay zekâ hususunda girilen yoğun beklentileri birçok yönden karşılayamamıştır. Bu durumla birlikte çok sayıda devlet fonu ve projenin iptali gerçekleştirilmiştir. Bunun ardından yapay zekâ ile ilgili alana karşı yoğun ilgi giderek azalmaya yüz tutmuştur.

Yapay zekayla ilgili çalışmalarını sürdürmekte olan araştırmacılar 1950'li senelerin orta dönemlerinden başlayarak 1980'li senelerde çok çeşitli alanda ve tüm hedeflere uyumlu akıllı niteliklere sahip makineler üreteceklerini, bu düşünceyi gerçekleştirebilmek adına insan ölçeğine dayalı veri tabanı yaratacaklarını, bununla da kalmayarak 2000'li senelere henüz ulaşmadan insan zekasını aşacaklarını öne sürmüşlerdir. Fakat 1970'li senelere gelindiği zaman bazı küçük çaplı sorunlarla alakalı makinenin zekâ özelliğinin yanı sıra, karışık, güç ve gerçek dünyayla alakalı bir sorunun çözülmesiyle alakalı en ufak bir gelişme dahi gerçekleşmemiştir (Dendral, 2019).



1960'lı yılların sonlarına doğru yapay zekâ alanı için bazı güçlükler oluşmuştur. Yapay zekaya yönelik çalışmalarını sürdürmekte olan araştırmacılar, çoğunlukla genel kapsamlı problemleri çözebilmeye yönelik adım attıklarından, sorunların çözülebilmesi adına da genel kapsamlı teknikler geliştirmişlerdir. Bu sebepten dolayı, buldukları genel kapsamlı çözümler, sorun alanıyla alakalı oldukça sınırlı alan bilgisine sahip olmaktadır (Allen ve Chan, 2017).

Problemlerin çözülebilmesi adına programlar içerisinden doğru ve uyumlu olanın bulunabilmesine dek birbirinden farklı çok sayıda kombinasyon denemesi gerçekleştirilmiştir. Bu kombinasyon teknikleri doğrultusunda küçük çaplı bazı sorunlar çözüme ulaşabilmiştir. Fakat bu kez de büyük çaplı sorunların çözülebilmesi adına aynı

tekniğin ölçeklendirilmesi sonucunda başarıya ulaşılabileceğine dair yanlış bir düşünce doğmuştur.

Tüm bu uğraşlar sonucunda günümüze kadar çok sayıda gelişme yaşanmıştır. Günümüze daha yakın bir sürece baktığımız zaman; 2012 senesinde yapay zekâ faaliyetlerine gereksinimi olan hızı kazandıran GPU işlemcilerin bulunduğu gözlemlenmektedir. Yapay zekâ alanı için GPU devri başlamış bulunmaktadır. 2014 senesinde akıllı özelliklere sahip ev teknolojilerinde ve çeşitli çok sayıda alanda kullanılmakta olan ses tanımaya yönelik "Amazon Alexa" isimli bir asistan geliştirilmiştir. 2016 senesinde Google DeepMind tarafından geliştirilmiş olan AlphaGo, oldukça karmaşık bir yapıya sahip ve o zamana dek herhangi bir makinenin galibiyet almasının imkânsız olduğunu dile getirilen Go isimli oyunda, daha önce dünya şampiyonluğunu kazanmış olan Lee Sedol, oyun sonunda 4-1 skorla yenilmiştir (Nabiyev, 2016).

Günümüzde de hala yapay zekâ ile ilgili çalışmalar yürütülmektedir. Sonuç olarak, sinirsel, bulanık ve uzman sistemler gelişim gösterdikleri tarih sonucunda aralarında bir rekabet ortamı oluşturmak yerine, entegre olarak aynı doğrultuda çalışabilmeyi tercih etmişlerdir. Bahsi geçen teknolojilerin entegre bir biçimde kullanılması otomotiv, finans, mühendislik, tıp, ekonomi ve daha çok sayıda alanda, sorunları başarılı bir biçimde çözmeye olanak tanımaktadır.

