T.C.
NECMETTİN ERBAKAN ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
YÖNETİM BİLİŞİM SİSTEMLERİ ANABİLİM DALI
YÖNETİM BİLİŞİM SİSTEMLERİ BİLİM DALI

DİJİTAL DÖNÜŞÜM SÜRECİNDE SİBER GÜVENLİK FARKINDALIĞI: KONYA'DA BİLİŞİM SEKTÖRÜNDE FAALİYET GÖSTEREN KOBİLER ÜZERİNE BİR ARAŞTIRMA

TUĞBA ÇALIŞKAN

YÜKSEK LİSANS TEZİ

DANIŞMAN:
PROF. DR. MUSTAFA KOCAOĞLU

KONYA-2025

İÇİNDEKİLER

İKİNCİ BÖLÜM

SİBER GÜVENLİK VE KOBİLER

ÜÇÜNCÜ BÖLÜM

BİLİŞİM SEKTÖRÜNDE FAALİYET GÖSTEREN KOBİLERDE SİBER GÜVENLİK UYGULAMALARI ÜZERİNE BİR ARAŞTIRMA

T.C.
NECMETTİN ERBAKAN ÜNİVERSİTESİ
Sosyal Bilimler Enstitüsü

BİLİMSEL ETİK SAYFASI

Öğrencinin	Adı Soyadı	Tuğba ÇALIŞKAN		
	Numarası	21081031007		
	Ana Bilim / Bilim Dalı	Yönetim Bilişim Sistemleri		
	Programı	Tezli Yüksek Lisans	X	
		Doktora		
	Tezin Adı	Dijital Dönüşüm Sürecinde Siber Güvenlik Farkındalığı: Konya'da Bilişim Sektöründe Faaliyet Gösteren Kobiler Üzerine Bir Araştırma		

Bu tezin hazırlanmasında bilimsel etiğe ve akademik kurallara özenle riayet edildiğini, tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada başkalarının eserlerinden yararlanılması durumunda bilimsel kurallara uygun olarak atıf yapıldığını bildiririm.

Öğrencinin Adı Soyadı
İmzası

T.C.
NECMETTİN ERBAKAN ÜNİVERSİTESİ
Sosyal Bilimler Enstitüsü

ÖZET

Öğrencinin	Adı Soyadı	Tuğba ÇALIŞKAN		
	Numarası	21081031007		
	Ana Bilim / Bilim Dalı	Yönetim Bilişim Sistemleri		
	Programı	Tezli Yüksek Lisans	**X**	
		Doktora		
	Tez Danışmanı	Prof. Dr. Mustafa KOCAOĞLU		
	Tezin Adı	Dijital Dönüşüm Sürecinde Siber Güvenlik Farkındalığı: Konya'da Bilişim Sektöründe Faaliyet Gösteren Kobiler Üzerine Bir Araştırma		

Bilgi ve İletişim Teknolojileri (BİT), bireylerin ve kurumların yaşamlarını dönüştürmeye devam etmektedir. Bu teknolojiler, küresel çapta hızla yayılmakta ve çeşitli alanlarda kullanılmaktadır. Özellikle dijitalleşmeyle birlikte, BİT'ler eğitim, sağlık, ekonomi ve kişisel yaşam gibi pek çok alanda kullanılmaktadır. Teknoloji kullanımı, işletmelere rekabet avantajı ve yenilikçi fırsatlar sunarken, yanlış yönetim ise güvenlik tehditlerine yol açabilmektedir. Kötü niyetli kişiler, dijital ortamları siber suçlar ve veri hırsızlığı gibi faaliyetler için kullanabilmektedir. Bu nedenle, işletmelerin teknolojiyi stratejik bir şekilde yönetmesi ve siber güvenliği güçlendirmesi, dijital dönüşümde kritik bir rol oynamaktadır.

Bu araştırmada nicel ve nitel araştırma yöntemlerinin bir arada kullanıldığı karma yöntem benimsenmiştir. Bu araştırmanın temel amacı, Konya ilinde bilişim sektöründe faaliyet gösteren KOBİ'lerin siber güvenlik farkındalık seviyelerini belirlemek ve bu farkındalık seviyelerinin katılımcıların demografik özelliklerine göre farklılık gösterip göstermediğini incelemektir. Araştırmanın nicel veri toplama aracı olarak "Siber Güvenlik Farkındalığı Ölçeği" kullanılmıştır. Konya ilindeki bilişim sektöründeki KOBİ'lere, kolayda örnekleme yöntemiyle ulaşılmış ve 228 çalışanın katılımıyla veriler toplanmıştır. Elde edilen veriler, IBM SPSS Statistics 23 programı aracılığıyla analiz edilmiştir. Araştırmanın nitel veri toplama yöntemi ise yarı yapılandırılmış mülakat tekniği olup, bu çerçevede işletme yöneticileri ve/veya müdürlerinden oluşan 18 katılımcı, amaçlı örnekleme yöntemiyle belirlenmiştir. Yüzyüze toplanan nitel veriler, MAXQDA 2020 programı ile analiz edilmiştir. Nicel bulgular, KOBİ'lerin siber güvenlik farkındalık düzeylerinin, katılımcıların demografik özelliklerine göre farklılık gösterdiğini ortaya koymuştur. Nitel veriler ise, siber güvenlik farkındalık seviyesinin genel olarak düşük olduğunu ve ayrıca teknik altyapının yetersizliği, eğitim ve bilgilendirme ihtiyacı, planlama ve önleme süreçlerindeki eksiklikler ile güvenlik politikalarının geliştirilmesinde önemli boşluklar bulunduğunu göstermektedir.

Anahtar Kelimeler: Dijital, Dijitalleşme, Dijital Dönüşüm, Siber Güvenlik

T.C.
NECMETTİN ERBAKAN ÜNİVERSİTESİ
Sosyal Bilimler Enstitüsü

ABSTRACT

Author's	Name and Surname	Tuğba ÇALIŞKAN		
	Student Number	21081031007		
	Department	Management Information Systems		
	Study Programme	Master's Degree (M.A.)	**X**	
		Doctoral Degree (Ph.D.)		
	Supervisor	Prof. Dr. Mustafa KOCAOĞLU		
	Title of the Thesis/Dissertation	Cyber Security Awareness in the Digital Transformation Process: A Research on SMEs Operating in the IT Sector in Konya		

Information and Communication Technologies (ICT) continue to transform the lives of individuals and institutions. These technologies are rapidly spreading globally and are used in various areas. Especially with digitalization, ICTs are used in many areas such as education, health, economy and personal life. While the use of technology provides businesses with competitive advantage and innovative opportunities, mismanagement can lead to security threats. Malicious individuals can use digital environments for activities such as cybercrime and data theft. Therefore, strategic management of technology and strengthening cybersecurity by businesses plays a critical role in digital transformation.

This study adopted a mixed method in which quantitative and qualitative research methods are used together. The main objective of this research is to determine the cyber security awareness levels of SMEs operating in the IT sector in Konya province and to examine whether these awareness levels differ according to the demographic characteristics of the participants. "Cyber Security Awareness Scale" was used as the quantitative data collection tool of the research. SMEs in the IT sector in Konya province were reached by convenience sampling method and data were collected with the participation of 228 employees. The obtained data were analyzed by IBM SPSS Statistics 23 program. The qualitative data collection method of the research is the semi-structured interview technique, and in this framework, 18 participants consisting of business managers and/or directors were determined by purposive sampling method. The qualitative data collected face-to-face were analyzed by MAXQDA 2020 program. Quantitative findings revealed that the cyber security awareness levels of SMEs differ according to the demographic characteristics of the participants. Qualitative data show that the level of cybersecurity awareness is generally low, and there are also inadequate technical infrastructure, need for training and information, deficiencies in planning and prevention processes, and significant gaps in the development of security policies.

Keywords: Digital, Digitalization, Digital Transformation, Cyber Security

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

GÖRSELLER LİSTESİ

GRAFİKLER LİSTESİ

KISALTMALAR LİSTESİ

AI	**:**Artificial Intelligence (Yapay Zekâ)
AR	**:**Augmented Reality (Artırılmış Gerçeklik)
AR-GE	**:**Araştırma Geliştirme
BİT	**:**Bilgi İletişim Teknolojileri
BT	**:**Bilgi Teknolojileri
GSYİH	**:**Gayri safi yurtiçi hasıla
IOT	**:**Internet of Things (Nesnelerin İnterneti)
ITU	**:**Uluslararası Telekomünikasyon Birliği
KOBİ	**:**Küçük ve Orta Büyüklükteki İşletmeler
KOSGEB	**:**Küçük ve Orta Ölçekli İşletmeleri Geliştirme ve Destekleme İdaresi Başkanlığı
OECD	**:**Organization for Economic Co-operation and Development (Ekonomik Kalkınma ve İş Birliği Örgütü)
TÜBİSAD	**:**Türkiye Bilişim Sanayicileri Derneği
TÜBİTAK	**:**Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
TÜSİAD	**:**Türk Sanayicileri ve İş İnsanları Derneği
VR	**:**Virtual Reality (Sanal Gerçeklik)

ÖNSÖZ/TEŞEKKÜR

Öncelikle bu çalışmanın ortaya çıkma ve yürütülme aşamasında, değerli bilgilerini benimle paylaşan, kendisine ne zaman danışsam bana kıymetli zamanını ayırıp sabırla ve büyük bir ilgiyle bana faydalı olabilmek için elinden gelenden fazlasını sunan, güler yüzünü ve samimiyetini benden esirgemeyen danışman hoca statüsünü hakkıyla yerine getiren PROF. DR. MUSTAFA KOCAOĞLU' na çok teşekkür ederim.

Bu yolda bana vesile olan, bilgi birikimleriyle her zaman yoluma ışık tutan, tecrübeleri ile yol gösteren çok kıymetli hocam PROF. DR. AHMET GÜZEL' e teşekkür ederim.

Bu uzun çalışma sürecinde her zaman yanımda olan, bana her zaman güvenen ve sevgiyle yol gösteren babam ZEYNEL ABİDİN ÇALIŞKAN'a; sabırlı ve her zaman en iyiye ulaşmam için beni destekleyen annem AYŞE ÇALIŞKAN'a; Yolculuğum boyunca hep yanımda olan ve moral kaynağım olan abim MAHMUT ÇALIŞKAN'a ve her an yanımda durarak bana neşe, güç ve huzur veren **k**ardeşimlerim FATMA ÇALIŞKAN ve ÜMMÜ ÇALIŞKAN'a sonsuz teşekkürlerimi sunarım. Hep birlikte olmak, birlikte mücadele etmek, bana gerçek anlamda güç verdi.

Hepinizin desteğiyle bu zorlu süreci başarıyla tamamladım. Bu çalışmanın her satırında sizin izleriniz var. Hepinize gönülden teşekkür ederim.

GİRİŞ

Dünya geçmişten günümüze sürekli değişip gelişmektedir. Bu değişim ve gelişim ağırlıklı olarak bilgi ve iletişim teknolojileri alanında meydana gelmektedir. Özellikle bilgi ve iletişim teknolojilerinin iş süreçleriyle etkileşim sağlanmasıyla dünya hızlı bir dijitalleşme sürecine girmiştir. Günümüzde bu dijitalleşme sürecinin getirdiği yenilikçi teknolojiler insanoğlunun her alanda yeni gelişmeler oluşturmasına ve çeşitli yeniliklere başvurmasına sebep olmuştur. Dijital teknolojilerin kullanılması ve entegrasyonu sıklıkla şirketlerin büyük bölümlerini etkilemekte ve hatta ürünleri, iş süreçlerini, satış kanallarını ve tedarik zincirlerini etkileyerek şirketlerin sınırlarının ötesine geçmektedir. Dijitalleşmenin beraberinde getirdiği yararlar çok çeşitlidir ve diğerlerinin yanı sıra satış ya da üretkenlikteki verimliliği, değer katmadaki yenilikleri ve ayrıca müşterilerle oluşturduğu yeni etkileşim biçimlerini kapsamaktadır (Matt vd., 2015: 339).

Teknolojik değişimin ve yeniliğin hızı her geçen gün daha da artmaktadır. KOBİ'ler bu değişim ve yeniliğe uyum sağlayabilmek, maliyetleri azaltmak ve rekabette avantaj sağlayabilmek için dijital dönüşümle iç içe olmak zorundadır. Bu anlamda KOBİ'lerde dijitalleşme ön plana çıkmaktadır. Hızla değişen rekabetçi iş dünyasında zaman ve maliyet avantajı sağlayan bu teknolojilerin etkin olarak kullanılması işletmeler için oldukça önemlidir. Böylece işletmeler bu anlayış çerçevesinde vatandaşlara dijital teknolojilerle uyumlu hizmet ve süreçleri sunmaya çalışmaktadır. İşletmeler teknolojideki gelişmeler sayesinde büyük miktarda verilerin toplanması, süreçlerin genel olarak web, mobil, bulut platformlarında yapılması gibi birçok işlemi otomatik ve dijital olarak gerçekleştirmektedir. Ancak dijital dönüşüm, getirdiği faydaların yanında siber güvenlik risklerini de beraberinde getirmektedir.

Dijital dönüşüm; 20. yüzyılda teknolojinin hızla ilerlemesi ve değişimi ile beraber, teknolojik materyallerin gelişiminden yararlanmaya bağlı olarak, kişiler ve örgütler tarafından kullanılmaya başlanmasıyla hız kazanmıştır. Zaman ve mekândan bağımsız bir şekilde bireylerin ve örgütlerin iletişim kurmalarına olanak sağlayan dijital teknolojik gelişmeler, örgütlerin ve bireylerin bu değişim süreci içerisinde yer almalarını gerekli kılmıştır. "*Dijital dönüşüm, dijital teknolojilerin yenilikçi odaklı*

*kullanımıyla beraber temel kaynak ve becerilerin stratejik gücünden faydalanan, bir kuruluşu köklü bir şekilde iyileştirmeyi ve paydaşlar açısından değerini yeniden açıklamayı amaçlayan temel bir değişim sürecidir.”(*Melo vd., 2023: 3) Diğer bir tanımlamada, *“Dijital dönüşüm, mobil teknolojiler, internet, nesnelerin interneti, otomasyon, robot teknolojileri, bulut bilişim teknolojileri, blok zincir, yapay zekâ, arttırılmış gerçeklik ve sanal gerçeklik gibi farklı ve yeni dijital teknolojilerin insan hayatına ve işletme süreçlerine girmesi ile oluşan değişim, işlem uygulama ve etkileşimlerin tümüdür.”* (Kocaoğlu, 2021: 82). Dijital dönüşümün temeli niteliğindeki nesnelerin interneti (IoT), büyük veri, sosyal medya, yapay zekâ, bulut bilişim, blockchain ve artırılmış gerçeklik gibi dijital teknolojiler işletmeleri dijital müşteri etkileşimi ile iş süreçleri ve hizmetlerinde bir üst seviyeye taşımaktadır (Al-Ruithe vd., 2018: 1037). Dijital dönüşümün gerçekleşmesindeki sebep bilgi toplumunun meydana getirdiği dijital çağdır. Sürekli gelişimini devam ettiren teknoloji sayesinde bilgi iletişim teknolojileri (BİT) daha düşük maliyetli ve daha güçlü konuma gelmiştir. Böylece toplumlar üzerinde etkisini hemen hissettirmiş ve kullanımı daha çabuk benimsenmiş olan bilgi ve iletişim teknolojileri tüm alanlarda kullanılmaya başlanmıştır. Bu durum çağa ayak uydurmak için hem kamudaki kurumların hem de özel sektördeki işletmelerin dijital anlamda dönüşüme gitmelerine sebep olmuştur (Cette vd., 2016: 5).

Yılda 250 kişiden daha az çalışanı bünyesinde barındıran, yıllık net satış hasılatı veya mali bilançosundan birinin 500 milyon TL’yi aşmayan işletmeler yönetmelikte “KOBİ” (Küçük ve Orta Büyüklükteki İşletmeler) olarak ifade edilmektedir (KOSGEB, 2024). KOBİ’ler açısından dijitalleşme, teknolojinin getirdiği faydaları kullanarak dijital çağın sunduğu zorunlulukları hızlı ve kolay bir şekilde yerine getirebilmek, iş süreçlerindeki performans artışını sağlamak için önemli bir araç konumuna gelmiştir. KOBİ’ler; geleneksel üretim veya hizmet süreçlerinin ortadan kaldırılmasına imkân sağlayan dijital teknolojilerin oluşturulması ve bu süreçleri yürütmek için bulut bilişim, büyük veri analitiği, yapay zekâ ve makine öğrenimi, nesnelerin interneti (IoT) ve blockchain teknolojisi gibi dijital dönüşüm ile ilgili teknolojilerinden yararlanarak yeni iş süreçlerinde bu tür yenliklere uyum sağlamak zorunda kalmaktadır.

KOBİ'ler ülkelere ve bulundukları bölgelere ekonomik olarak olumlu katkılar sağlamaktadır. Bu işletmeler; ekonominin gelişim göstermesi, istihdam sağlaması, ülke ekonomilerini inovasyona sevk etmeleri nedeniyle ülke ve bölge ekonomisine ciddi yararlar sağlamaktadır. Günümüz dünyasında KOBİ'ler yatırım, iş birliği ve ticaret konularında yalnızca faaliyet gösterdikleri ülkede değil dünya genelinde de yer edinmeye başlayarak uluslararası pazarda büyük işletmelerle bir arada varlık göstermektedir. Teknolojiyi kullanan KOBİ'ler, büyük işletmelerle karşılaştırıldığında büyük oranda ihracat yapma ve daha hızlı büyüme ihtimaline sahip olmalarından ötürü ön plana çıkmaktadır (Yağcı, 2023: 1).

Dijital dönüşüm, organize edilmiş süreçleri bilgi teknolojileri çözümlerine aktararak iş alanını dönüştürmekte ve bir organizasyonun farklı yönlerinde ciddi değişikliklere yol açmaktadır. Operasyonlar, kullanıcı deneyimi, müşteriler, ilişkiler, kültürel farklılıklar ve pazarlar gibi birçok unsuru etkilemektedir. Yapay zekâ (AI), blockchain, büyük veri ve analitik, bulut bilişim ve diğer hizmetler dahil olmak üzere gelişen farklı teknolojiler, dünya genelinde dijital dönüşümü teşvik ederken, bu süreçlerden geçen iş yerleri için siber güvenlik tehditleri de artmaktadır. (Saeed vd., 2023: 16). Bir kuruluşun veya kurumun sistemlerine yönelik gerçekleştirilen başarılı bir siber saldırı, önemli zararları ve maddi kayıpları ortaya çıkarabilecek önemli bir risk oluşturmaktadır (Borca, 2022: 58). Günümüz çağında, işletmelerin önemli bilgi kaynakları elektronik ortamlara taşınıp bilgisayar ortamında kaydedilip saklanmaktadır (Aydın, 2022: 4). Teknolojinin gelişmesiyle işletmeler arasında fiziksel mesafeler ortadan kalktıkça birçok uygulama bilgisayar üzerinden gerçekleşmektedir. Elektronik imza, e-posta, bulut teknolojisi vb. çoğu bilgi teknolojisi işletmelerde siber güvenlik sorunlarını ortaya çıkarmaktadır. Siber güvenlik, bilgi ve bilgi sistemlerinin (ağlar, bilgisayarlar, veri tabanları, veri merkezleri ve uygulamalar) uygun prosedür ve teknolojik güvenlik tedbirleriyle korunmasıdır (Tonge vd., 2013: 67). Literatürde siber güvenlik ile ilgili birçok tanımlama mevcuttur. Kaspersky (2020) siber güvenliği, *"Siber güvenlik, bilgisayarları, sunucuları, mobil cihazları, elektronik sistemleri, ağları ve verileri kötü niyetli saldırılara karşı koruma uygulamasıdır"* olarak tanımlamaktadır. Uluslararası Telekomünikasyon Birliği (ITU) ise siber güvenliği, *"Siber güvenlik, siber ortamı,*

kuruluşu ve kullanıcının varlıklarını korumak için kullanılabilecek araçlar, politikalar, güvenlik kavramları, güvenlik önlemleri, yönergeler, risk yönetimi yaklaşımları, eylemler, eğitimler, en iyi uygulamalar, güvence ve teknolojilerin toplamıdır" olarak tanımlamaktadır (Von Solms ve Van Niekerk, 2013: 97).