Neredeyse 50 sene önce yalnızca bir hayal olarak görülen akıllı niteliklere sahip makineler, günümüzde hayatımızın bütün alanlarında yerlerini almış durumdadır. Teknolojik alanda bu derece hızlı gelişilmiş olması ve gelinmiş olan yerde akıllı niteliklere sahip teknolojiler ve yapay zekaya karşı gösterilen ilgi gelecek senelerde de bu alanların hızlı bir biçimde gelişmeyi sürdüreceğini ispatlamaktadır.

### 2.2.2. Yapay Zekâ ve İnsan Arasındaki İlişki

Yüzyıllardır bilim insanları ve filozoflar, insan zihninin hangi şekilde çalıştığı ile insan haricindeki canlıların zihinlerinin bulunup bulunmadığına yönelik sorulara cevap aramıştır. Fakat bahsi geçen 2 soruya da henüz açık ve net bir yanıt bulunamamıştır. Bununla birlikte kimi bilim insanları, günümüzde işlem yeteneği bulunan akıllı niteliklere sahip eşyalarda ve akıllı bilgisayarlarda gerçekleşen gelişmelerin etkisi altında kalarak, makinelerin de işlevsel olarak insanın yapabileceği tüm faaliyetleri yapabileceğine dair ve insandan daha üstün bir zihinsel yapıya dahi sahip olabileceklerine dair inanışlar içerisine girmişlerdir (Yılmaz, 2017). Bu bakış açısına tam anlamıyla zıt görüşe sahip olanların savunucularıysa; yaratıcı keşifler, sevgi, hoşgörü, saygı ve ahlaki seçimler benzeri oldukça karmaşık becerilerin hiçbir süreçte herhangi bir makinenin imkân dahilinde yapabilecekleri konusuna dahil olamayacağını ifade ederek, bahsi geçen bir önceki bakış açısına karşı tepki göstermişlerdir.

Söz edilen her 2 görüşün de hiç şüphesiz yanlış ve doğru tarafları bulunmaktadır. Ancak bu konuda önemli olan durum, makine ile insan rekabetinden çok, makine ile insan uyumluluğuna dayanmalıdır. 1940'lı senelerin son dönemlerinde makinelerin herhangi bir zekayı içerip içeremeyeceği ya da düşünüp düşünemeyecekleri sorusu ortaya çıkmıştır. Fakat bahsi geçen sorunun yanıtı kolay bir şekilde yalnızca hayır ya da yalnızca evet değil, belirli olmayan ve bulanık bir yanıttır. Bu konuda yapay zekânın genel olarak bir disiplin kapsamında görevi, insanlar doğrultusunda yapıldığı zaman zekâ gerekliliği bulunan işleri makinelerin de yürütebilmesini sağlamaktır.



İnsanlar, çeşitli ve birbirinden farklı durumlar için farklı beceriler sergileyebilmektedir. Herhangi bir insan, başka bir insandan daha üstün zekaya sahip olabilir ve bazı insanlar mühendislik ya da matematik alanlarında çok daha başarılı olabilirken bazı insanlar da sosyal bilimler alanında çok daha büyük başarılar elde edebilmektedir. Zekâ kavramı, bir insandan başka bir insana göre niteliksel farklılıklar gösterebilmektedir. Yine zekâ kavramı, bazı durumlarda ise zamana dayalı olarak insanlarda farklılık gösterebilmektedir. Yani kimi zaman mühendislik ya da matematikle alakalı bir sorunu üstün bir başarı doğrultusunda çözebilmiş olan insan, kimi zaman da birbirine benzer olan sorun karşısında başarısızlığa uğrayabilmektedir. İnsan beynini baz alarak modelleme esasında geliştirilmiş olan

makinelerde de bahsi geçen insan farklılıkları gibi bir makine diğer makineden daha akıllı durumda olabilecektir (Say, 2019).

Zeki niteliklere sahip makinelerle alakalı ilk örnek makale 1950 senesinde ünüyle nam salmış olan İngiliz kökenli matematikçi Alan Turing doğrultusunda kaleme alınmıştır. 2. Dünya Savaşı esnasında, Alman kökenli kripto cihazı olan Enigma'nın anahtarlarının kırılmasında oldukça önemli bir yere sahip olan Turing, "*makineler de insanlara benzer şekilde düşünebilir mi?*" çerçevesindeki monoton anlamsal ve kavramsal tartışmalarda bulunmak yerine, diğer makinelerin uyguladıklarını taklit edebilme yeteneği olan Turing makinelerini meydana getirerek düşünebilme becerisine sahip makinelerin temelini oluşturmuştur (Warner, 2009).

Bunun dışında Literatür dâhiline Turing testi ismiyle geçmiş olan ve geçerlilik özelliğini günümüzde dahi koruyabilen bir yapay zekâ bünyesindeki testi de Alan Turing geliştirmiştir. Bahsi geçen Turing testi, eş zamanlı olarak yapay zekâ ile ilgili yapılan çalışmalarda, zeki niteliklere sahip bir makine oluşturulduğuna ve geliştirildiğine dair varılmak istenen bir referans merkezi ve hedef olmaktadır. Turing testi içeriğinde 2 tane aşama barındırmaktadır.

İlk aşamada; bir erkek, bir kadın ve bir sorgulayıcı birbirinden farklı odalara yerleştirilerek yalnızca yazılı şekilde aralarında iletişim kurabilmeleri sağlanmaktadır. Sorgulayıcının, yönelteceği sorulara karşılık alacağı yanıtlara göre hangisinin kadın hangisinin erkek olduğunu bulması gerekmektedir. Diğer aşamadaysa; sorgulayıcı benzer biçimde kendisi ile aynı yerde olmayan, bir insana ve bir makineye sorular yöneltmektedir. Sorgulayıcının yönelteceği sorulara karşılık olarak alacağı yanıtlar sonucunda yanıt verenlerden kimin insan kimin makine olduğunu bulmaya çalışmaktadır (Russell ve Norving, 2003).

Sorgulayıcı, makineyi belirleyebilmek adına insan elinden çözülmesi oldukça fazla zaman alabilecek karmaşık niteliklere sahip matematiksel sorular yönelteceği gibi insanı belirleyebilmek adına da duygusal niteliklere sahip sorular yöneltebilmektedir. Bu durumda, matematiksel niteliklere sahip yöneltilen sorular karşısında, makinenin hangi sürede gecikmeli yanıt vereceğini hangi zamanda hata yapabileceğini daha önceden bilmesi gerekmektedir. Bu örneğe benzer biçimde duygusal niteliklere sahip yöneltilen sorular karşısında ise makineden yöneltilen sorularla, insanda yaşanan duygusal reaksiyonları simule edebilecek olması beklenmektedir (Negnevitsky, 2005). Yapılan testin sonucunda

sorgulayıcı, makineyi belirleyebilmek için ne kadar fazla güçlük çektiyse bu durum makinenin o derece zeki olduğunu göstermektedir. Alan Turing, bu testi oluşturduktan sonra 20. yüzyılda testin şartlarını geçebilecek niteliklere sahip bir bilgisayarın yapılandırılabileceğini inanmıştır. Günümüzde halen Turing testi doğrultusunda, kimi özel kapsamlı uzmanlık alanları dahilinde geliştirilen zeki niteliklere sahip makinelerin gösterdiği performans alanında uzman bir kişi tarafından değerlendirilerek ölçülebilmektedir.

# BÖLÜM III
# YÖNTEM

Bu bölüm içerisinde yapılmakta olan çalışmanın yöntemi açıklanmaktadır. Bu bağlamda araştırmanın modeli açıklandıktan sonra evren ve örneklem, verilerin toplanmasında kullanılan araçlar, verilerin toplanma tarzı ve analiz edilmesine dair bilgilere yer verilmiştir.

## 3.1. Araştırmanın Modeli

Yapılmakta olan bu çalışma nitel bir araştırma özelliği taşımaktadır. Araştırmanın gerçekleştirilmesi esnasında araştırma modelleri içerisinden tarama modeli seçilmiştir. Tarama modeli ile ilgili konunun geçmişten günümüze tasvir edilebilmesi sağlanmıştır. Konu ile ilgili önceki çalışmaların tasnif edilerek incelenmesi ve yorumlanması amacıyla tarama modelinin kullanımına karar verilmiştir.