Günümüzde siber güvenlik BT'ye bağımlı olan, çevrimiçi ve dijital bir varlığa sahip olan hem büyük hem de küçük kuruluşlar için endişe kaynağı olmaya devam etmektedir. Çünkü *"siber suç milyarlarca dolar kaybına, bilgisayar sistemlerinin arızalanmasına, kritik bilgilerin yok olmasına, ağ bütünlüğünün ve gizliliğinin tehlikeye atılmasına vb. yol açmıştır."* (Abubakar vd., 2015: 221). Bu olumsuzluklara rağmen, özellikle siber güvenlik konusuna ilişkin çok az çalışma bulunmaktadır.

Bu çalışmada öncelikle KOBİ'lerin dijital dönüşüm düzeyleri incelenmiş, siber güvenliğin bilişim sektörüne yansımaları ortaya konulmaya çalışılmıştır. KOBİ'lerde dijital dönüşümünün beraberinde getirdiği siber güvenlik farkındalıkları üzerinde durulmuş; ilgili başlıklarda yapılan çalışmalar incelenmiştir. Karşılaşılan siber güvenlik olayları ve çözüm önerileri incelenmiştir. Bu amaç doğrultusunda, çalışmada öncelikle dijital dönüşüm kavramı açıklanarak, dijital dönüşümün önemi, tarihsel gelişimi ve dijital teknolojilerin çok yönlü analizi yapılmıştır. Ayrıca, KOBİ'lerde dijital dönüşümün önemi, gelişimi, avantajları ve dezavantajları detaylı bir şekilde incelenmiştir.

Çalışmanın ikinci bölümünde, siber güvenlik kavramı detaylı bir şekilde incelenmiş ve bilgi ile iletişim teknolojileri kavramı açıklanmıştır. Bu çerçevede, siber güvenlik ile ilgili temel kavramlar ele alınmış, siber tehdit yöntemleri ve çeşitleri açıklanmıştır. Bölümün sonunda ise, KOBİ'lerde siber güvenliğin önemi vurgulanmış ve KOBİ'lerin karşılaştığı siber tehditler ile bu tehditlere karşı alınabilecek önlemler açıklanmıştır.

Çalışmanın son bölümünde ise, araştırmanın amacı, önemi, yöntemi, bulguları ve bu bulguların değerlendirilmesine yer verilmiştir.

BİRİNCİ BÖLÜM
KOBİLERDE DİJİTAL DÖNÜŞÜM

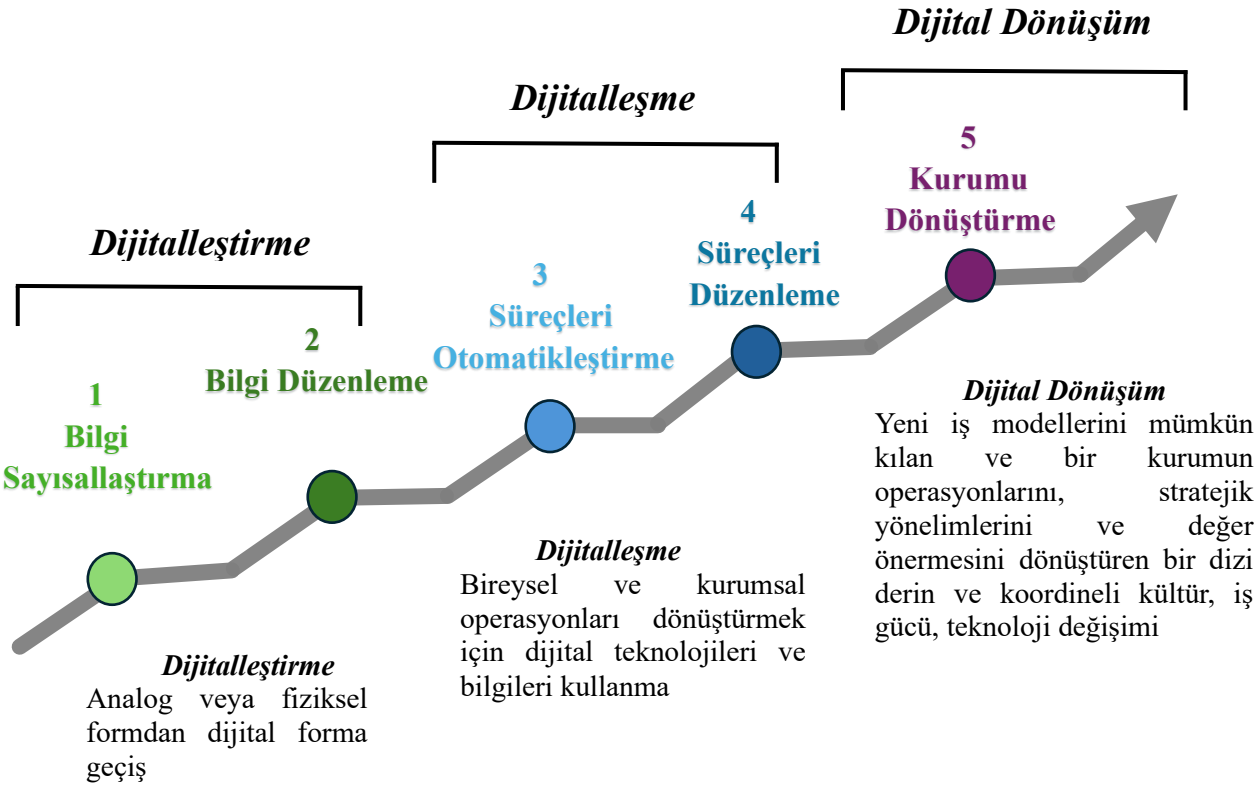
1.1. Dijital Dönüşüm: Kuramsal ve Kavramsal Çerçeve

İşletmelerin dijitalleşmeyi benimseme ihtiyacı, hızla gelişen dijital ortamda kendisini daha çok göstermektedir. İşletmelerin verimliliğini, maliyet etkinliğini ve sürdürebilirliklerini artırmada dijitalleşmenin büyük bir rolü vardır. Dijital dönüşümün başlangıcı olarak görülen endüstri 4.0 kavramı birçok alanda etkisini göstermiştir. Bu etkiler de işletme alanında köklü dijital dönüşümlere sebep olmuştur.

Günümüzde teknolojinin gelişmesi ile birlikte robotlar, 3D yazıcılar, nesnelerin interneti, yapay zekâ, artırılmış gerçeklik ve bulut sistemi gibi birçok yeni nesil teknoloji, günlük yaşamda önemli bir yer edinmiştir (Tonga ve Tonga, 2022:44). Bu nedenle işletmelerin rekabet avantajı sağlamasında dijital yenilikler büyük bir rol oynamaktadır. Bu kapsamda bu bölümde dijital, dijitalleştirme, dijitalleşme ve dijital dönüşüm gibi kavramların açıklamalarına yer verilmiştir.

1.1.1. Dijital, Dijitalleştirme, Dijitalleşme ve Dijital Dönüşüm Kavramları

Günümüzün hızla değişen teknolojik dünyasında dijitalleşme, dijital dönüşüm ve dijitalleştirme çok sık rastlanan kavramlardır. Bu kavramlar literatürde birbirlerinin muadili olarak da kullanılmaktadır. Ancak bu terimler anlam olarak her ne kadar yakın olsalar bile önemli farklara sahiptirler. Dijital dönüşümü üç aşamada ele alırsak, ilk aşamayı "verilerin dijital formata dönüştürülmesi" olarak tanımlanan dijitalleştirme almaktadır. İlk aşamayı oluşturan dijitalleştirmedeki süreçlerin ve verilerin dijital teknolojilerle nasıl daha etkili kullanılabileceğini ifade eden dijitalleşme ise dijital dönüşümün ikinci aşamasında yer almaktadır. Son olarak, dijital dönüşüm en kapsamlı aşamayı ifade etmektedir. Ayrıca, dijital dönüşüm kurumların kültürünü ve tüm yapısını dijital teknolojilerle yeniden şekillendirmeyi amaçlamaktadır (Karaaslanoğlu, 2023: 7).



Şekil 1.1. Dijital Dönüşüm Süreci
(**Kaynak:** Educase, 2020)

Şekil 1.1' de görüldüğü gibi dijital dönüşüm dijital çağda gelişimi sağlayan sinerjik bir evrim niteliğinde olup; teknolojik gelişmeleri ve iş gücünün adaptasyonunu uyumlu hale getiren, kurumun temel yapısını yeniden şekillendiren sürecin kültürel değişimini tetiklemektedir. Dijitalleştirme ilk aşama olan ve analog veya fiziksel formdan dijital forma geçişi ifade eden bilgi düzenlemeyi ve sayısallaştırma tanımlamaktadır. Süreçleri otomatikleştirme ve düzenleme ikinci aşama olup dijitalleşme olarak ifade edilir. Dijital dönüşüm son aşama olup, kuruluş içerisindeki bir dizi teknolojik, kültürel ve operasyonel değişikliği uygulayarak ve koordine ederek kurumsal dönüşümü gerçekleştirmeyi hedeflemektedir.

1.1.1.1. Dijital

Son yıllarda çok sık karşılaştığımız dijital kavramının tarihine bakıldığında 1 ve 0 rakamlarından oluştuğu ve 17. yüzyılda ortaya çıktığı görülmektedir. Bilişimde

“1” bir şeyin var olduğunun göstergesi iken “0” ise olmadığının göstergesidir. 1 ve 0 bit olarak adlandırılmaktadır (Yapıcı, 2021: 402). Türk Dil Kurumu’nun sözlüğüne bakıldığında, Fransız kökenli olan dijital terimi “*sayısal*”, “*verileri bir ekran üzerinde elektronik olarak gösteren*” ve “v*erilerin bir ekran üzerinde elektronik olarak gösterilmesi*”, olarak üç farklı şekilde açıklanmıştır (TDK, 2024). Teknoloji araştırma ve danışmanlık firması olan Gartner’ın (Amerika Birleşik Devletleri) IT Sözlüğü ise dijital kavramını, “*fiziksel öğelerin veya etkinliklerin ikili kod aracılığıyla temsili*” olarak tanımlamıştır. Dijital kavramı bir sıfat olarak kullanıldığında ise, genellikle insanlar, nesneler ve kuruluşlar arasındaki etkileşimleri daha da geliştirmek, organizasyonel süreçleri iyileştirmek veya yeni iş modelleri oluşturmak için en son teknolojilerin baskın kullanılması olarak tanımlanmaktadır (Gartner, 2024).

1.1.1.2. Dijitalleştirme

Makine tarafından analog verilerin ve süreçlerin okunabilir bir biçime dönüştürülmesi dijitalleştirme olarak tanımlanmaktadır. Ayrıca dijitalleştirme, verilerin ve dijital teknolojilerin (yazılım ve donanım) kullanımı, yeni ve/veya mevcut faaliyetlerde değişikliklerle sonuçlanan bağlantı olarak da ifade edilebilmektedir (OECD, 2024). Dijitalleştirme, 0'lar ve 1'ler dizisine dönüştürmekle ilgili olup, temel unsuru evrensel hale getirmektedir (Vrana ve Singh, 2021: 16). Örnekler arasında; dijital anketlerin kullanımı, dahili finansal beyanlar için dijital uygulamaların ve sipariş süreçlerinde dijital formların kullanımı yer almaktadır. Dijitalleştirme esas olarak dahili ve harici dokümantasyon süreçlerini tipik olarak dijitalleştirmektedir. Fakat, dijitalleştirme değer yaratma faaliyetlerini değiştirme görevini uygulayamamaktadır (Verhoef vd., 2021: 891)

Genellikle kurumsal bağlamda, dijitalleştirme operasyonları daha verimli hale getirmek ve süreçleri optimize etmek için bir ön koşuldur. Ayrıca, dijitalleştirme belgelerin dijital olanlarla ve örneğin basılı formlarının değiştirilmesi görevini yapmaktadır. Genel bir terim olarak ise dijitalleştirme, hizmetlerin, ürünlerin, bilgilerin ve süreçlerin bilgi ve iletişim teknolojisi tarafından işlenebilen veya desteklenebilen bir forma dönüştüren faaliyetleri ifade etmektedir (Vitera vd., 2022: 57).

1.1.1.3. Dijitalleşme

Sağlıktan ulaşıma ve iletişime kadar insan yaşamı için gerekli olan birçok alanda bireyin talep ettiği hizmete daha hızlı bir şekilde erişmesi dijitalleşme olarak tanımlanmaktadır (Durmuş ve Kasımoğlu, 2022: 18).

Dijital teknolojiler, uzun bir süredir sosyal ve kurumsal yapılarla iç içe geçmiş bir şekilde varlık göstererek, yaşamın pek çok yönünü köklü bir şekilde dönüştürmektedir. Dijitalleşme, dijital teknolojilerin sosyal ve organizasyonel yapıları dönüştürdüğü, bu yapıları dijital iletişim ve medya olanakları doğrultusunda yeniden şekillendirdiği ve hatta farklı işlevlerle donattığı evrimsel bir süreci ifade etmektedir. (Heiets vd., 2022: 2). Dijitalleşme, toplumsal dönüşüm ve kültürel evrim sürecini simgelemektedir. Şirketler açısından bu durum, mevcut iş modellerinin yeniden yapılandırılmasını veya tamamen yeni iş modellerinin geliştirilmesini gerektirmektedir. Bu bağlamda, şirketlerin değişen dinamiklere uyum sağlayabilmesi için iş modellerini gözden geçirmeleri ve gerektiğinde yenilikçi stratejiler benimsemeleri önemlidir (Henriette vd., 2016: 2).

Artan rekabetin getirdiği yenilik arayışları ve tüketicilerin bu yeni ürünlere gösterdiği ilgi, yenilikçi ekonomi politikaları ve üretim stratejilerinin geliştirilmesine yol açmıştır. Böylece tüketici tercihleri sektörleri, sektörler teknolojileri, teknolojiler de tüketici tercihlerini etkilemiş ve sürekli bir döngü içinde olan dijital çağın tüketim alanını günümüzdeki konumuna yükseltmiştir. Günümüzde dijitalleşme kavramı birçok alanda; üretim, eğitim, finans, sağlık yayıncılık, eğitim, ticaret, finans gibi alanlarda kullanılmaya başlamıştır. Aynı zamanda bu alanlarda farklı uygulamaları ile ortaya çıktığı gibi tüketim alanında da kendini göstermektedir (Aksoy, 2014: 46).

Dijitalleşme süreci teknolojinin hızla gelişmelerinin ve ilerlemesinin ardından toplumlarla birlikte kurumların geçirdiği dönüşümün dijitalleşme olarak tanımladığı bir süreci oluşturmaktadır (Habibov, 2024:11). Davidsson ve arkadaşları (2016), dijitalleşme sürecini dört ayrı dalgada tanımlamıştır. İlk olarak 80'li yıllarda bilgisayarların topluma girişiyle birinci dalga başlamıştır. Daha sonra ikinci dalga, 90'lı yıllarda bilgisayar ve internet kullanımının yaygınlaşması ve bilgiye erişimin kolaylaşmasıyla devam etmiştir. Üçüncü dalga mobil internet erişimin her yerde

mümkün olması ile sürmüştür. Son olarak interneti sadece insanlar bilgiye erişmek veya paylaşmak için değil, ayrıca makineler, cihazlar ve araçlar gibi varlıklar tarafından da kullanılmaya başlanması ile dördüncü dalga başlamıştır.

Dijitalleşme kavramı, kaynaklarda pek çok şekilde tanımlanmış ve birçok bilimsel çalışmada ele alınmıştır. Dijitalleşme en basit ifadeyle, dijital teknolojilerin kullanılmasıdır (Srai ve Lorentz, 2019: 79). Cherkasova ve Slepushenko (2021: 129), dijitalleşme tanımını genişleterek, *"iş modellerinin yeniden yapılandırılması, iç ve dış süreçlerin yürütülmesi ile ilgili yaklaşımların değiştirilmesi"* şeklinde kapsamlı bir açıklama yapmışlardır. Dijitalleşme, bilgi teknolojileri veya dijital teknolojilerin mevcut iş süreçlerini yeniden şekillendirmek amacıyla nasıl kullanılabileceğini açıklamaktadır (Li vd., 2016: 2). Gartner BT Sözlüğünde ise dijitalleşme kavramı, *"bir iş modelini değiştirmek, yeni gelir ve değer yaratan fırsatlar sağlamak için dijital teknolojilerin kullanılması; dijital bir işletmeye geçiş süreci"* olarak açıklanmıştır (Gartner, 2024). Brennen ve Kreiss' e göre dijitalleşme "*toplumsal yaşamın birçok alanının dijital iletişim ve medya altyapıları etrafında yeniden yapılandırılma biçimi*" anlamına gelmektedir. (Brennen ve Kreiss 2016: 3).

Rekabette bir adım önde olmak isteyen kuruluşların teknolojileri benimsemek ve yenilikler için dijitalleşmesi gerekmektedir. Böylelikle çalışma alanının her sektörünü dönüştüren dijital devrime neden olacaktır (Gruia vd., 2020: 287). Marc Andreessen'in (2011) ünlü "yazılım dünyayı yiyor" söyleminde ifade ettiği gibi, artık her zamankinden daha fazla dünyanın veri tarafından desteklenen dijital tarafından yönetildiğini söyleyebilmek mümkündür. Dolayısıyla, hayatın her alanını dijitalleşme ve dijital teknolojilerin kullanımı ele geçirmeye başlamaktadır (İlcüş, 2018: 350). Dijitalleşmenin verdiği destekle beraber herhangi bir kuruluş rekabetçi kalabilmekte, üretkenliği artırabilmekte, müşterilerle yeni yollarla bağlantı kurabilmekte, üretim maliyetlerini azaltabilmekte, iş modelini ve yapısını dönüştürebilmektedir (Gruia vd., 2020: 287).