## 3.2. Evren ve Örneklem

Araştırmanın evreni; güvenlik hizmetleridir. Örneklem olarak da güvenlik hizmetleri içerisinden siber güvenlik konusu belirlenmiş olup; yapay zekâ ile ilişkilendirilmesi ele alınmıştır.

## 3.3. Veri Toplama Araçları



Yapılmakta olan çalışmada birincil veri kaynakları üzerinden çalışmanın ana hatları belirlenmiştir. Ana hatlar üzerinde yapılan incelemeler sonucunda ikincil veri kaynakları ile çalışmanın detaylandırılması sağlanmıştır. Veri toplama aracı olarak da doküman ve kayıt incelemesinin kullanımı gerçekleştirilmiştir.

## 3.4. Verilerin Toplanması

Çalışmanın nitel bir araştırma olma özelliğinden kaynaklı olarak doküman ve kayıt incelemeleri gerçekleştirilmiştir. Verilerin toplanması aşamasında olasılıklı örnekleme yöntemlerinden biri olan sistematik tesadüfi örnekleme tercih edilmiştir. Bu yöntem ile

taranan veriler konu, kronoloji ve ilişi ağları doğrultusunda tasnif edilerek çalışmanın çerçevesi belirlenmiştir.

### 3.5. Verilerin Analizi

Veri analizi, toplanmış olan ham verinin en etkili ve en verimli şekilde işlenebilmesinin sağlanmaya çalışıldığı bir süreci ifade etmektedir. Çalışma kapsamında elde edilen verilen analizi için birden fazla yöntem kullanılarak konunun daha spesifik bir biçimde ortaya konulabilmesi hedeflenmiştir. Nitekim çalışma kapsamında kullanılmakta olan veri analiz teknikleri şunlardır;

- Metin Analizi,

- Tanımsal Analiz,

- Çıkarımsal Analizi.

# BÖLÜM IV
# SONUÇ

Araştırma için belirlenen tekniklerin seçilmesinin sebebi literatür taraması odaklı olan bu çalışmaya uygun analizleri gerçekleştirebilmektir. Öyle ki metin analizi ile incelenmekte olan kaynakların içerik olarak detayına inilmesi işlemi gerçekleştirilmiştir. Tanımsal analiz ise yapılan metin analizi sonucunda elde edilen detaylar ile özgün tanımlamalar ve açıklamalar sunmaktadır. Çıkarımsal analizin kullanılmasının sebebi ise hızlı bir değişim ve dönüşüm geçiren araştırma konusunun geleceğine dair birincil kaynaklara dayanarak yorumlar ve öneriler getirebilme olanağını elde edebilme isteğidir.

Buradaki çalışmada, yapay zekâ yöntemlerinin mevcut durumdaki siber savunma faaliyetleri içerisinde kullanılmasının önemi vurgulanmıştır. Kullanılmakta olan yapay zekâ yöntemleri genel kapsamda analiz edilmiştir. Günümüzde sıkça karşılaşılmakta olan siber saldırılara karşı, siber ortamı daha fazla koruma ve güven altına alma ihtiyacı hissedilmektedir. Siber savunma özelliğine sahip olan yazılımların işlevlerini doğru bir biçimde yerine getirebilmelerini sağlayabilmek için, kolay dizayn edilmiş algoritmalar güncel saldırılar karşısında yeterli olmamaktadır.

Bu sebeple yapay zekâ temelli algoritmalar güncel saldırılara karşı daha güçlü yapılara sahip olduğu için, siber güvenlik adına kullanılabilecek en uygun teknikler olacaktır. Yapılmış olan araştırma çalışmalarında elde edilen verilere bakıldığı zaman da yapay nitelikli sinir ağlarının mevcut durumdaki siber savunma faaliyetleri içerisinde daha çok kullanıldığı gözlemlenmiştir. Ancak hâlihazırda bulunan yapay zekâ yöntemleri de belli başlı siber savunmaya yönelik teknikleri bazı hususlarda karşılayamamaktadır. Bu hususlar şu şekilde sıralanabilmektedir:

- Elde edilmiş olan bilgilerin yönetimi,

- Mevcut haldeki durumların farkına varılması,

- Karar destek süreçleri.

Bahsi geçen üç hususun da karşılanabilmesi adına, gelişmiş sistematik teknolojiler dahilinde çalışmalar sürdürülmekte ve sürdürülen çalışmaların ise olumlu sonuçlar vereceği ön görülmektedir.

Amerika Birleşik Devletleri Savunma Bakanlığı, yayına sunmuş olduğu siber stratejiye yönelik dokümanında, siber savaşın mevcut olduğu ortamda 5 adet esas olan ilkeyi ortaya koymuştur. Buradaki ilkeler şu şekildedir (USDDCS, 2015):

1. Siber ortam, yeni niteliklere sahip bir uygulama alanı olarak birbirinden farklı ve başka savaş ortamlarına benzerlik göstermektedir. Bu durumdan dolayı uzay, hava, deniz ve karadan sonra siber alan da yeni niteliklere sahip bir savaş ortamı olarak kabul görmelidir.

2. Pasif niteliklere sahip savunma teknikleri yerine proaktif yapılı savunma tekniklerine geçilmelidir.

3. Kritik altyapıların güvenliğinin sağlanması ve korunabilmesi adına kritik temelli alt yapısal koruma konseptlerinin entegresi düzenlenmelidir.

4. Ortak savunma yöntemlerinin, önceden tespit edebilme becerisini kazanabilmesi için, kendi özellikleriyle savunma mekanizmalarına dahil edilmesi ve bu şekilde aktif olarak kullanılabilmesi sağlanmalıdır.



5. Teknolojik özellikli değişim olanakları güvence altına alınarak korunmalı, iyileştirilip geliştirilerek daha verimli hale getirilmeli ve yeni niteliklere sahip olan teknolojiler, siber güvenlikle alakalı tüm savunmaya yönelik sistemlere uyumlu bir şekilde dahil edilmelidir.

Yukarıda verilmiş olan 5 adet esas ilke içerisinde özellikle beşinci sırada yer alan madde oldukça büyük bir öneme sahiptir. Siber ortamın, insanlar doğrultusunda idaresi sağlanamayacak ve kategorize edilemeyecek kadar fazla bilgi ve veri oranı elde etmesi, teknolojik alanlardaki gelişmelerin sürati ve bahsi geçen gelişmelerle beraber ortaya çıkan oldukça sofistike ve karmaşık yapılı siber tehditler ve mevcut durumdaki bu tehditlerin verebileceği zararları minimum seviyeye indirebilmek için mümkün olduğu kadar önceden tespitinin sağlanması ve herhangi bir tespitte tehdidin önlenmesi benzeri hususlar yapay zeka tekniklerini siber güvenlik için çok önemli kılmıştır.

# KAYNAKÇA

Akdağ, İ. (2021). "*Siber Güvenlik ve Türkiye: Örgütsel Yapı, Uygulamalar ve Gelecek*". (Doktora Tezi) Sosyal Bilimler Enstitüsü, Hacettepe Üniversitesi, Ankara.

Akyeşilmen, N. (2018). *Disiplinler Arası Bir Yaklaşımla Siber Politika ve Güvenlik*. Ankara: Orion.

Allen, G. and Chan, T. (2017). *Artificial Intelligence and National Security*. Camridge: Belfer Center.

Amerika Birleşik Devletleri Savunma Bakanlığı (2015). "US Department of Defense Cyber Strategy", US DoD.

Dan Craigen, N. D. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, 13-21.

Horowitz, M.C., Allen, G.C., Saravealle, E., Cho, A,. Frederick, K., and Scharre, P. (2018). *Artificial Intelligence and International Security*. Center for a New American Security.

Iftikhar, B. and Alghamdi, A.S. (2009). Application of artificial neural network in detection of dos attacks, SIN '09: Proceedings of the 2nd international conference on Security of information and networks. *ACM*, pp. 229–234.

Kalaycı, T. E. (2018). Kimlik Hırsızı Web Sitelerinin Sınıflandırılması İçin Makine Öğrenmesi Yöntemlerinin Karşılaştırılması, *Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi*, 5(2).