Bilgi yoğun süreçlerin dijitalleştirilmesiyle maliyetlerin %90'a kadar düşürülmesi ve geri dönüş sürelerinin birkaç kat daha iyileştirilebilmesi dijitalleşmenin potansiyel faydaları arasında yer almaktadır. Bunun yanı sıra, işletmelerin süreç performansını, maliyet sürücülerini ve risk nedenlerini daha iyi

anlamak için, kâğıt ve manuel süreçlerin yazılımla değiştirilmesi ve çıkarılabilecek verileri otomatik olarak toplamasına dijitalleşme olanak sağlamaktadır (Parviainen vd., 2017:64). İşletmelerin AR-GE ve yenilik faaliyetlerine etkin bir biçimde katılmaları; e-tedarik sistemleri, sosyal medya ve web siteleri gibi çeşitli içerik paylaşım platformları, giyilebilir cihazlar ve otomasyon teknolojileri gibi dijital teknolojilerin kullanımı yeni pazar fırsatlarından faydalanmalarına zemin hazırlamaktadır (Lupton, 2020: 10). Dijitalleşmenin potansiyel faydaları arasında değer yaratmadaki yenilikleri ve müşterilerle yeni etkileşim biçimlerini yanı sıra satış veya üretkenlikteki artışları da içermektedir (Matt vd., 2015: 339). Rekabet ortamında başarılı olmayı hedefleyen kurumlar, bu gelişme ve değişimin sonucu olarak dijital teknolojilerin potansiyellerini açığa çıkarmalı, dijital çağ için iş modellerini yeniden geliştirmeli ve uygulamalıdır (Legner vd., 2017: 123).

1.1.1.4. Dijital Dönüşüm

Bir kurumun dijitalleşmeye doğru ilerlediği sürecin en geniş ve yaygın aşaması dijital dönüşümü oluşturmaktadır. Dijitalleşme ve dijitalleştirme tanımlarını da içeren dijital dönüşüm, dijitalleşmenin de ötesine geçmektedir. Dijital dönüşüm özellikle işletmenin temel iş modelinin dijital teknolojinin kullanımı yoluyla değiştiği durumlarda, bir kurum olgusu ve çeşitli organizasyonel süreçleri içermektedir (Verhoef vd., 2021: 891). 1970'li yıllar dijital dönüşümün başlangıcı olarak tanımlanabilmektedir. Bu yıllarda bilgisayarlaşma, toplam kalite yönetimi, otomasyona dayalı üretim, BT gelişmesi, makine ve robotların kullanımı gibi pek çok kavram toplumsal hayata dahil olmuştur (Körpe, 2021: 110). Ancak dijital dönüşüm kavramına ilişkin literatür incelendiğinde evrensel bir kavram tanımlanamamıştır. Tablo 1.1.'de dijital dönüşümün yaygın tanımları özetlenmektedir:

Tablo 1.1. Dijital dönüşüme ilişkin literatürde geçen tanımlar

Yazar	Dijital Dönüşüm Tanımı
Stolterman (2004: 689)	"Dijital dönüşüm, dijital teknolojinin insan toplumunun her alanında uygulanmasıyla ilişkili değişiklikleri kapsar."
Martin (2008: 130)	"Dijital dönüşüm, bilgi ve iletişim teknolojilerinin, basit otomasyonların gerçekleştirildiği değil, iş dünyasında, kamu yönetiminde, insanların ve toplumun yaşamında kökten yeni kabiliyetlerin yaratıldığı durumlarda kullanılmasıdır."
Westerman vd. (2011: 5)	"Dijital dönüşüm, işletmelerin performansını veya erişimini kökten iyileştirmek için teknolojinin kullanılmasıdır."

Liu vd. (2011: 1728)	"Dijital dönüşüm, dijital teknolojileri ve iş süreçlerini dijital ekonomide bütünleştiren bir organizasyonel dönüşümdür."
Bharadwaj vd. (2013: 472)	"Dijital kaynakların etkin bir şekilde kullanılarak farklı değer yaratılmasını hedefleyen bir organizasyon stratejisi."
Fitzgerald vd. (2014: 2)	"Dijital dönüşüm, gelişmiş müşteri deneyimleri, sorunsuz operasyonlar veya yeni iş modelleri gibi önemli iş iyileştirmelerini mümkün kılmak için sosyal medya, mobil teknoloji, analitik veya gömülü cihazlar gibi yeni dijital teknolojilerin kullanılmasıdır."
Solis vd. (2014)	"Dijital dönüşüm, müşteri deneyimi yaşam döngüsünün her temas noktasında dijital müşterilerle daha etkili bir şekilde etkileşim kurmak için teknoloji ve iş modellerinin yeniden düzenlenmesi veya bunlara yeni yatırım yapılmasıdır."
Matt vd. (2015: 339)	"Dijital dönüşüm stratejileri farklı bir bakış açısı benimser ve farklı hedefleri takip eder. İş merkezli bir bakış açısıyla gelen bu stratejiler, yeni teknolojiler nedeniyle ürünlerin, süreçlerin ve organizasyonel yönlerin dönüşümüne odaklanır."
Schuchmann ve Seufert (2015: 31)	"Müşteri deneyimi yaşam döngüsünün her temas noktasında dijital müşterilerle daha etkili bir şekilde etkileşim kurmak için teknolojinin yeniden düzenlenmesi ve yeni iş modelleri."
Chanias ve Hess (2016: 3)	"Dijital teknolojilerin bir organizasyonda neden olduğu değişikliklerin yaygınlığını yansıtın."
Bondar vd. (2017: 33)	"Dijital dönüşüm, tüm ekonomik sektörlerin tutarlı bir şekilde ağ oluşturması ve bir adaptasyondur Aktörlerin dijital ekonominin yeni koşullarına uyum sağlamasıdır."
Parviainen vd. (2017: 64)	"Dijital dönüşüm, bir organizasyonda veya organizasyonun operasyon ortamında dijital teknolojilerin benimsenmesiyle oluşan çalışma biçimleri, roller ve iş tekliflerindeki değişiklikler olarak tanımlanmaktadır."
Kane (2017)	"Dijital dönüşümün en iyi anlaşılması, giderek dijitalleşen bir dünyada organizasyonun etkin bir şekilde rekabet etmesine yardımcı olacak iş süreçlerini ve uygulamalarını benimsemektir."
Hinings vd. (2018: 53)	"Dijital dönüşüm, kuruluşlar, ekosistemler, endüstriler veya alanlar içindeki mevcut oyun kurallarını değiştiren, tehdit eden, değiştiren veya tamamlayan yeni aktörler (ve aktör takımyıldızları), yapılar, uygulamalar, değerler ve inançlar ortaya çıkaran çeşitli dijital yeniliklerin birleşik etkileridir."
Davenport ve Westerman (2018)	"Dijital dönüşüm, iş yapma şeklinizi değiştirmeye yönelik devam eden bir süreçtir. Becerilere, projelere, altyapıya ve sıklıkla BT sistemlerini temizlemeye yönelik temel yatırımlar gerektirir. İnsanları, makineleri ve iş süreçlerini, beraberinde getirdiği tüm karmaşayla birlikte karıştırmayı gerektirir. Ayrıca hem dijital liderlerin hem de dijital olmayan liderlerin dönüşüm çabaları hakkında iyi kararlar aldıklarından emin olmak için en üstten sürekli izleme ve müdahale gerektirir."

Young ve Rogers (2019:683)	"Yaygın verilerden, bağlantılardan ve karar alma mekanizmalarından türetilen, teknoloji odaklı bir değişim süreci."
Warner ve Wager (2019: 344)	"Dijital dönüşüm, bir organizasyonun iş modelini, iş birliğine dayalı yaklaşımını ve kültürünü yenileyen veya değiştiren yetenekler oluşturmak için dijital teknolojilerdeki gelişmeleri kullanan devam eden bir stratejik yenilenme sürecidir."
Leyh vd. (2021)	"DT, dijital teknolojiler kullanılarak toplumun ve ekonominin temel dönüşümü anlamına gelir. DT'nin yalnızca sosyal, kültürel, yasal ve politik etkileri değil, aynı zamanda tüm kurumsal yapılar ve değer zincirleri için de sonuçları vardır. Şirketlerin DT'de başarılı bir şekilde ustalaşması için yeni iş modelleri, stratejiler, organizasyonel biçimler ve süreçlerin yanı sıra güçlü bir müşteri odaklılık gereklidir."

Kaynak: (Yazar tarafından oluşturulmuştur.)

Tablo 1.1'de görüldüğü üzere dijital dönüşüm kavramına ilişkin tanımların odak noktası yeni teknolojilerin benimsenmesi ve kullanımından; operasyonlarda, müşteri ilişkilerinde ve performansta iyileştirmelere, süreçlerde, yeni iş modelleri yaratılmasına kadar geniş bir dönüşümü kapsamaktadır. Markaların, kurumların, şirketlerin ve organizasyonların dijital çağa uyum sağlamak için dijital ve mobil gibi yeni toplumsal teknolojilerle geçiş yapma süreci dijital dönüşüm olarak tanımlanmaktadır (Gömükpınar, 2022: 11). Bireylerin, işletmelerin, nesnelerin ve makinelerin birbirleriyle sürekli iletişimde olduğu bu süreçte tüketici talepleri ve verinin değeri giderek daha önemli hale gelmekte ve bu da yeni iş modellerine geçişi zorunlu kılmaktadır (TÜSİAD, 2017: 13). Bu dönüşümün gerçekleştirilmesinde dijital dönüşüm; teknolojinin iş süreçlerine entegre edilmesi olarak düşünüldüğünde Endüstri 4.0. teknolojilerinin rolü büyüktür. Bu dijitalleşme yarışında şirketlerin ön sıralarda yar alabilmesi için bu teknolojileri iyi anlaması ve avantajlarının ve dezavantajlarının farkında olması gerekmektedir (Ünal, 2022: 6). Dijital dönüşüm sayesinde işletmeler operasyonel süreçlerini kolaylaştırmakta, rekabette avantaj sağlamakta, iş hacmini büyütmekte, iş süreçlerini hızlandırmakta ve verimliliğinin artırılmasını sağlamaktadır (Altuntaş, 2018: 8).

1.1.2. Dijital Dönüşümün Önemi

Dijital, geleceğin en önemli yapı taşlarındandır. Teknolojinin ilerlemesi katlanarak artmıştır ve günümüzde hemen hemen her sektör bu büyümeden etkilenmiştir. Ürün ve hizmetler de sürekli olarak yenilikler yapılmıştır. Bu yeniliklerle

işletmeler yeni fırsatlar yaratmak ve gelirleri arttırmak için önemli bir potansiyel elde etmişlerdir. Günümüzün pazar senaryosunda küçük oyuncular, daha büyük kuruluşların ilgi düzeyine gözdağı veren devrimci teklifleriyle büyük kuruluşlara meydan okumaktadır. Dolayısıyla, geleneksel kuruluşların değişime uyum sağlaması ve benimsemesi zorunlu hale gelmektedir. Bu noktada dijital olarak dönüşüm, onların yeni ve geliştirilmiş iş modelleri bulmalarına yardımcı olmakla kalmayacak aynı zamanda yerlerini korumalarına da yardımcı olarak bütün paydaşlar için değer yaratmaya yardımcı olacaktır (Shahi ve Sinha, 2020:17).

Dijital dönüşüm, bilgi teknolojilerinin yoğun kullanımı ile iş süreçlerinin para ve zaman tasarrufu sağlayarak bilgilerin hızla, dijital ortama taşınmasını ifade etmektedir. Dijitalleşme ve dönüşüm toplumsal hayatta birçok alanda kolaylık sağlamaktadır. Alışveriş yaparken, güvenlik sistemlerinde, ödeme sistemlerinde; aynı zamanda iş hayatında yer alan kâğıt, evrak gibi belge ve saklama yöntemlerinde dijitalleşme ve dönüşümün etkisi, hızlılığı ve kolaylığı görülebilmektedir. Yine dijital dönüşümün getirileriyle, gereksiz iş yükleri azalıp verimlilik artmakta; ekonomik avantajlar ve zaman kazanımları ile rekabette bir adım öne çıkılmasına olanak sağlanmaktadır (Kılcı, 2020).

Günümüzde kuruluşlar için dijital dönüşüm, giderek daha önemli bir süreç olarak görülmektedir ve kuruluşların faaliyetlerini sürdürebilmesi için kritik önem taşımaktadır. Toplumlar arasında dijital teknolojilerin yaygınlaşması, iş süreçlerinde, iş modellerinde ve kurumsal kültürde farklı değişikliklere neden olmaktadır (Kő vd., 2019: 371). Teknoloji ve düzenlemelerdeki hızlı değişimler, talep ve rekabet gibi faktörler, kurumların ortamlarına uyum sağlayabilmelerini ve yanıt verebilmelerini her zamankinden daha önemli hale getirmektedir. Bu açıdan, kurumların iş stratejilerini çevredeki teknolojik değişikliklerle uyumlu hale getirmede; büyük veri ve analitik, gömülü cihazlar, 3d baskı, nesnelerin interneti sosyal medya, bulut bilişim ve yapay zekâ gibi yeni dijital teknolojiler giderek önem kazanmış ve bu teknolojilerin kurumlar üzerinde baskısı önemli hale gelmiştir. Bu dijital teknolojiler, “kuruluşların stratejik bağlamını kökten dönüştürmektedir: rekabetin yapısını, müşterilerin davranışlarını ve beklentilerini, işin yürütülme biçimini, ürünlerin üretilme ve hizmetlerin sunulma biçimini, çalışma biçimini ve nihayetinde tüm endüstrilerin doğasını” derinlemesine

değiştirmektedir (Teichert, 2019: 1673). Bu doğrultuda, dijital dönüşümün üç ana hedefi vardır. Bunlar aşağıdaki gibi açıklanmaktadır (Saray, 2024: 4):

1. *Karlılığı geliştirme:* Kar oranı farklı ve çok sayıda ürünün hızlı bir şekilde üretilerek artmasıdır. Ürünlerin üretim sürecinin hızlanması giderlerde düşüşü sağlar ve taleplere daha kolay yanıt verilmesine olanak tanımaktadır. Bunun sonucunda gelir ve karlılıkta artış sağlanmaktadır.
2. *Rekabet avantajı sağlama:* Piyasada kısa süre içerisinde yüksek ve çeşitli standartlı ürün üretilebilmesi sayesinde rekabet açısından avantaj sağlanmaktadır. Bu teknoloji özellikle kişisel istekler özelinde ürünlerin üretilmesi ve müşterilere ürünlerin çabuk tesliminin sağlanması açısından kullanan kurumlara avantaj sunacaktır. Bu dönüşüme uyum adapte olamayan kurumlar ise ciddi riskler ve zorluklarla karşılaşmaktadır.
3. *Yeni gelir yaratma:* Yeni alanların ve ürünlerin geliştirilmesinde ileri teknolojilerin kullanılması kazançlarda artışı tetiklemektedir. Dijital ikiz ve 3D teknolojisini kullanan yazıcılar gibi yeni uygulamalarla birlikte farklı ürünlerin geliştirilmesi oldukça kolaylaşmıştır. Bu da çeşitli ürünlerin hızlı bir şekilde piyasaya sürülmesini ve yeni kazanç olanaklarının elde edilmesini sağlamaktadır.

Yenilikçi teknoloji ve dijital çözümlerin entegrasyonu sayesinde kuruluşlar daha iyi hizmetler sunabilmektedir. Ayrıca, dijital dönüşüm kurumlara yalnızca bugün değil gelecekte de sürdürülebilir rekabet avantajı sağlayan dinamik bir süreçtir. Doğru şekilde uygulandığında kurumlar; verimliliklerini artırma, sürekli yenilik yapma ve müşteri beklentilerine uyum sağlamada dijital dönüşümün avantajlarından yararlanabilmektedir (Aksoy, 2024: 12).

1.1.3. Dijital Dönüşümün Tarihsel Gelişimi

Teknolojik gelişmeler, tarihsel süreç içerisinde sunduğu yeni talep ve tüketim seçenekleri ile üretim süreçlerinde önemli değişikliklere yol açmıştır. Bu değişiklikler, istihdam biçimlerini etkileyerek, aynı zamanda bireylerin yaşam tarzlarında da dönüşümlere neden olmaktadır (Aksoy, 2012: 402). Sanayi Devrimi, toplumsal ve ekonomik yapıları köklü bir şekilde dönüştüren bir olgu ve gelişme süreci olarak

nitelendirilebilir. Bu çerçevede, sanayi devriminin başlangıcından bu yana gelişen teknolojiler, üretim verimliliğinde önemli sonuçlar elde edilmesine olanak sağlamıştır (Bloem vd., 2014: 11). Endüstriyel devrimler, ekonomik gelişmelere hayati katkılarda bulunmuş ve hızla evrilen teknolojiler sayesinde günümüzün dijital ve yapay zekâ temelli üretim sistemlerinin itici gücü haline gelmiştir. Bu nedenle, endüstriyel devrimlerin önemi büyük bir şekilde ortaya çıkmaktadır (Koç ve Teker, 2019: 305).Bu kısımda, 18. yüzyılın ikinci yarısında başlayan ve günümüze kadar devam eden sanayi devrimlerinin tarihsel dönüşümü ve özellikleri incelenmiştir.

Şekil 1.2. Endüstrinin gelişim evreleri

Kaynak: (Laurent, 2020: 128) *uyarlanmıştır.*

Şekil 1.2'de görüleceği üzere genel bir değerlendirme yapıldığında, endüstri dönemi tarihsel süreç içerisinde dört ayrı dönemde araştırılabilir. Endüstriyel 1.0 dönemi, su ve buhar gücünün kullanımını içeren devam eden üretim faaliyetleri olarak nitelendirilmektedir. Ardından, elektriğin keşfi ve seri üretime geçilmesi Sanayi 2.0 dönemi kapsamında incelenmiştir. İnsan hayatı üzerine teknolojideki ilerlemelerin ve bu ilerlemelerin etkisinin artmasıyla birlikte çok farklı teknolojik ve dijital ürün ve hizmetler geliştirilmiştir. Bu gelişme Sanayi 3.0 dönemi çerçevesinde tanımlanmaktadır. Mevcut teknolojik gelişmelerin ve satışların bir adım ileri taşındığı, ürünlerin interneti, bulut teknolojisi, yapay zekâ gibi bilişimini kapsayan endüstriyel devrim ise Endüstri 4. 0, olarak ele alınmaktadır.

1.1.3.1. Endüstri 1.0

Birinci sanayi devriminden bu yana, yıllar boyunca insanlık, gelişmek için bir araç olarak teknolojiyi kullanmanın potansiyelini anlamıştır (Mourtzis vd., 2022: 1). İngiltere'de ortaya çıkan ve ilk olarak Avrupa'ya ardından da tüm dünyaya yayılan Birinci Sanayi Devrimi, sanayileşmenin başlangıcı olarak kabul edilmektedir. Birinci sanayi devriminin temel amacı, su ve buhar gücünün daha verimli bir şekilde kullanımına dayanmaktadır. Bu devrim, üretim sürecinde insan emeği yerine makine kullanımını sağlamış ve üretimin fabrikalara taşınmasına neden olmuştur. Birinci Sanayi Devrimi ile buhar gücü, çimento, demir, madencilik, aletler, tarım, kâğıt, tekstil, gaz, kimyasallar, cam, ulaşım ve aydınlatma gibi sektörlere odaklanılmıştır. Tarımsal kalkınma, ulaşım, istihdam edilebilirlik ve sürdürülebilir büyüme bu devrimin başarıları arasında yer almaktadır (Akundi vd., 2022: 2). Çok fazla faktör sanayi devriminin ilerlemesinde etkili olmuştur. Ancak buhar, kömür ve demir en önemli faktörler arasında yer almaktadır. Birinci Sanayi Devrimi döneminde kömür ve buhar gücünün kullanılmaya başlamasıyla, demiryollarında hızlı bir gelişim sağlanmıştır. Bu sayede Avrupa ülkelerinde, yeni hammadde kaynaklarına erişebilirlik daha kolay hale gelmiş ve ağır sanayide büyüme fırsatları artmıştır. En önemlisi ulaşımın kolaylaşması ile, hammaddeye erişim kolaylaşmıştır. Bunun sonucunda hızlı ve çeşitli ürünlerin büyük miktarlarda uzak pazarlara ulaştırılması mümkün olmuştur. (Gabaçlı ve Uzunöz, 2017: 151). Böylelikle, Birinci Sanayi Devrimi'nde meydana gelen gelişmeler, diğer endüstri devrimleri ve süreçlerinin ortaya çıkmasına katkıda bulunmuştur (Taş, 2018: 1821).

1.1.3.2. Endüstri 2.0

1840- 1870 yılları arasında montaj bantlarıyla gerçekleştirilen iş bölümü temelli seri üretime geçiş İkinci Sanayi Devrimi (Endüstri 2.0) olarak tanımlanmaktadır. Bu devrimin temel taşlarını elektrik enerjisinin kullanımı ve 1870 yılında Cincinati'de mezbahalarda uygulanan seri taşıma oluşturmuştur. Ford T'nin 1914 yılında tasarladığı seri üretim bandı, üretimi artırıp maliyetleri düşürmüştür. Bu devrimde gelişen elektrikli ve içten yanmalı motorlar endüstriyel üretimi merkeziyetsiz hale getirmiştir. Sendikaların önemini işçilerin refah talepleri ve sosyal gerilimler artırmış ve tüketim odaklı toplumun temelini atmıştır. ABD, Japonya,

Almanya ve İngiltere'nin öncülüğünde çelik ve demirin yaygın kullanımıyla ağır sanayi gelişmiştir (Derya, 2018: 3). İkinci sanayi devrimi daha çok elektrik ve içten yanmalı motorlarla ilgili olup, 19. yüzyılda mekanik üretim sistemlerinin elektrifikasyonuna odaklanmıştır. Elektrik, üretim için suya ihtiyaç duyan buharla kıyaslandığında, üretimde daha kolay kullanılabilmekte ve bu sayede elektrik transferi çok daha basit hale gelmektedir (Kumar vd., 2024: 2). Daktilo, ucuz gazete kâğıdı, radyo ve telefon gibi haberleşme araçlarının kullanılması dönemin haberleşme araçlarında sağlanan gelişmelerdir. Bu gelişmeler iletişimin daha etkin ve hızlı bir şekilde sağlanabilir hale gelmesine neden olmuştur (Pamuk ve Soysal, 2018:3).

1.1.3.3. Endüstri 3.0

20. yüzyılın ortalarında Endüstri 3.0 diğer adıyla Üçüncü Sanayi Devrimi başlamıştır. Otomasyon çağı olarak da bilinen bu dönem; elektronik, internet, üretim ve otomasyon kullanımına dayanmaktadır. Sanayileşmeye önemli iyileştirmeler getirmesine rağmen Endüstri 3.0, karmaşık sistemlerin kullanılması ve bu sistemlerin belirli koşullarda çalışmaması, gibi birçok sebepten dolayı kurum için ek maliyetlere neden olmuştur (Tunji-Olayeni vd., 2024: 3). 1960'lı yıllarda Üçüncü Sanayi Devrimi başlamıştır. Bu devir; yarı iletkenlerin, ana bilgisayarların (1960'lı yıllar), kişisel bilgisayarların (1970 ve 80'li yıllar) ve internetin (1990'lı yıllar) katalizörlüğünde geliştiğinden dolayı genellikle bilgisayar devrimi olarak tanımlanmaktadır (Schwab, 2017: 16). Üçüncü Sanayi Devrimi'nin ana faktörü internettir. İnternet, bilgisayar donanımı, yazılımı ve telekomünikasyondaki teknolojik gelişmeleri mümkün kılarak, kurumların kendilerini ve iş yapma şekillerini yeniden keşfetmeye teşvik etmiştir. Çalışma uygulamalarındaki bu dönüşüm hem yeni pazarların yaratılması hem de verimlilikteki gelişmelerle birlikte üretkenlikte benzeri görülmemiş kazanımlara sebep olmuştur. Ayrıca, internet insanların kendilerini ifade etme, birbirleriyle iletişim kurma ve eğlenme şekillerini de derinden değiştirmiştir (Smith, 2001: 2). Üçüncü Sanayi Devrimi, internet, dijitalleşme ve otomasyon ile daha çok ilgilenmiştir. Bu dönemde internet hesaplamalar ve veri aktarımı için kullanılmaya başlanmış ve verilerin dijitalleşmesi gerçekleşmiştir (Kumar vd., 2024). Piyasaların doygunluğa ulaşmasına neden olan Üçüncü Sanayi Devrimi'nin ardından gelişmeler sürekli farklılaşma ve bireyselleşme eğilimine girmiştir. Bu süreçte makineler, iş hayatında olduğu gibi

günlük yaşamda da önemli bir rol oynamaya başlamıştır. Bunun sonucunda insan gücüne olan ihtiyaç azalmıştır. İlk defa 2011 yılında Almanya'nın Hannover şehrinde düzenlenen fuarda "Endüstri 4.0" terimi öne sürülmüştür (Derya, 2018: 3). Bu döneme kadar üç sanayi devrimi birlikte değerlendirildiğinde; sanayi devrimleri arasında geçen sürenin oldukça kısaldığı, bir önceki devirle kıyaslandığında üretimde emeğe olan ihtiyacın azaldığı saptanmıştır. Bu bağlamda emek yoğun teknolojinin artık sermaye yoğun teknoloji ile yer değiştirmesi ve insan emeğinin giderek sermaye ile ikame edilmesi günümüzde nitelikli insan kaynağını ihtiyacını artırmaktadır (Koca, 2020: 4541).

1.1.3.4. Endüstri 4.0

İlk olarak 2011 yılında Hannover Fuarı'nda Endüstri 4.0 tanıtılmıştır. Daha sonra 2013 yılında, Almanya'nın imalat sektöründe devrim yaratan endüstrilerde öncü rol üstlenmek amacıyla stratejik bir girişimi olarak resmen duyurulmuştur (Xu vd., 2018: 2941). İnsan, makine ve ürün arasındaki gerçek zamanlı iletişim Endüstri 4.0'ın en önemli özelliğidir. Bu bağlamda Endüstri 4.0, esneklik çerçevesinde bağlantı tanımları oluşturması ile ürün ve hizmet satın alan kişilerin isteklerine göre özelleşmiş ve dijitalleşerek akıllı bir imalat modelini gerçekleştirmiştir (Fırat ve Fırat, 2017:10).

Farklı aşamalara dağılmış endüstrinin evrimi eşit derecede önem arz etmektedir. Bu aşamalar sırasıyla; Birinci, İkinci, Üçüncü ve Dördüncü Sanayi Devrimi olarak tanımlanmaktadır. Daha önce gerçekleşen sanayi devrimlerinden Endüstri 4.0'ın tamamen habersiz yeni bir model olduğunu söylemek doğru olmaz. Aslında, önceki sanayi devrimlerinin tüm temellerini tam olarak Endüstri 4.0 kullanmaktadır. Ancak diğer devrimlerden Endüstri 4.0; dijitalleştirme, teknolojiler, sanallaştırma, daha yüksek entegrasyon oranları ve uyaranlara hızlı yanıt süreleri ile farklılık göstermektedir. Günümüzde endüstrinin her aşaması birçok değişiklik ve iyileştirmeye maruz kalmıştır. Bu durum müşteri taleplerinin, insanların çalışmalarının, geliştirilen ürünlerin, dağıtım yollarının ve iç ve dış yönlerin değişmesinden kaynaklanmaktadır. Potansiyelinin tam olarak kullanılması için Endüstri 4.0'ı ve farklı alanlardaki tüm yeteneklerini bilmek önemlidir. Ayrıca, Endüstri 4.0'ın yeni sunduğu tüm yeni fırsatları bilmek endüstride iş birliği elde etmek isteyenler için önemlidir (Ortiz vd., 2020: 3).

Endüstri 4.0 şirketlerin ve organizasyonların makineler, tedarik sistemleri, üretim ekipmanları, nihai ürünler ve müşteriler arasında iletişim kurma yeteneğini geliştirmek için dijital teknolojilerin entegrasyonunu sağlamaktadır (Sharifabadi vd., 2024: 356). Rupp vd. (2021: 12) literatürde Endüstri 4.0'ı tanımlamak için en sık kullanılan kelime öbeklerinin genel görünümünü bibliyometrik analiz ile inceleyerek şu tanımı geliştirmiştir: *"Endüstri 4.0, akıllı fabrikalar oluşturmak için siber fiziksel sistemlerin, nesnelerin interneti, büyük veri, bulut bilişim, yapay zekâ ve iletişim teknolojilerini kullanarak, değer zinciri boyunca gerçek zamanlı bilgi ve iletişim sağlamak amacıyla uygulanmasıdır."* Mrugalska ve Wyrwicka (2017) ise Endüstri 4.0 kavramını, *"karmaşık fiziksel makine ve cihazların, ticari ve toplumsal sonuçları daha iyi tahmin etmek, kontrol etmek ve planlamak için kullanılan ağa bağlı sensörler ve yazılımlarla entegrasyonu"* veya *"ürünlerin yaşam döngüsü boyunca yeni bir değer zinciri organizasyonu ve yönetimi seviyesi"* olarak tanımlamaktadırlar.

Endüstri 4.0'ın insanlık tarihine girmesi ile birlikte sanayide yeni bir dönüşümü; 3D yazıcılar, büyük veri, nesnelerin interneti, robotik teknolojiler, akıllı üretim, bulut bilişim ve yapay zekâ gibi alanlarda ortaya çıkan gelişmeler oluşturmaktadır. Ayrıca, büyük veri, IoT ve yapay Zekânın (AI) bir bütün olarak kullanılmasını Endüstri 4.0 teşvik etmektedir. Bu devrim, akıllı makinelerin yalnızca üretim hatlarının otomasyonunu sağlamak için değildir. Bununla birlikte belirli bir düzeydeki üretim sorunlarını anlamak ve analiz etmek, bunları asgari düzeyde insan müdahalesiyle çözmek için insan ve makinenin birbirleriyle iletişim kurabileceği bir ortam öngörmektedir. Bu devrimin başlangıçta çoğunlukla üretim endüstrilerini etkileyeceği düşünülmüştür. Ancak bu yenilikler hizmet sağlayıcıları, operasyon şirketlerini ve perakendecileri de etkilemiştir (Tjahjono vd., 2017: 1176).

Endüstri 4.0 tanımlanırken literatürde sık sık bileşenleri üzerinde durulmaktadır. Geleneksel sanayi üretiminin yerini alan Endüstri 4.0, sistemlerin verimli ve uyumlu bir şekilde çalışmasını sağlamaktadır. Bu sebeple Endüstri 4.0, bilgisayarlaşmanın ön planda olduğu dokuz bileşen üzerine kurulmuş bir yenilikçi yaklaşımdır. Şekil 1.3'te bu bileşenler detaylı olarak gösterilmektedir.

Şekil 1.3. Endüstri 4.0 ve bileşenleri
Kaynak: (Rüßmann vd. 2015: 2) uyarlanmıştır.

Sanayi üretkenliğin yükselişine teknolojik ilerlemeler neden olmuştur. Bu yeni dijital sanayi devrimi Endüstri 4.0 olarak tanımlanmış ve dokuz temel teknolojinin gelişimi ile ifade edilmiştir (Rüßmann vd., 2015: 1). Bu kavram çerçevesinde geliştirilen bileşenlerin detayları, çalışmanın ilerleyen bölümlerinde incelenmiştir. Bu bileşenler, Endüstri 4.0'ın temel özelliklerini oluşturmaktadır, ancak sanayi devrimi sürecinde sağladığı avantajların yanı sıra siber güvenlik sorunlarını da beraberinde getirmiştir.

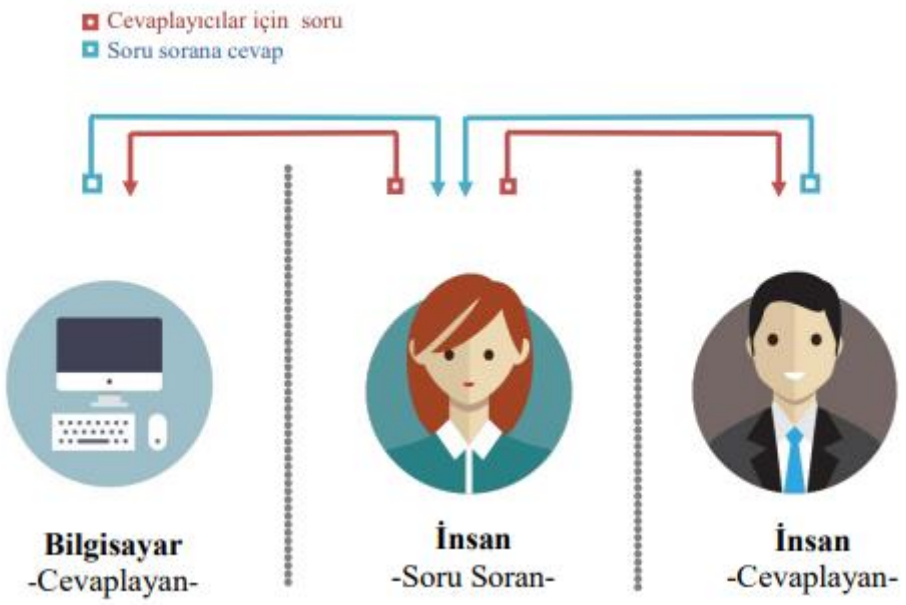
1.1.4. Dijital Dönüşüm Teknolojilerinin Çok Yönlü Analizi

Bu bölümde, dijital dönüşüm süreçlerini destekleyen teknolojiler detaylı bir şekilde ele alınmıştır.

1.1.4.1. Yapay Zekâ

Bir makine veya sistem tarafından insan zekasının simülasyonunun ifade edilmesi yapay zekâ olarak tanımlanmıştır. Yapay zekânın amacı insan davranışlarını taklit edebilen; insanlar gibi düşünebilen ve algılama, öğrenme, tahmin

etme, muhakeme etme, planlama, vb. dahil olmak üzere özellikleri taşıyan makine ve teknolojileri geliştirmektir (Xu vd.,2021: 1). 1950 yılında bilgisayar bilimcisi ve İngiliz matematikçi olarak bilinen Alan Turing yayınlamış olduğu "Computing Machinery and Intelligence" adlı makalesinde, Turing Testi olarak bilinen bir test ile bir makinenin düşünüp düşünemeyeceğini belirlemek için kullanılmasını önermiştir (Turing, 1950). Önerilen Turing testi, "*bir makinenin insan davranışlarından ayırt edilemeyen davranışlar sergileme yeteneğini test etmeyi"* amaçlamaktadır (Jannai vd., 2023: 1). Bu test, bir bilgisayarın insan benzeri düşünme yeteneğine sahip olup olmadığını anlamak için tasarlanmış bir yapay zekâ sorgulama sistemidir. Test zamanı iki insan katılımcısı ve bir bilgisayardan oluşan üç terminalden yararlanır. Bu sistemde, insan katılımcılardan biri soru sorarken, diğer insan ve bilgisayar, sorulara yanıt vermekle yükümlüdür. Belirli bir bağlam ve formatta soru soran kişi, sorularını yöneltir. Ardından, hangi yanıtın insana, hangisinin bilgisayara ait olduğunu belirlemesi istenir. Test, birden fazla kez tekrarlanır. Eğer bilgisayar, bu denemelerin en az yarısını kazanırsa, "zeki bir makine" olarak nitelendirilir (Arslan, 2020: 79). Turing testi süreci Şekil 1.4'te yer almaktadır:



Şekil 1.4. Turing Testi
Kaynak: (Arslan, 2020: 79).