Karakuş, C. (2013). *Kritik Alt Yapılara Siber Saldırı*, İstanbul Kültür Üniversitesi.

Klein, A., Ojamaa, P., Grigorenko, M., and Jahnke, E. T. (2010). *Enhancing Response Selection in Impact Estimation Approaches.* Military Communications and Information Systems Conference (MCC), Wroclaw, Poland.

Kotenko, I. (2007). "Multi-agent Modelling and Simulation of Cyber-Attacks and Cyber-Defense for Homeland Security", *IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems*, Technology and Applications.

Kramer, F. D. (2009). Cyberpower and National Security: Policy Recommendations for a Strategic Framework. Kramer, F. D., Starr, S., Wentz, L. K. (edt.) *Cyberpower and National Security.* Washington D.C.

Lindsay, R. K., Buchanan, B. G., Feigenbaum, E. A., & Lederberg, J. (1993). *DENDRAL: a case study of the first expert system for scientific hypothesis formation. Artificial intelligence, 61*(2), 209-261.

McCulloch, W., and Pitts, W. (1943) "A Logical Calculus of The Ideas Immanent in Nervous Activity", *Bulletin of Mathematical Biophysics*, 5, pp. 115- 133.

Nabiyev, V. (2016). *Yapay Zekâ, Stratejili Oyunlar-Örüntü Tanıma- Doğal Dil İşleme.* Ankara: Seçkin Yayınları.

Negnevitsky, M. (2005). *Artificial Intelligence: A Guide Intelligent Systems*. Essex: Addison-Wesley.

Nilsson, N.J. (2019). *Yapay Zekâ, Geçmişi ve Geleceği*. İstanbul: Boğaziçi Üniversitesi Yayınevi.

Özen, Y. ve Mert, B. (2018). *Saldırı Tespit Sistemlerinde Kullanılan Makine Öğrenmesi Algoritmalarının Karşılaştırılması*, ICONCS.

Patel, A., Taghavi M., Bakhtiyari, K. J. and Celestino J. J., (2013) .Junior, "An Intrusion Detection and Prevention System in Cloud Computing: A Systematic Review", Journal of Network and Computer Applications, Elsevier.

Russell, S. and Norving, P. (2003). *Artificial Intelligence – A Modern Approach*. New Jersey: Prentice Hall.

Sağıroğlu, Ş., Yolaçan, E. N. ve Yavanoğlu U. (2011). *Zeki Saldırı Tespit Sistemlerinin İncelenmesi, Tasarımı ve Gerçekleştirilmesi*, Gazi Üniversitesi, Ankara.

Say, C. (2019). *50 Soruda Yapay Zekâ*. İstanbul: 7 Renk Basım Yayım.

Stanford (2019). Proffessor John McCarty, Father of AI.

Sundaram, A. (1996). An İntroduction To İntrusion Detection, *Crossroads: The ACM Student Magazine*, New York, 2(4), 3-7.

Şenkaya, Y. ve Adar U.G. (2014). *Siber Savunmada Yapay Zeka Sistemleri Üzerine İnceleme*, Akademik Bilişim Konferans Yayını, Mersin.

Takcı, H. (2021). *Veri Madenciliği İle Saldırı Tespiti*, Cumhuriyet Üniversitesi, Sivas.

Ulaştırma ve Haberleşme Bakanlığı (2020). *Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023),* Ankara.

Ünver, M., Canbay, C., Mirzaoğlu, A. G. (2009) Mirzaoğlu, *Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler*, Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı, Ankara.

Warner, M. (2009). "Intelligence as Risk Shifting", *Studies in Intelligence*, 53(2).

Yıldırım, M. Z., Çavuşoğlu, A., Şen, B. ve Budak, İ. (2014). *Sinir Ağları ile Ağ Üzerinde Saldırı Tespiti ve Paralel Optimizasyonu*, 15. Akademik Bilişim Konferansı Bildirileri.

Yılmaz, A. (2017). Yapay Zekâ. İstanbul: Kodlab Yayınları.

Zadeh, L.A. (1965). 'Fuzzy Sets', *Information and Control*, 8 (1), pp. 338-353.