Tarihsel sürece bakıldığında yapay zekânın temelleri oldukça eski dönemlere kadar uzanmaktadır. Bu adımları şu şekilde sıralamak mümkündür:

Tablo 1.2. Yapay Zekâ Tarihsel Gelişimi

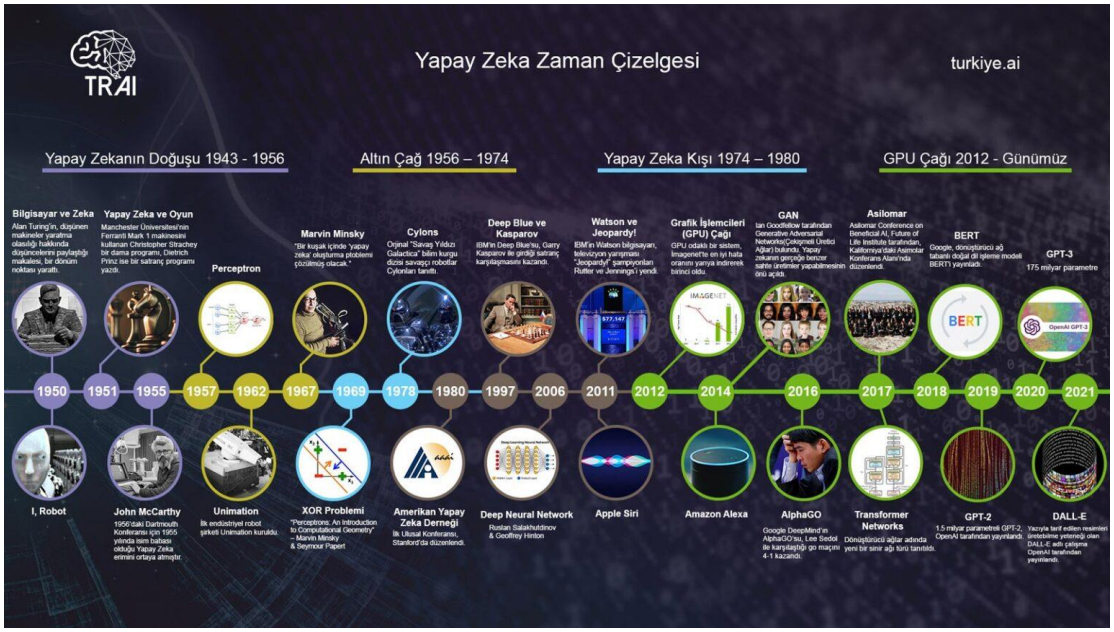
• 1923 - Londra'da sahnelenen Karel Čapek'in "Rossum'un Evrensel Robotları" (RUR) adlı oyununda "robot" kelimesi İngilizcede ilk kez kullanılmıştır.
• 1943 - Yapay sinir ağlarının temelleri atıldı.
• 1945 – Columbia Üniversitesi'nden mezun olan Isaac Asimov Robotik terimini icat etmiştir.
• 1950 - Turing testi, Alan Turing tarafından zekânın değerlendirilmesi için geliştirilmiştir ve Computing Machinery and Intelligence'ı yayınlamıştır. Claude Shannon, bir araştırma olarak Detailed Analysis of Chess Playing eserini yayınlamıştır.
• 1956 - John McCarthy, yapay zekâ terimini ortaya atmıştır. Carnegie Mellon Üniversitesi'nde ilk yapay zekâ (AI) programının gösterimi yapılmıştır.
• 1958 - John McCarthy, yapay zeka için LISP programlama dilini icat etmiştir.
• 1964 - Danny Bobrow'un MIT'deki tezi, bilgisayarların doğal dili cebirsel kelime problemlerini doğru bir şekilde çözebilecek kadar iyi anlayabildiğini göstermiştir.
• 1965 - MIT'de Joseph Weizenbaum, İngilizce diyalog içeren etkileşimli bir problem olan ELIZA'yı geliştirmiştir.
• 1969 - Stanford Araştırma Enstitüsü'ndeki bilim insanları, hareket, algılama ve problem çözme yetenekleriyle donatılmış Shakey adlı robotu geliştirmiştir.
• 1973 - Edinburgh Üniversitesi'ndeki Montaj Robotik grubu, görme duyusunu kullanarak modelleri bulma ve birleştirme yeteneğine sahip Ünlü İskoç Robotu Freddy'yi inşa etmiştir.
• 1979 - İlk bilgisayar kontrollü otonom araç olan "Stanford Cart" üretilmiştir.
• 1985 - Harold Cohen, Aaron çizim programını yaratmış ve tanıtmıştır.
• 1990 - Yapay zekanın tüm alanlarında önemli ilerlemeler: o Makine öğreniminde önemli gösteriler o Vaka tabanlı akıl yürütme o Çoklu ajan planlama o Zamanlama

- Veri madenciliği, Web Tarayıcısı
- Doğal dil anlama ve çevirisi
- Görme, Sanal Gerçeklik
- Oyunlar

- 1997 - Deep Blue isimli Satranç Programı, dönemin dünya satranç şampiyonu Garry Kasparov'u yenmiştir.

- 2000'ler - Etkileşimli robot evcil hayvanlar ticari olarak satışa sunuluyor. MIT, duyguları ifade eden bir yüze sahip bir robot olan Kismet'i sergilemiştir. Nomad adlı robot Antarktika'nın uzak bölgelerini keşfediyor ve meteorları tespit etmiştir.

Kaynak: (Gür vd., 2019: 145-146).



Şekil 1.5. Yapay Zekâ Zaman Çizelgesi
Kaynak: Türkiye Yapay Zeka İnisiyatifi (TRAI), https://turkiye.ai/kaynaklar/yapay-zeka-zaman-cizelgesi/, (Erişim Tarihi: 05.11.2024).

Şekil 1.5'te yapay zekâ alanındaki yaşanan önemli dönüm noktalar gösterilmiştir. Yapay zekâ çalışmaları tarih boyunca, "*Yapay zekâ yazı/ baharı"* olarak adlandırılan dönemlerde büyük bir ilgi ve popülarite kazanmıştır. Ancak bazı dönemlerde; *"yapay zekâ kışı"* olarak bilinen duraklama evrelerinde bu ilginin azaldığı görülmüştür. Bu nedenle yapay zekâ araştırmalarında bu terimler, zaman içerisindeki iniş ve çıkışları özetlemektedir.

Dartmouth Koleji'nde 1956 yılında düzenlenen bir konferansta yapay zekâ kavramı, McCarthy tarafından ilk kez kullanılmıştır (Mijwel, 2015: 2). Yapay zekâ;

makinelerin insan gibi düşünme ve hareket etmesini sağlamak için yapılan ve araştırmalara konu olan kavramdır. Bu alanda geçmişten günümüze birçok kuruluş ve kişi araştırmalarını sürdürmektedir. Ayrıca, yapay zekâ kavramı ile ilgili benzer ama birbirinden farklı tanımlamalar da yapılmıştır. McCarthy J'ye göre (1988: 308); *"Yapay zekâ, mevcut bilginin belirli bir karmaşık karaktere sahip olduğu durumlarda hedeflere ulaşma yöntemleriyle ilgilenir. Kullanılması gereken yöntemler, durumun sunduğu sorunla ilgilidir ve sorun çözücünün insan, Marslı veya bilgisayar programı olması fark etmeksizin benzerdir"*. Nilsson (2009) ve Russell ve Norvig'e (2022) göre, Yapay Zekâ (YZ), bilgisayar biliminin alt alanıdır. *Akıllı varlıkların inşa edilmesi, yani bu varlıkların çevrelerinde uygun ve öngörülü bir şekilde işlev görmelerinin sağlanması görevini ele almaktadır* (Wäschle vd., 2022: 3). Ginsberg yapay zekâ kavramını, *"akıllı bir eser inşa etme girişimi"* olarak tanımlamaktadır (Ginsberg, 2012: 3). Haugeland (1985) ise yapay zekayı, *bilgisayarları düşünmeye iten, tam ve gerçek anlamda zihinleri olan makineler olması için heyecan verici çabalamalar* olarak tanımlamıştır. Russel ve Norvig' e göre ise yapay zekâ, "*akıllı varlıkları anlamak ve bunları taklit ederek karar verme sürecini basit, hızlı ve verimli hale getirmek için tasarlanmış bir mantık sistemidir*." (Russel ve Norvig, 2016: 1).

Genel olarak bakıldığında tanımlara bakıldığında yapay zekâ araştırmalarının temel amacı, insanlara özgü zekâ ve akla dayalı davranışları makinelerde gerçekleştirebilmektir. Bir başka deyişle yapay zekâ, makineleri daha akıllı hale getirerek onların daha faydalı ve verimli hale gelmesini sağlamaktır.

1.1.4.2. Nesnelerin İnterneti (IoT)

ARPANET'in başlangıcından bu yana geçen kırk yıl sürecinde, "internet" kavramı, dünya çapında milyarlarca kullanıcıya 7/24 hizmet veren ve birbiriyle bağlantılı bilgisayar ağlarından oluşan, çok kapsamlı bir uygulama ve protokol sistemini ifade etmektedir. İnsanlık artık her yerde bağlantı ve iletişimin bir hayal veya zorluk olmadığı bir çağı yaşamaktadır. Günümüzde odak noktası, fiziksel alanı insan yapımı sanal ortamlarla birleştirmek için insanların ve cihazların sorunsuz bir şekilde entegre edilmesine doğru kaymıştır. Bu süreçte, "Nesnelerin İnterneti" (IoT) ütopyası yaratılmıştır. Bu olgu daha detaylı incelendiğinde, IoT'nin daha fazla açıklama gerektiren iki önemli sütunu ortaya çıkmaktadır; "internet" ve "nesneler". İlk olarak

"nesneler" kategorisine internete bağlanabilen her nesnenin gireceği gösterilmiştir. Bu tanımlama, insanlar arasında iletişim kurabilen; akıllı cihazlar, sensörler her zaman her yerden erişilebilir hale gelen daha genel varlık kümelerini kapsamak için kullanılır. Bu nedenle, herhangi bir zaman veya yer kısıtlaması olmadan nesnelerin erişilebilir olması gerekmektedir (Khodadadi vd., 2016: 2).

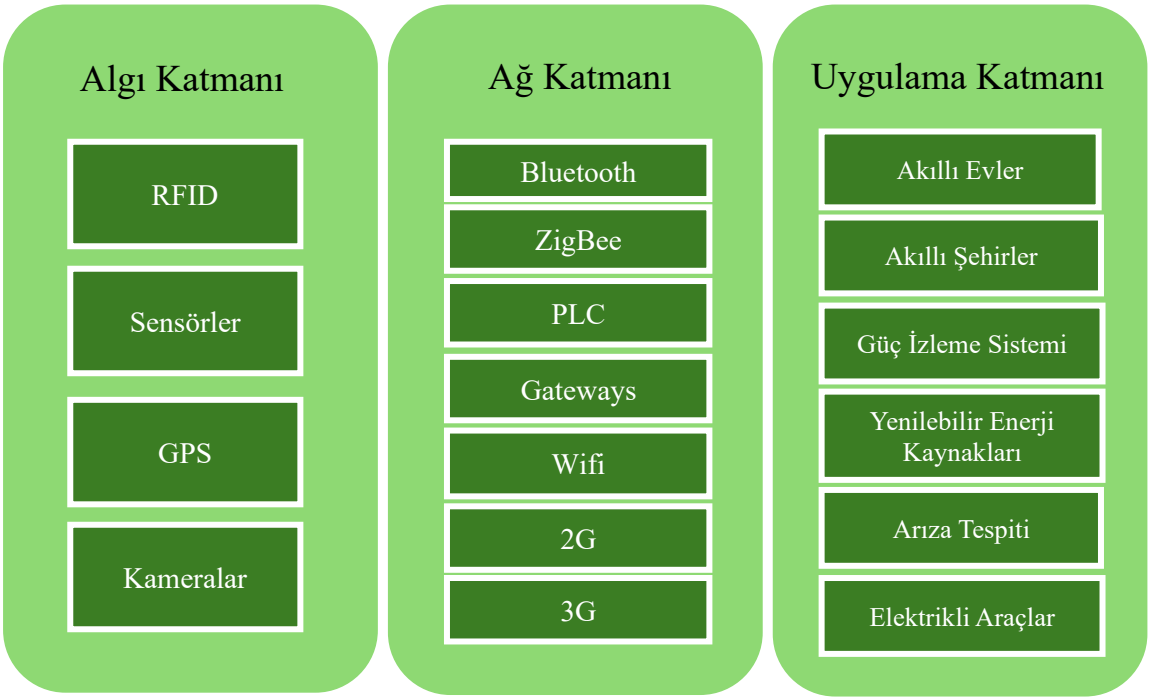
İlk olarak 1999 yılında Procter & Gamble (P&G) şirketinde Kevin Ashton tarafından yapılan sunumun başlığında "Nesnelerin İnterneti" kavramı kullanılmıştır (Ashton, 2009). 1991 yılında tarihteki ilk kez nesnelerin interneti uygulaması, İngiltere'de Cambridge Üniversitesi'nde bir grup akademisyen tarafından bir adet kahve makinesinin birlikte kullanılması gösterilmektedir. Akademisyenler çalıştıkları yerin üst katında bulunan kahve makinesini her seferinde boş bulmaktan sıkılmışlardır. Bu nedenle kahve makinesinin dakikada, üç kez görüntüsünü alan ve bu görüntüleri kendi bilgisayarlarına aktaran bir sistem tasarlamışlardır. Bu kahve makinesi "Nesnelerin İnterneti" kavramının uygulamada ilk örneği olarak bilinmekte ve bağlı nesnelerin varlığının kanıtı oluşturmaktadır (Kutup, 2011: 1).

Şekil 1.6. Nesnelerin İnterneti İlk Uygulama Örneği
Kaynak: (Kutup, 2011:1).

Dünyadaki hemen hemen her fiziksel şeyin aynı zamanda İnternet'e bağlı bir bilgisayara dönüşebileceği, Nesnelerin İnterneti'nin temel fikrini oluşturmaktadır (ITU, 2005). Daha doğru bir ifadeyle, nesneler bilgisayara dönüşmezler. Ancak minik bilgisayarlara sahiptirler. Bu özelliklere sahip olan nesneler, akıllı nesneler olarak

tanımlanırlar. Çünkü etiketlenmemiş nesnelerden daha akıllı davranabilmektedirler (Fleisch, 2010: 3).

Fabrika katından hastane ameliyathanesine ve konut bodrumuna kadar sayısız ağa bağlı, otomatik cihaza bağlanma, iletişim kurma ve uzaktan yönetme IoT yeteneğini oluşturmaktadır. Ayrıca IoT, günlük nesnelere bilgi işlem iletişim ve depolama teknolojilerinin yerleştirildiği bir senaryodur. Bir nesneye eklenen iletişim, işleme ve depolama yeteneklerinin yerleştirilmesi nesneyi kullanıcıların kullanım başına ödeme yaptığı bir hizmete dönüştürmektedir (Navani vd., 2017: 473). Nesnelerin interneti şekil 1.7' de gösterildiği gibi Algı Katmanı, Ağ Katmanı ve Uygulama katmanından oluşur (Wu vd., 2010: 484).



Şekil 1.7. Nesnelerin İnterneti Teknolojisinin Katmanları
Kaynak: (Talari vd., 2017: 2) uyarlanmıştır.

A. Algı Katmanı

Algı Katmanı, IoT'nin yüz derisi ve beş duyu organını oluşturmaktadır. Esas olarak nesneleri tanımlamak ve bilgi toplamak için kullanılmaktadır. Algı Katmanı; RFID etiketleri ve okuyucu-yazıcılar, 2 boyutlu barkod etiketleri ve okuyucuları, GPS, kamera, terminaller sensörler ve sensör ağını kapsamaktadır.

B. Ağ Katmanı

Ağ katmanı, IoT'nin beyni ve sinir ağını oluşturmaktadır. Esas görevi bilgiyi işlemek ve iletmektir. Ağ katmanı; bir iletişim ve internet ağının birleşme ağını, ağ yönetim merkezini, akıllı işleme ve bilgi merkezini içermektedir. Ağ katmanı, algı katmanından elde edilen bilgileri iletmek ve işlemektedir.

C. Uygulama Katmanı

Uygulama Katmanı, IoT'nin sosyal bölünmesi ve endüstri talebinin birleşimini oluşturmaktadır. Kapsamlı entelektüelleştirilmeyi gerçekleştirmeyi amaçlamaktadır. Ayrıca, endüstri teknolojisinin ve IoT'in derin birleşmesini ifade etmektedir. Uygulama katmanı entelektüelleştirilmiş endüstriyi gerçekleştirmek için endüstri ihtiyaçlarıyla birleşmektedir. Bu kişinin sosyal iş bölümüne benzer, sonunda insan toplumunu oluşturmaktadır (Wu vd., 2010: 484).

GPS, lazer tarayıcılar, RFID'ler (radyo frekansı kimliği) ve kızılötesi sensörler gibi bilgi algılama ekipmanlarını Nesnelerin interneti, birbirine bağlayarak bilgi alışverişinde bulunmayı ve İnternet üzerinden iletişim kurmayı sağlamaktadır. Bu iletişimi Nesnelerin İnterneti; akıllı tanımlama, izleme konumlandırma ve bilgi yönetimi ile gerçekleştirebilmektedir. Genel ve teknik bağlantı için Nesnelerin İnterneti; nesneden nesneye, nesneden bilgisayara ve bilgisayardan bilgisayara kullanılabilmektedir (Bao, 2016: 168).

Nesnelerin İnterneti her geçen gün daha da ilerleyen bir kavram olması nedeniyle (Internet of Things (IoT)) için birçok tanımı bulunmaktadır. Nesnelerin İnterneti'nin en yaygın tanımı şu şekilde tanımlanmaktadır: Nesnelerin İnterneti (IOT), "fiziksel nesnelerden oluşan bir ağdır" (Patel ve Patel, 2016: 6122). Nesnelerin İnterneti (IoT), geleceğin internetinin entegre bir parçasıdır. Ayrıca, Nesnelerin İnterneti; Fiziksel ve sanal "şeylerin" kimliklere, fiziksel niteliklere ve sanal kişiliklere sahiptir. Nesnelerin İnterneti, akıllı arayüzler kullandığı ve bilgi ağına sorunsuz bir şekilde entegre edildiği, standart ve birlikte çalışabilir iletişim protokollerine dayalı kendi kendini yapılandırma yeteneklerine sahip dinamik bir küresel ağ altyapısı olarak tanımlanabilmektedir (Guillemin ve Friess 2009: 6). Nesnelerin İnterneti kavramına ilişkin diğer tanımlamalar ise şu şekildedir:

- Genellikle Nesnelerin İnterneti terimi ağ bağlantısının ve hesaplama yeteneğinin normalde bilgisayar olarak kabul edilmeyen günlük eşyalara, sensörlere ve nesnelere, kadar uzandığı ve bu cihazların asgari insan müdahalesiyle veri üretmesine, alışverişinde bulunmasına ve tüketmesine olanak tanıyan senaryoları ifade etmektedir. Ancak, evrensel ve tek bir tanımı yoktur (Rose vd., 2015: 1).
- Karmaşık süreçlerin keyfi mesafeler üzerinden hassas bir şekilde izlenmesini ve kontrol edilmesini ve sağlayan Endüstriyel Nesnelerin İnterneti (IoT), akıllı sensörlerden oluşan dağıtılmış bir ağ olarak tanımlanmaktadır (Huberman, 2016:1).
- İnternet altyapısındaki her nesnenin dinamik, küresel ve genişleyen bir ağ halinde birbirine bağlı olması kavramı nesnelerin interneti olarak tanımlanmaktadır (Farash vd., 2016: 1).
- Saatler, oyuncaklar, sağlık monitörleri, ev aletleri vb. gibi çok çeşitli cihazlarda ağ ve bilişimin kullanılması eğilimini Nesnelerin İnterneti (IoT) kavramı tanımlamaktadır (Siever ve Rogers, 2016).

Farklı tanımlara sahip olmakla birlikte, Nesnelerin İnterneti'nin, genellikle sahip olduğu özellikler bu şekilde tanımlanabilir (Bao, 2016: 168):

Bağlantı: Nesnelerin internetinin özüdür. Nesnelerin İnternetinde bağlantının üç yönü bulunmaktadır; her zaman bağlantısı, her yer bağlantısı ve her şey bağlantısı.

Teknoloji: Nesnelerin interneti, merkezi işleme, mikro işleme teknolojisi ve yazılımı, RFID, kablosuz sensör ağları (WSN), akıllı gömülü ve bulut sistemler dahil olmak üzere güçlü teknolojilerle desteklenmesi gerekmektedir.

İstihbarat: Nesnelerin internetinin birçok şeyi birbirine bağlaması gerekmektedir. Ayrıca, Nesnelerin internetinin sadece şeyleri algılaması değil, aynı zamanda çevreyi veya insanların ince duygusal değişimlerini de algılamasını gerektirecek durumlar olmaktadır. Bunun için de zekâ ve işlem gücü gerekir.

Nesnelerin İnterneti; acil durumlar, lojistik, endüstriyel kontrol, alışveriş, güvenlik, akıllı şehirler, akıllı enerji, akıllı hayvancılık, akıllı tarım, akıllı ölçüm, akıllı

çevre, akıllı su, ev otomasyonu ve e-sağlık gibi uygulamalarda kullanılmaktadır. Bu alanlarda daha yüksek kaliteli hizmet sunmak, üretkenlik ve verimliliği artırmak amacıyla sensörler aracılığıyla gerekli veriler toplanmaktadır. Bu veriler Bulut Bilişim sistemlerinde Büyük Veriyi oluşturarak depolanmaktadır. Makine Öğrenimi yöntemleriyle bu veriler analiz edilmekte ve ilgili iyileştirmelerin yapılmasına katkı sağlamaktadırlar (Gökrem ve Bozuklu, 2016: 49). Kullanım erişilebilirlik ve kolaylığı açısından Nesnelerin interneti, çok alanda yaygın olarak kullanılmaktadır. Bu teknoloji örnekleri Şekil 1.8' de gösterilmektedir.

Şekil 1.8. IoT teknolojileri ile örnek uygulamalar
Kaynak: (Gökrem, 2016 akt. Bıçakçı, 2019).

Micoach Akıllı Top: Bu top sayesinde, hangi ayakla kaç gol atıldığı, maçlarda kaç penaltının gol olduğu ve kaç kilometre hız ile vurulduğu gibi bilgiler uygulama üzerinden takip edilebilmektedir.

Nest:2014 Ocak ayında Google tarafından 3,2 milyar dolara satın alınan bu uygulama ofisler ve evlerin sıcaklığı dışarıdan kontrol edilebilmektedir. Herhangi bir acil durumda uygulamanın sahip olduğu duman dedektörü kullanıcıları uygulama üzerinden haberdar etmektedir.

Babolat: Bu ürün, akıllı bir raket olarak ifade edilmektedir. Tenisle ilgilenenler; topa vuruş açılarını, hangi el ile hangi stil ile vurdukları ve vuruş hızlarını takip edebilmektedir. Oyunun ardından da uygulama üzerinden istatistikleri anlık olarak kullanıcıyla paylaşmaktadır.

Edyn: Bahçeler için geliştirilmiştir. Toprağın hangi aralıklarla sulanması, ne ekilmesi ve nasıl ekilmesi gerektiği konularında kullanıcıya öneriler vermektedir.

Dropcam: Nest tarafından satın alınmıştır. Yaşam alanlarına kurulan kameralar sayesinde bilgisayarlar ve akıllı telefon üzerinden izleme imkânı vermektedir. Görüntülerin kameralar tarafından belleğe kaydediliyor olması sistemin avantajları arasında yer almaktadır.

August: Bir akıllı kilit üreticisidir. Kapıda kalmak kavramını akıllı cep telefonu sayesinde ortadan kaldırmaktadır.

Hapifork: Akıllı bir çataldır. Gün içerisinde fazla yemek tüketildiğinde veya hızlı yemek yendiğinde kullanıcıları uyarır ve insanların düzenli beslenmesini desteklemektedir.

Smart Things: Akıllı evlerde en çok tercih edilen ürünlerden birisidir. Akıllı telefon üzerinden desteklenen aygıtlarla ürün entegre edilmektedir. Sabah uyanıldığında çay veya kahve yapılabilmekte, ya da eve gelindiğinde ışıklar veya ihtiyaç duyulan nesne otomatik şekilde açılabilmektedir.

Ring: Amazon tarafından satın alınmış akıllı zil üreticisidir. Evin içerisinde olmadan da eve kimlerin geldiğini bu zil üzerinden görülebilmektedir (Bıçakçı, 2019: 27-29).

1.1.4.3. Büyük Veri (Big Data)

Bilgisayarın 20. yüzyılın ikinci yarısından itibaren hızlı gelişimine bağlı olarak yaygınlaşan dijital teknolojiler, insan yaşamında büyük bir değişim ve dönüşümün yaşanmasına neden olmuştur. Dijital teknolojilerin kullanılmasıyla insanlar günlük

yaşamlarındaki işlerini daha verimli ve basit şekilde halletmeye başlamıştır. Ayrıca, insanların bilgiye ulaşım hızı yaşanan bu gelişmeler neticesinde artmış ve daha önce hiç olmadığı kadar geniş bilgi kümeleri oluşmaya başlamıştır. Bu kadar hızlı bilgi birikiminin oluşmasını internetin gelişimiyle açıklamak mümkün olmaktadır. Bugünkü toplumsal yaşamda hemen her konuyla ilgili bilgiye internet üzerinden ulaşılabilmektedir. Aynı zamanda, insanların bilgiye ulaşım şekillerini de internet değiştirmiş ve bireylere daha kolay bilgi edinebilme imkânı sağlamıştır. Bu durum yalnızca bireylere özel değil kurumlar için de geçerli olmaktadır. Toplumsal yaşam içerisinde internetin sunmuş olduğu imkanları devletler de dahil olmak üzere bütün kurumsal yapılar sonuna kadar kullanmaktadır. Ayrıca, kurumsal yapılar internetten temel bir ifadeyle veri veya bilgi kaynağı olarak istifade etmektedir (Ergen, 2018: 54).

Milyarlarca telefondan, internet işlemlerinden, ödeme sistemlerinden, e-postalardan, tıklama akışlarından, sosyal ağ hizmetlerinden, sensörlerden, kameralardan, videolardan ve çeşitli araçlardan büyük veriler üretilmektedir (Sun ve Huo, 2021: 1). Toplanan veriler, "bankacılık, halkla ilişkiler, pazarlama, bankacılık, güvenlik vb. pek çok alanın yanında araştırmacıların yaptıkları araştırmalarda da kullanılabilir nitelik taşıyabilmektedir". Bu veriler, büyük bir kapasite, hız, çeşitlilikte üretilmekte ve artış göstermektedir. Bu verilerin işlenip fayda sağlayabilecek enformasyona dönüştürülebilmesi için teknolojik çözümlerin desteğine ihtiyaç duyulmaktadır. Bunun sonucunda da büyük veri kavramı ortaya çıkmıştır (Doğan ve Arslantekin, 2016: 15). Günümüz teknolojisinin insan hayatına getirdiği uygulamalar, cihazlar, internet vb. unsurların ortaya çıkardığı devasa veri kümelerinin boyutlarını anlaşılır kılmak için veri birimlerinin boyutu Tablo 1.3' te yer almaktadır.

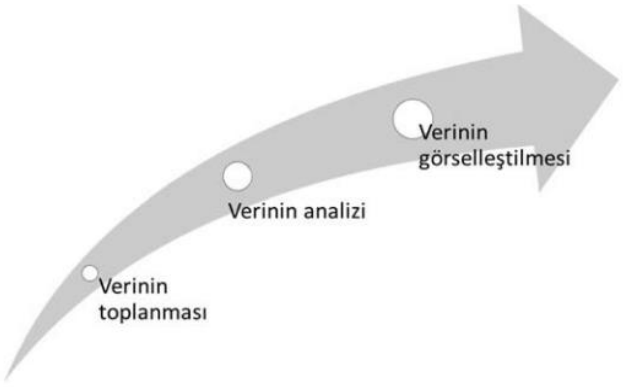
Tablo 1.3. Veri birimlerinin boyutları

Ad	Eşittir	Bayt cinsinden boyu
Bit	1 bit	1/8
Nibble	4 bits	½
Bayt	8 bits	1
Kilobayt	1024 bayt	1024
Megabayt	1024 kilobayt	1,048,576
Gigabayt	1024 megabayt	1,073,741,824
Terabayt	1024 gigabayt	1,099,511,627,776
Petabayt	1024 terabayt	1,125,899,906,842,624
Exabayt	1024 petabayt	1,152,921,504,606,846,976
Zettabayt	1024 exabayt	1,180,591,620,717,411,303,424

Yottabayt	1024 zettabayt	1,208,925,819,614,629,174,706,176

Kaynak: (Chen ve Zhang, 2014: 336).

Veri geçerliliği; verilerin doğruluğu anlamına gelmektedir. Verilerin oynaklığı kavramı, verilerin uzun ömürlülüğü ve analiz sonuçlarıyla alakalılığı ile ilişkilidir. Verinin uzunluğu; kavramı ise uygun katma değerli analiz için verileri kullanışlı bir biçimde depolamak için gereken başka özelliklerdir. Bu özelliklere ilave olarak, herhangi bir organizasyonda Büyük Veri'nin değerini açığa çıkarmak için gereken üç aşama bulunmaktadır. Bunlar, "veri toplama", "veri analizi" ile "görselleştirme ve uygulama"dır (Daniel, 2015: 6).



Şekil 1.9. Büyük Verinin Üç Temel Aşaması
Kaynak: (Daniel, 2015: 6).

Toplama: Büyük Veri'den elde edilen değeri açığa çıkarmanın ilk adımını veri toplama almaktadır. Bu, değerli ve yararlı bilgileri ortaya çıkarabilecek verilerin belirlenmesini gerekmektedir. Alaka düzeyine göre verilerin filtrelenmesi ve yararlı bir biçimde saklanması gerekmektedir. Çünkü içerisindeki verilerin büyük kısmı kullanılmazsa büyük miktarda veriye ve depolama altyapısına yatırım yapmanın getirisi oldukça düşük olmaktadır.

Analiz: Eyleme dönüştürülebilir bilgiler üretmek için veriler kullanılabilir bir biçime dönüştürüldükten sonra, analiz edilmesi, gerekmektedir. Fakat, verilerin doğasındaki artan çeşitlilikler sebebiyle, çeşitli veri kümelerini yönetmek ve analiz etmek çok karmaşık bir süreç haline gelmektedir. Bu veriler tarafından iletilmesi gereken bilgileri kavrayabilmek için farklı veri kümelerini ilişkilendirmek ve bağlamak analiz ile

yapılmaktadır. Bu sebeple bu durum, Büyük Veri'nin 'karmaşıklığı' olarak adlandırılmaktadır.

Görselleştirme ve uygulama: *A*naliz edilen verilerin yorumlanabilir ve mevcut süreçlere entegre edilmiş bir biçimde kullanıcılara sunulmasını ifade etmektedir. Neticede karar almaya rehberlik etmek için kullanılan son aşamayı oluşturmaktadır (Daniel, 2015: 5).

Literatürde "Büyük veri" kavramıyla ilgili pek çok tanım yapılmıştır. Manyika ve diğerleri (2011), büyük veriyi; "*veritabanı yazılım araçlarının, bilgilerini toplayabileceği, depolayabileceği, yönetebileceği ve analiz edebileceğinden daha büyük veri kümeleridir.*" şeklinde tanımlamıştır. Kaur ve Sood (2017)'in tanımına göre; *"büyük veri, son teknoloji veri işleme platformlarının bile işleyemediği kadar çeşitli ve büyük veri kümeleri olarak"* adlandırılmıştır. Stylianou ve Talias (2017) yapmış oldukları tanıma göre: "*Büyük veri elde edilmiş çeşitli veri türlerinin hacim olarak terabayt ya da daha üstü olması ile bir sürü yönlerle dağıtılması"*dır. Raja, Mukherjee ve Sarkar (2020) büyük veriyi "*çok geniş ve karmaşık olan geleneksel veri tabanı sistemleri tarafından işlenmesinin zor olduğu kümeler"* olarak ifade etmişlerdir. Miah, Camilleri ve Vu (2022) ise; "*Büyük veri, yapılan bir işlem ile çabukça oluşan ve oluşan şeyin analiz olup büyük hacimli bir veri haline gelmesidir"* şeklinde bir tanım yapmışlardır. 'Büyük veri' kavramını daha iyi anlamak için onu oluşturan temel bileşenler üzerinde durmak gerekir. Büyük verinin 5V'si (Bkz. Şekil 1.10) olarak adlandırılan bu bileşenler: Büyüklük (volume), çeşitlilik (variety), hız (velocity), değer (value) ve doğruluk (veracity)'dir.

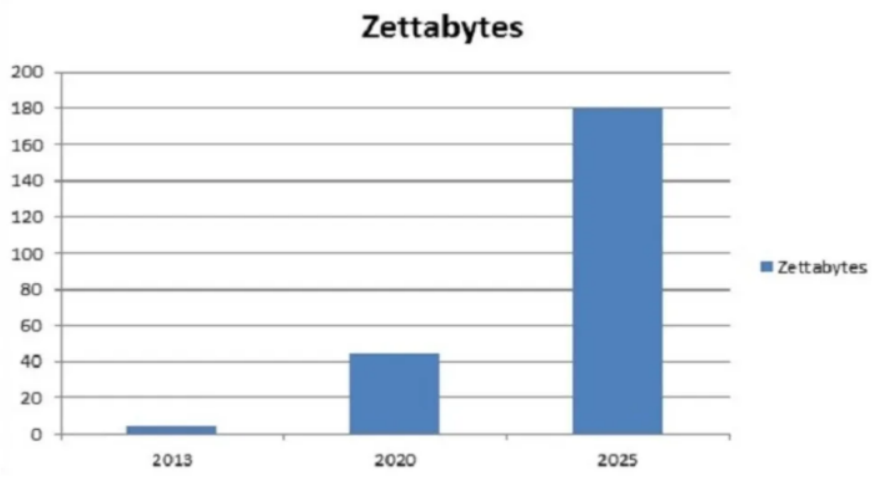
Şekil 1.10. Büyük Verinin 5V' si

Hacim (Volume): Tüm kaynaklardan oluşturulan verilerin boyutunu tanımlamaktadır (Nuaimi, 2015: 4). Bilgi ve iletişim teknolojilerinin hızlı bir şekilde gelişmesiyle birlikte çoğu şirket, her yerde çekilen trilyonlarca fotoğraftan veya sosyal

medya hizmetleri aracılığıyla belge paylaşım hizmetlerinden, YouTube'a yüklenen yüzlerce saatlik videodan, küresel mobil trafikten milyarlarca gigabayttan, günlüklerden ve her olası sensörden gelen veri veya bilgi biçiminde arşivlenmiş "Veri Okyanusu" büyüklüğüne sahiptir (Hussien, 2020: 19).

Aktaş (2024)'e göre; "*Her gün 328,77 milyon terabayt veri üretilmektedir. İnternet veri trafiğinin yaklaşık %53,72'si videolar aracılığıyla oluşturulmaktadır. Twitch'te 480p bir video için saatte 0,405GB ve 0,54GB veri gerekiyor. Twitter'da kullanıcılar tarafından her gün 2 milyar video izleniyor. WhatsApp'ta bir mesaj paylaşmak için Kilobaytlarca veri gerekiyor. 2024 yılında her gün yaklaşık 361 milyar e-posta gönderiliyor. Bir kısa mesaj göndermek için 0,0001335 MB veriye eşdeğer bir veri kullanılıyor.*"

Veri hacmindeki hızlı artış, verilerin yapılandırılmasını, anlamlı bilgilere dönüştürülmesini ve analizini zorunlu kılmaktadır. Dünya genelinde 2025 yılına kadar 181 zettabayt veri üretilmesi beklenmektedir (Aktaş, 2024).



Şekil 1.11. Zettabytes Veri Miktarı
Kaynak: (Aktaş, 2024).

Hız (Velocity): Geçmiş zamana göre veri çok daha hızlı üretilmektedir. Duran statik verilerden gerçek zamanlı ve akışkan dinamik veri üretim sürecine geçilmiştir. Günümüzde gerçekleştirdiği faaliyetleri kayıt altına alabilen birbirlerine kablosuz veya kablolu bağlanan, birbirleriyle haberleşen ve internete bağlanabilen cihazların çoğunluğu veri üretebilmektedir (Doğan ve Aslantekin, 2016: 26). Veri ve içerikler kesintisiz bir şekilde oluşmakta ve aynı anda ilişkilendirilmektedir. Aynı zamanda bu veri ve içeriklere internet üzerinden erişim sağlanmaktadır. Veri akışları sosyal

paylaşım ağları aracılığıyla gerçekleşmekte ve kullanıcıların en küçük bir olaya anlık cevap vermelerini sağlamaktadır (Özcan, 2021: 17). Büyük verinin hız boyutu sadece verilerin üretildiği hızı değil, bununla birlikte analiz edilmesi gereken oranı da tanımlamaktadır. Gerçek zamanlı sensörlerin ve akıllı telefonların her yerde bulunması, akıllı evler gibi teknolojilerin geliştirilmesiyle çevremizle hızlı bir şekilde etkileşim kurma ihtiyacını da artırmaktadır. Bu nedenle Büyük Veri'nin hızı dikkate alınması gereken önemli bir faktör haline gelmiştir (L'Heureux vd., 2017: 7782).

Çeşitlilik (Variety): Online cihazlar, sosyal medya, Sensörler, vb. pek çok büyük veri kaynağı bulunmaktadır. Elde edilen veriler farklı farklı türleri içermektedir. Video ve kameralardan elde edilen görüntüler, GPS, cep telefonları, sosyal medya hesaplarından resim, video gibi içerikler, online akıllı cihazlar, sensörler, vb. yapılandırılmış, yarı yapılandırılmış ya da yapılandırılmamış formatta verilerin akışı söz konusu olmaktadır (Chen, vd., 2014: 173-174). Çoğunlukla yapısal olmayan ve farklı kaynaklardan farklı formatlarda elde edilen veriler üretilmektedir. Büyük ölçekli ve farklı formatlarda üretilen verileri, işlemek için ilişkisel veri tabanları yetersiz kalmaktadır. Bu nedenle yapısal olmayan veriler; veri madenciliği, doğal dil işleme, metin madenciliği vb. sistemler kullanılarak dönüştürülmekte, anlaşılabilir ve işlenebilir hale getirilmektedir. Aynı zamanda, yapısal olmayan verinin depolanabilmesini destekleyen ve dağıtık paralel işlem kabiliyetine sahip sistemlerin kullanımına da gerek duyulmaktadır (Zafar vd. 2016: 120).

Değer (Value): Büyük veri sistemlerinin faydasını, değer özelliği, kullanılabilirliğini ve kullanışlılığını tanımlamaktadır. Bu özellik, daha çok veri işleme ve veri analitiği ve süreçlerinin sonuçlarına yönelik bir kavramdır. Büyük veri sistemlerindeki diğer 5V'lerle doğrudan orantısı bulunmaktadır (Rehman vd., 2016: 267).

Doğruluk (Veracity): Büyük verinin doğruluk boyutu iki yönü içermektedir: İlk olarak istatistiksel güvenilirlikleriyle tanımlanabilen veri tutarlılığı (veya kesinliği); ikinci olarak ise, güvenilir altyapı ve tesis de dahil olmak üzere veri kökeni, toplama ve işleme yöntemleri gibi bir dizi faktörle tanımlanan veri güvenilirliği. Büyük veri doğruluğu, kullanılan verilerin güvenilir, yetkisiz erişim ve değişiklikten korunduğundan emin olmaktadır. Veriler, güvenilir kaynaklardan toplanmasından

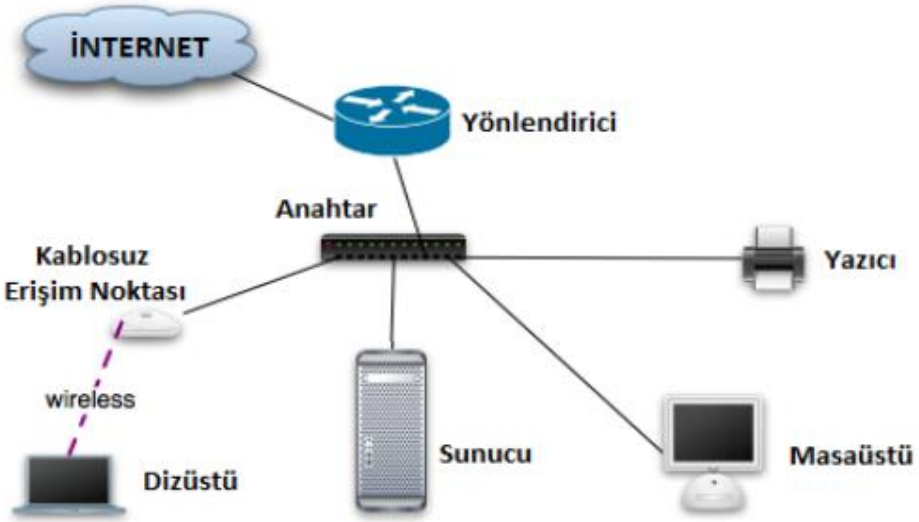
güvenilir bilgi işlem tesislerinde işlenmesine ve korumalı ve güvenilir depolama tesislerinde depolanmasına kadar tüm yaşam döngüsü boyunca güvence altına alınması gerekmektedir. Aşağıdaki yönler, veri doğruluğunu sağlamak için tanımlanmakta ve ele alınması gerekmektedir:

1. Verilerin ve bağlantılı verilerin bütünlüğü (örneğin, dağıtılmış veriler, karmaşık hiyerarşik veriler için)
2. Veri güvenirliği ve özgünlüğü
3. Hem kaynağın hem de verilerin tanımlanması
4. Bilgisayar ve depolama platformunun güvenilirliği
5. Zamanında olma ve kullanılabilirlik
6. İtibar ve hesap verebilirlik

Veri doğruluğu tamamen Büyük Veri altyapısından dağıtılan ve erişilebilen güvenlik altyapısına dayanmaktadır (Demchenko vd., 2013: 50).

1.1.4.4. Bulut Teknolojisi

İlgili altyapının karmaşıklığını gizlemek amacıyla kullanılan bilgisayar ağı diyagramlarından "Bulut'' terimi, türetilmiştir (Birje vd., 2017: 33). Bilişim sektöründeki "Bulut" kavramının karşılığı internet alanı olarak ifade edilmektedir. Bulut teknolojisi en sade tanımıyla; *"internet üzerinden erişime açık bulunan yazılım uygulamaları, veri depolama işlem ve hizmeti kapasitesi"* olarak tanımlanmaktadır. Bu teknolojide kullanıcılar bilişim alanında kullandıkları araçlara istedikleri zaman veya ihtiyaç duyduklarında erişim sağlayabilmektedir (Yıldırım ve Onay, 2013: 60).



Şekil 1.12. Bulut Bilişim Şekli
Kaynak: Korkmaz, 2010: 3

Şekil 1.12'de de gösterildiği gibi; bilgisayar ağı (network) diyagramlarında istemci ve sunucu bilgisayarlar, anahtar (switch), ağ geçidi (gateway) ve yönlendirici (router) vb. ağ elemanları ile beraber iletişim için aralarında oluşan bağlantılar gerçekleştirildikten sonra kalan kısımları ifade etmek için kullanılmaktadır (Korkmaz, 2010: 3).

Literatürde birçok yerde "bulut bilişim" tanımı geçmektedir. Bulut bilişimin tanımı Amerikan Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology (NIST)), tarafından şu şekilde yapılmıştır; "*Ağ, sunucu, uygulama, servisler ve depolama gibi düzenlenebilen bilgisayar kaynaklarına ait paylaşım havuzuna talebe uygun ağ erişimi sağlayan bir teknolojidir*" (Mell ve Grance,2011: 2). Buyya ve diğerleri (2009: 3), bulut bilişimini şu şekilde tanımlamıştır: "*Bulut, hizmet sağlayıcı ile tüketiciler arasındaki müzakereler yoluyla oluşturulan hizmet seviyesi anlaşmalarına dayalı olarak dinamik olarak sağlanan ve bir veya daha fazla birleşik bilgi işlem kaynağı olarak sunulan, birbirine bağlı ve sanallaştırılmış bilgisayarların bir koleksiyonundan oluşan bir tür paralel ve dağıtılmış sistemdir."* Foster ve diğerleri (2008: 1), bulut bilişimi "*Ölçek ekonomileri tarafından yönlendirilen, soyutlanmış sanallaştırılmış, dinamik olarak ölçeklenebilir, yönetilen bilgi işlem gücü, depolama, platformlar ve hizmetlerin bir havuzunun internet üzerinden harici müşterilere talep üzerine sunulduğu büyük ölçekli bir*

dağıtılmış bilgi işlem paradigması" olarak tanımlamıştır. Genel olarak bakıldığında, bulut bilişim, verilerin ve uygulamaların internet üzerinden erişilebilen uzak sunucularda depolandığı ve işlendiği bir teknoloji modeli olduğu ve Kullanıcılar, fiziksel altyapı kurmak zorunda kalmadan bu kaynakları ihtiyaçlarına göre kullanabilecekleri internet tabanlı bir yapıdır.

Kullanıcılar tarafından kolay erişim, performans, kullanım kolaylığı, hız ve verimlilik ve güvenlik gibi çeşitli nedenlerden dolayı Bulut bilişim çok tercih edilen popüler bir araçtır. Günümüzde birçok firma bulut bilişim hizmeti sağlamaktadır. Bunlara; Google, Microsoft, Amazon ve IBM örnek gösterilebilmektedir. Genellikle, kullanıcılara bulut bilişim sağlayıcıları, üç temel modelde hizmet sağlamaktadırlar. Bunlar; altyapı hizmeti (IaaS), yazılım hizmeti (SaaS) ve platform hizmeti (PaaS)'dir (Taşlı,2022: 5)

Altyapı Hizmetleri (Infrastructure as a Service – IaaS): Bulut bilişim sistemlerinin temel katmanı olarak Altyapı hizmetleri kabul edilmektedir. Hizmet Olarak Altyapı (IaaS) tüketicilere; ağ kaynakları ve diğer temel bilişim kaynakları işleme ve depolama alanı sunmaktadır. IaaS müşterileri, dinamik olarak hızla ölçeklenebilen altyapıya yazılım ve işletim sistemleri dağıtabilmektedir. Bulut IaaS'nin başlıca sağlayıcılarına örnek olarak; Amazon Web Services, Rackspace, GoGrid, HP, SoftLayer, Eucalyptus Community cloud ve IBM gösterilebilmektedir (Attiya ve Zhang, 2017: 33).

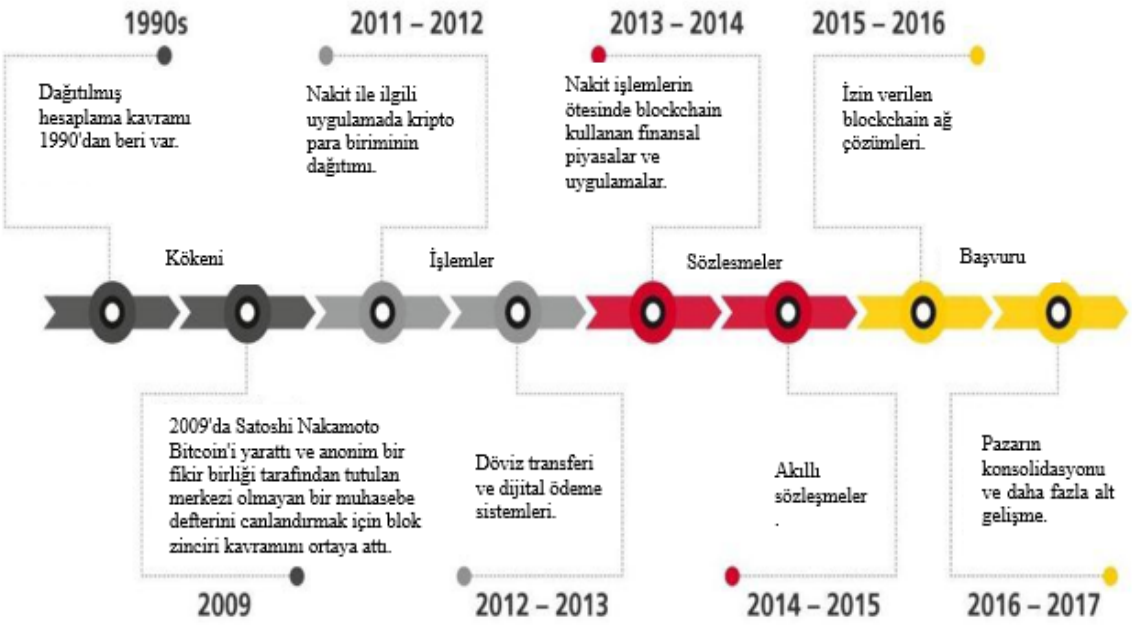
Yazılım Hizmetleri (Software as a Service – SaaS): Başkalarının geliştirdiği ve web üzerinden bir hizmet olarak sunduğu yazılıma erişmek için diğer kullanıcılar yalnızca bir web tarayıcısı kullanmaktadır. SaaS düzeyinde, kullanıcıların yazılımı barındırmak için kullanılan temel altyapı üzerinde kontrolü veya erişimi bulunmamaktadır. Salesforce'un Müşteri İlişkileri Yönetimi yazılımı3 ve Google Docs4, bulut bilişimin SaaS modelini kullanan popüler örnekler arasında yer almaktadır (Sriram ve Hosseini, 2010: 3).

Platform Hizmetleri (Platform as a Service – PaaS): Müşteri tarafından oluşturulan veya edinilen uygulamaları geliştirmek, test etmek, barındırmak ve dağıtmak için üst düzey entegre bir ortam ve çözüm yığınları sağlamaktadır. Bu

uygulama; tüketicilerin uygulamaları ve barındırma ortamı yapılandırılmalarını dağıtmalarına ve kontrol etmelerine izin vermektedir. Ancak, tüketicilerin ağ, sunucular, işletim sistemleri ve depolama gibi temel bulut altyapısı üzerinde hiçbir kontrolü bulunmamaktadır. PaaS'nin başlıca sağlayıcılarına örnek olarak; Amazon Web Services, Windows Azure, VMforce, Engine Yard, Heroku ve Google AppEngine ve vb. gösterilebilmektedir (Attiya ve Zhang, 2017: 33).

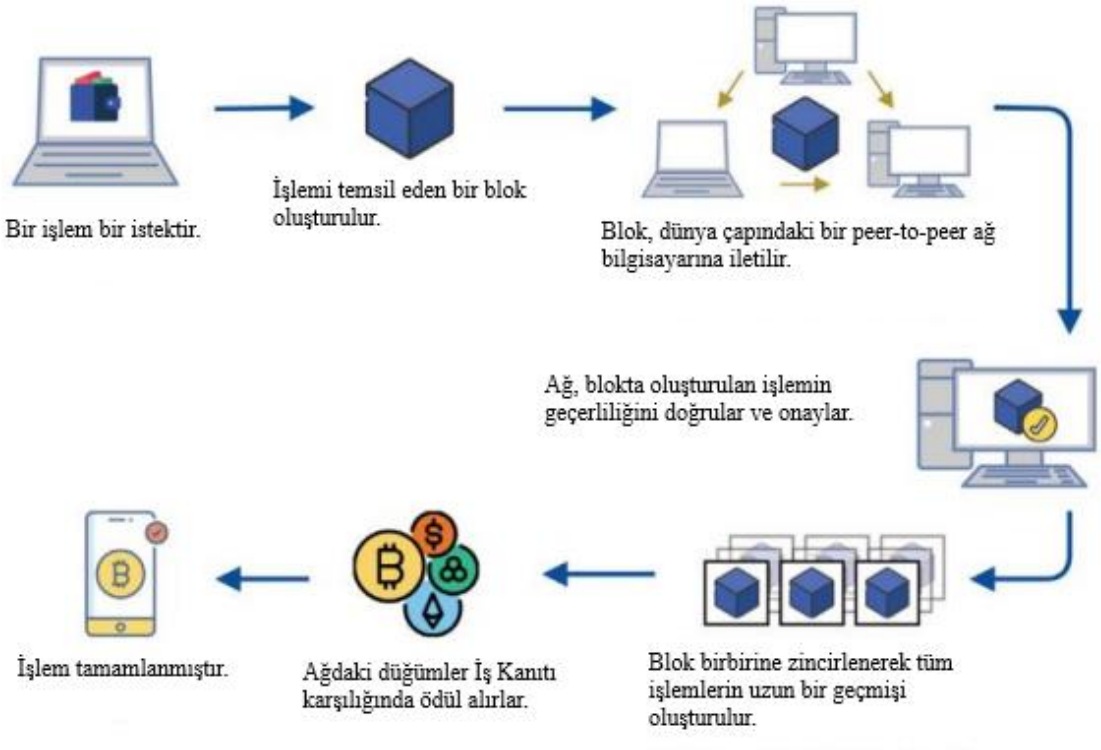
1.1.4.5. Blok Zinciri (Blokchain) Teknolojisi

Her şey 2008 yılında, Satoshi Nakamoto takma adıyla bilinen bir kişi ya da grup tarafından kripto paraların temellerinin atılmasıyla başlamıştır (Holotescu, 2018: 1). Şekil 1.13'te blok zincirinin tarihi kısaca gösterilmektedir. Blokzinciri teknolojisi, verilerin yüksek güvenlik önlemleriyle bir noktadan diğerine aktarılmasını, saklanmasını ve hızlı bir şekilde erişilmesini sağlayan, şifreli ve dağıtık bir dijital veri tabanıdır. Bu yapı, merkezi bir otorite (banka, hükümet veya diğer üçüncü taraflar) olmadan, dağıtılmış hesapların bulunduğu dijital defterlerdir. Genellikle açık kaynaklı olan bu teknoloji, bireylerin ya da grupların birbirleriyle gerçekleştirdiği her türlü dijital işlemin ve bilginin ana defter üzerine kaydedilmesini sağlamaktadır. Blokzincirinin temel yeniliği, ağın düzgün işleyişi sağlandığında, bu dijital defterdeki verilerin ve işlemlerin geri alınamayacak ve değiştirilemez şekilde kaydedilmesidir. Diğer bir ifadeyle, blokzinciri bloklar halindeki kriptografik olarak şifrelenmiş ve imzalanmış işlemlerin bulunduğu, dağıtılmış dijital defterlerdir (Özden, 2021: 277).



Şekil 1.13. Blockchain'in geçmişi
Kaynak: (Bucerzan ve Bejan, 2021: 2) *uyarlanmıştır.*

Blockchain teknolojisinin işleyişi şu şekilde özetlenebilir: Bir kullanıcı blockchain ağı üzerinde veri göndermek veya mevcut veriyi değiştirmek istediğinde, bu veri önce tüm ağdaki düğümlere (bilgisayarlar) iletilir. Ağdaki her bilgisayar bir "düğüm" olarak adlandırılmaktadır. Veriler, her bir düğüm tarafından bir blok haline getirilip ardından diğer düğümlere doğrulama için sunulmaktadır. Düğümler, bloğun doğruluğunu, güvenliğini ve protokollerle uyumunu kontrol etmek amacıyla matematiksel işlemler yapmaktadır. Eğer ağdaki çoğunluk bloğun doğru olduğuna karar verirse, blok şifrelenmektedir. Şifreleme sırasında her yeni blok, önceki bloğa ait şifreleme kodu içermekte bu da blokların birbirine zincirlenmesini sağlamaktadır. Yani, her blok hem kendisini hem de kendisinden önceki bloğu güvence altına almaktadır. Blockcahin ismi de buradan gelir, çünkü bloklar birbirine bağlı zincir gibi işleyişini göstermektedir. Son olarak, şifrelenmiş ve birbirine bağlı bu bloklar, ağdaki diğer bilgisayarlar tarafından onaylanır ve ağdaki blockchain zincirine eklenir. Bu işlem, verilerin değiştirilemez ve silinemez hale gelmesini sağlamaktadır (Kurnaz, 2021: 65).



Şekil 1.14. Blockchain teknolojisi ile işlenen bir işlemin gösterimi.
Kaynak: (Huynh-The vd., 2023: 404).

Blockchain teknolojisinin sunduğu başlıca avantajlar şunlardır (Grech ve Camilleri, 2017: 8):

Öz egemenlik: Kullanıcılar, kimliklerini tanımlama ve kişisel verilerini depolama ile yönetme konusunda tam kontrol sahibi olmaları;

Güven: Kullanıcılara, ödemeler veya sertifikalar gibi işlemleri gerçekleştirme konusunda yeterli güven sağlayan bir teknik altyapı sunması;

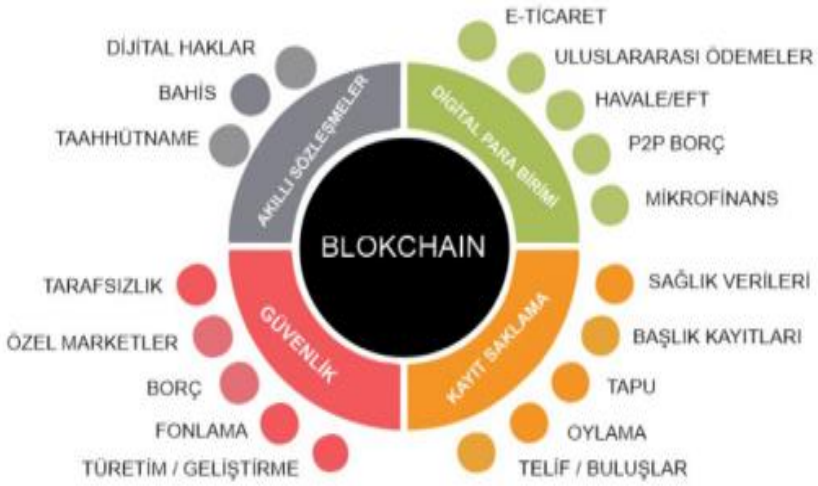
Şeffaflık ve Köken: İşlemlerin her iki tarafının da gerekli kapasiteye sahip olduklarından emin olarak işlem yapabilmesini sağlaması;

Değiştirilemezlik: Verilerin, geri dönülemez bir şekilde kaydedilip saklanması;

Aracısızlaştırma: İşlemleri yürütmek ya da kayıtları tutmak için merkezi bir otoriteye olan ihtiyacı ortadan kaldırması;

İş birliği: Tarafların, üçüncü şahıslara ihtiyaç duymadan doğrudan birbirleriyle güvenli bir şekilde işlem yapabilmesi.

Bu avantajlar, blockchain'in güvenli, verimli ve merkeziyetsiz yapısının kullanıcılar için sunduğu önemli faydaları göstermektedir. Blok zinciri teknolojisi, henüz tüm dünyada yaygın olmasa da verimlilik ve sosyo-ekonomik gelişmelere önemli katkılar sağlamaktadır. Bankacılık, lojistik, ticaret gibi birçok sektörde kullanılan bu teknoloji, karşılaşılan sorunların çözümünü kolaylaştırırken, taraflar arasındaki belge onay süreçlerini de güvence altına almaktadır. Özellikle finans sektöründe ödeme işlemleri, dijital kimlik yönetimi, para transferi, e-ticaret, hisse senedi işlemleri ve belge yönetimi gibi alanlarda benimsenmiş olup, aynı zamanda değerli belgelerin korunması, vergilendirme, bulut bilişim, dijital sözleşmeler ve dijital pasaport gibi birçok uygulama alanına sahiptir. Blok zinciri teknolojisinin kullanım alanları geniş yelpazeye yayılmaktadır.



Şekil 1.15. Blok Zinciri Kullanım Alanları
Kaynak: (Ünal ve Uluyol, 2020: 168).

Blok zinciri teknolojisi, kuruluşların merkezi bir otoriteye ihtiyaç duymadan güvenli bir şekilde işlem yapmalarını ve bilgileri yönetmelerini sağlayan bir araçtır. Bu teknolojinin uygulamaları, tüm işlemlerin kaydedildiği ve küresel olarak dağıtılan bir elektronik para sistemi şeklinde ortaya çıkmıştır. Bu sistemde, işlemler "kriptografik hash" algoritmalarıyla güvence altına alınır ve asimetrik anahtar çiftleri kullanılarak imzalanır ve doğrulanır. Yapılan tüm işlemler ve işlem geçmişleri blok zincirinde tutulur. Bir işlemde herhangi bir değişiklik yapılmak istendiğinde, sonraki tüm blokların yeniden hesaplanması gerekir, bu da mevcut verilerin değiştirilmesini

son derece zor ve maliyetli hale getirir. Bu özellik, blok zincirinin verilerin güvenliğini sağlama ve değiştirilemezliğini garanti etme yeteneğini pekiştirmektedir (Özden, 2021: 294).

1.1.4.6. Simülasyon Modelleri

Simülasyon; Türk Dil Kurumu Sözlüğü'nde "öğrence" ve "benzetim" olarak tanımlanmıştır (TDK, 2024). "Gerçek dünyanın var olan yönlerini çağrıştırarak veya yineleyerek yaratılan bir doğallık içinde tamamen katılımcı bir tarzda tanımlanması" simülasyon olarak ifade edilmiştir. Ayrıca, simülasyon "gerçek deneyimleri rehberli deneyimlerle değiştiren ya da geliştiren teknik" olarak tanımlanmaktadır (Gaba, 2004: 2). Landriscina (2013) göre simülasyon kavramı, "*günlük yaşamda var olan ya da var olma olasılığı bulunan durumların benzerinin dinamik bir yapı olarak ortaya konmasıdır"*. Simülasyon tanımını yapan diğer araştırmacılardan farklı olarak Landriscina simülasyonun tanımını; insanların zihinlerinde kurguladıkları bir şeyin durağan olmayan şekilde insan zihninde canlandırılmasını da bilgisayar temelli olabileceği olarak ele almıştır (Doğru, 2020: 23).

Gerçekte var olan ilişkilerin, görevlerin, ekipmanların, bazı bilişsel aktivitelerin ve davranışların gerçeğe uygun şekilde taklit edilmesi simülasyon olarak ifade edilmektedir. Yani, simülasyon gerçeğe en yakın şekilde yaşanmış olmaktadır. Gerçek dünyada var olan tüm olası durumlar simülasyon senaryosunda hem psikolojik hem fiziki olarak taklit edilmekte ve gerçekliğe uygun şekilde katılımcının hareket edebileceği bir ortam sağlanmaktadır. Bir konudaki yetkinliği ve ustalığı değerlendirmek, eğitim amacı ile araştırma ve planlama yapmak için simülasyon kullanılabilmektedir (Mıdık ve Kartal, 2010: 389). Patrick (2002) tarafından simülasyon tekniğinin temel kullanım amaçları üç şekilde ifade edilmiştir: İlki yeni bir problemin (olayın durumun, vs.) test edilmesi ve planının yapılması; ikincisi gerçek hayatta yapılması tehlikeli ve maliyetli olan durumların eğitiminin verilmesi, üçüncüsü ise öğrenenlerin gerçek hayatta değerlendirilmesinin ölçülebilmesi için kullanılmasıdır.

Simsoft şirketine ait "TÜBİTAK 1002-Öğretmen Yetiştirmede Sanal Sınıf Simülasyonlarının Kullanımı Projesi" bünyesinde hazırlanan "Dijital Sınıflarda

Öğretmen ve Öğretmen Adaylarının Eğitimi İçin Sınıf Simülasyonu'' projesi kapsamında hazırlanan simülasyon, kavramın daha iyi anlaşılabilmesi ve örnek olması için öğretmen ve öğretmen adaylarına önemli katkılar sağlamaktadır. Aşağıda bu simülasyona ait bazı görseller verilmiştir. (https://www.sinifta.com/).

Görsel 1.1. Simülasyonun Yapay Zekâ Etkileşimli Öğrencileri ve Sınıf Tasarımları

Görsel 1.2. Simülasyonun Yapay Zeka Etkileşimli Öğrenci Özelliklerini Seçebilme Tasarımları

Görsel 1.1. ve Görsel 1.2'de ekran görüntüsü verilen SINIFTA simülasyonu ile öğretmen veya öğretmen adayları yapay zekâ tarafından kontrol edilen sanal öğrencilerle etkileşim kurabilme ve genel sınıf ortamında gerçek sınıf deneyimi sunmaktadır. Simülasyonu kullanan kullanıcının performansları belirlenerek sınıf yönetimi becerisi, öğrenci profilini analiz etme, ders içeriğini teknoloji ile destekleme becerileri kriterlerine göre sınıf profili çıkarma ve uygun ders anlatma yöntemini belirleme, değerlendirilmiştir. Söz konusu uygulamanın simülasyonu; öğretim konusunun belirlenmesi, uygulamanın giriş arayüzü, öğrenci özelliklerinin incelenmesi, ders etkinliklerinin oluşturulması ve ders anlatım yönteminin belirlenmesi, oturma düzenin belirlenmesi, olumsuz durumlar için çözüm yolları üretme, dersi uygun şekilde sonlandırma ve değerlendirme aşamalarını içermektedir.

Kullanıcı, simülasyon zamanı bağımsız değişkenleri değiştirerek kendi yürüttüğü bir deneyim canlandırır. Örneğin bu simülasyon: kullanıcının değişkenleri değiştirerek fen kavramını, matematik- fen arasındaki ilişkiyi deneyimleyerek anlamasına imkân tanır (Atıcı, 2023: 27).

1.1.4.7. Otonom Robotlar

1970'lerde dijital kontrol elektroniği ve yapay zekânın ortaya çıkması otomatik algılama ve bilgi işleme teknolojilerine olan ilgiyi artırmıştır. Bu dönemde sensörler, aktüatörler ve işlemcilerin maliyetlerinin düşmesi, otonom sistemlerin ve robotların gelişmesini hızlandırmış ve bu teknolojilerin çeşitli uygulama alanlarında kullanılmasını mümkün kılmıştır (Watson ve Scheidt, 2005: 369).

Robot, önceden belirlenmiş ya da otonom olarak görevleri yerine getirebilen elektro-mekanik bir cihazdır. Otonom robotlar, çevresindeki bilgileri sensörler aracılığıyla algılayıp ve bu veriler doğrultusunda hareket ederek görevlerini bağımsız bir şekilde tamamlayabilmektedir. Bu robotların tasarımında en büyük ilham kaynağı genellikle doğadaki canlılardır. Örneğin, insanlar ve birçok hayvanın iki gözü vardır ve beyin, bu gözlerden gelen sinyalleri işleyerek derinlik algısı olgusu oluşturur. Bu doğal özellikten esinlenen mühendisler, robotlarda stereo görme teknolojisini kullanmaya başlamışlardır. Benzer şekilde, yarasaların gözleri yoktur; bunun yerine ses dalgalarını gönderip geri alarak etraflarını algılarlar. Bu özellikten ilham alan bilim insanları, yüksek frekansta ses dalgaları yayarak mesafe ölçen sensörler geliştirmişlerdir. Bugün ise, bu sensörlerden gelen verileri işleyip kararları alabilen otonom robotlar tasarlanmaktadır (Durmuş, 2015: 1).

İnsan-robot iş birliği, robotların yetenek artırıcı araçlar olarak kullanılmasını sağlamaktadır. Özellikle sanayi ve üretim sektörlerinde kullanılan robotlar iş süreçlerindeki belirsizlikleri azaltarak çalışma koşullarında iyileşme ve verimlilik artışı sağlamaktadır. Teknolojinin hızlı gelişimiyle, robotik sistemler son yıllarda daha yaygın hale gelmiş ve insanlarla daha yakın bir etkileşim biçimi geliştirmiştir. Robotlar, evlerden hastanelere kadar pek çok alanda kullanılmaya başlanmış böylece insan-robot işbirliği de giderek artmıştır. Başlangıçta insanlar ile ayrı bir şekilde çalışan robotlar, sadece basit görevleri yerine getirirken; zamanla gelişen teknolojilerle

bu ayrım ortadan kalkmış ve robotlar insanlarla doğrudan etkileşim içinde çalışmaya başlamıştır (Başalan, 2021: 36).

Robotlar, insan şeklini taklit edebilecek şekilde tasarlanabileceği gibi, farklı şekillerde de inşa edilebilir. Çoğu robot estetikten çok işlevselliğe odaklanarak, belirli görevleri yerine getiren makineler olarak geliştirilmiştir. Robotlar, otonom ya da yarı otonom olabilmektedir. Otonom robotlar, çevrelerini sensörler aracılığıyla algılayabilmekte ve bu verilerle kendi kararlarını alarak hareket edebilmektedir. Örneğin, bir temizlik robotu bulunduğu evin düzenini ve koordinatlarını kendi başına öğrenip, buna göre hareket ediyorsa, otonom bir robot olarak kabul edilmektedir. 16.02.2017 kabul tarihli Robotikler Hakkında Medenî Hukuk Kuralları Tavsiye Raporu'nda otonom olma, "karar verebilme ve bu kararları dış dünyada, dışarıdan bir yönlendirme veya etkileşim olmaksızın uygulayabilme kabiliyeti" olarak tanımlanmaktadır. İnsan müdahalesinin olduğu durumlarda yarı-otonom robotlardan bahsedilmektedir (Akbulut, 2023: 290).

Günümüz üretim ekosistemlerinde, maliyet avantajı elde etme, ürün çeşitliliği ve kalitesini artırma, kitlesel üretimden ziyade daha özelleştirilmiş müşteri odaklı üretime geçiş yapma gibi hedefler, organizasyonların daha yenilikçi, esnek ve otonom üretim yöntemlerine yönelmesini sağlamaktadır. Piyasa dalgalanmaları ve rekabet baskıları, yeterli işgücüne sahip olmalarına rağmen, şirketleri üretim süreçlerinde daha etkili ve yenilikçi çözümler aramaya itmektedir. Bu bağlamda, özellikle yüksek hassasiyet, esneklik ve güvenilirlik gerektiren karmaşık ürünlerin üretiminde, insan operatörlerin fiziksel ve beceri sınırlarını aşmak için otonom robotlar ve sistemler kullanmak ön plana çıkmaktadır. Ayrıca, otonom robotlar, işçi güvenliğini artırmak, üretim süreçlerini daha esnek hale getirmek, kaliteyi yükseltmek ve çevresel etkileri azaltmak gibi pek çok alanda da önemli çözümler sunmaktadır. Bu teknolojiler, üretim süreçlerini daha verimli hale getirirken aynı zamanda sürdürülebilirliği de desteklemektedir (Esmaeilian vd., 2016: 82).

Otonom bir mobil robotun sahip olması gereken temel özellikler şunlardır (Tozan, 2007: 1):

- Bulunduğu ortamı, tasarlandığı işlevi yerine getirecek şekilde algılayabilme,

- Hem beklenen hem de beklenmeyen durumlar karşısında kendi başına karar alabilme yeteneği,
- Topladığı verileri insanlarla paylaşabilme ve gerektiğinde dışarıdan kontrol edilebilme imkânı.

Bir gezgin robotun otonom olabilmesi için, en kritik bileşenlerinden biri karar verme mekanizmasıdır. Bu bağlamda, robotun çevresindeki nesneleri doğru bir şekilde algılamasında sensörlerin büyük rolü bulunmaktadır. Sensörler, robotun çevresini gerçek zamanlı olarak öğrenebilmesini sağlamalı, ayrıca ekonomik olmalı ve donanım açısından verimli olmalıdır.

"Otonom robotlar genellikle uzaktan kumandayla çalıştırılmayan, ancak kendi eylemlerini planlayan ve uygulayan, serbest dolaşan mobil robotlar anlamına gelir." Bu durumda, otonomi uzaktan kumanda ile kontrol edilmeyen ve mobil olan bir özellik anlamına gelmektedir. Temel fikir, kabloya bağlı olmayan bir mobil robotta, belirli bir seviyede bağımsız çalışma yeteneğine sahip, yani bir dereceye kadar öz düzenleme veya kontrol kapasitesine sahip bir robota kadar uzanıyor gibi görünmektedir (Smithers, 2007: 2).

1.1.4.8. Sanal Gerçeklik (VR) ve Artırılmış Gerçeklik (AR)

Sanal Gerçeklik

Sanal (virtual) terimi, var olmayan ancak algılarımızın etkisiyle varmış gibi bir izlenim uyandıran bir kavramdır ve kökeni "virtualis" kelimesine dayanmaktadır. Sanal Gerçeklik (Virtual Reality) ise, kullanıcının veya izleyicinin, yaratılmış bir görüntü alanına, zaman içinde değişebilen bir yapı içerisinde dahil olmasını ve sonrasında bu alanla etkileşime girmesini sağlayan bir teknolojidir. Bu ortam, çeşitli veri girdi ve çıktı sistemleri kullanarak, güç, hareket, dokunma gibi duyusal etkileri taklit etmekte ve üç boyutlu görseller, ses aygıtları gibi teknolojilerle zenginleştirilmiş bir deneyim sunmaktadır (Kuruüzümcü, 2010: 94). Sanal gerçeklik teknolojisi (Virtual Reality, VR) kavramı için literatürde farklı tanımlamalar mevcuttur. Stone'un (1991) ve Oppenheim'ın (1993) tanımlamaları sanal gerçeklik tarihinin ilk tanımlarını özetlemektedir. Stone (1991) sanal gerçekliği, *"Makine ile insanlar arasında iletişimin gelişmesi için oluşturulan, insan duyularına hitap eden bir çoklu ortamlar"* olarak

tanımlarken; Oppenheim'a (1993) göre sanal gerçeklik, *"Makine ile insan etkileşimini, görsel ve işitsel iletişimle yetinmeyip, hissetme yoluyla artırmaya çalışan teknoloji"* olarak tanımlanmaktadır (Öztürk, 2024: 34). Başka bir tanıma göre ise sanal gerçeklik, *"kullanıcıların bilgisayar tarafından yapay bir ortama girmelerini sağlayan"* bir teknoloji olarak ifade edilmektedir (Lee, 2012: 13). Sanal Gerçeklik teknolojisi, kullanıcılara gerçekçi bir deneyim sunan ve onlara dinamik bir ortamla etkileşime girme imkânı tanıyan, bilgisayarlar tarafından oluşturulmuş üç boyutlu bir simülasyondur. Bu teknoloji ile tasarlanan sistemler insanların kavrayış ve algılama yetilerini önemli ölçüde geliştirmektedir (Bayraktar ve Kaleli, 2007: 1) Sanal gerçeklik teknolojileri; daldırma (immersion), etkileşim (interaction) ve hayal etme (imagination) gibi özellikleri ile dikkat çeker ve bu teknolojiler, kullanıcılara oluşturulan ortamda gerçek bir varlık hissi (presence) yaşatmaktadır (Bütün vd., 2019: 257).

Sanal gerçeklik sistemleri, kullanıcı deneyimini en iyi şekilde sunabilmek için çeşitli donanım bileşenlerinden oluşur. Bu bileşenler şunları kapsamaktadır (Uluçay ve Küçük, 2023: 119):

Başa takılabilir ekranlar (HMD): Kullanıcının gözlerine, üç boyutlu ve gerçek zamanlı görsel geri bildirim sağlayan cihazlardır. Oculus Rift, HTC Vive ve PlayStation VR, popüler HMD örnekleridir.

Oculus Rift HTC Vive PlayStation VR

Şekil 1.16. Başa takılabilir ekranlar (HMD) örnekler

Takip sistemleri: Kullanıcının hareketlerini anlık olarak izlemek için kullanılmaktadır. Hareketler, kullanıcının baş, eller ve hatta bütün vücut hareketlerini kapsayabilmektedir. Takip sistemleri, kızılötesi kameralar, manyetik alanlar veya ultrasonik sensörler kullanarak çalışmaktadır. Bu sistemler, kullanıcıların sanal

ortamda etkileşimde bulunmasını mümkün kılmaktadır. Örnek olarak hareket sensörleri, dokunmatik eldivenler ve oyun kumandaları verilebilir.

Giriş cihazları: Kullanıcıların sanal ortamda etkileşimde bulunmalarını sağlamaktadır. Buna örnek olarak hareket kontrol cihazları, dokunmatik eldivenler ve oyun kontrolcüleri bulunur.

Sanal gerçeklik teknolojisinin tarihsel gelişimine bakıldığında, çok eski zamanlara dayandığı anlaşılmaktadır. Sanal gerçeklik teknolojisindeki 1838 yılından başlayarak 2016 yılına kadar olan gelişmeler şöyledir (Sherman ve Craig, 2018: 30-57):

• 1838 yılında, Sir Charles Wheatstone, stereopsisi (iki ya da daha fazla görüntüden elde edilen derinlik bilgisine ve 3 boyutlu modele ulaşma yöntemi) araştırarak, stereoskopu icat etmiştir.

• 1862 yılında, John Pepper, aydınlatma kullanımıyla oluşturulan yanılsamanın gelişmiş bir versiyonunu ortaya çıkararak, iki mekânın (dünyaların) aynı anda görüntülenmesini sağlayan yansıtıcı şeffaf bir yüzeyalternatif bir gerçeklik oluşturmuştur (bu uygulama ismi ile anılmış: Pepper'ın Hayaleti.).

• 1901 yılında, Frederic E. Ives tarafından bilinen ilk otostereoskopik görüntü (gözlük veya benzeri cihazlara gerek kalmadan iki boyutlu bir yüzey üzerinde üç boyutlu görüntü oluşturabilme teknolojisi) sergilenmiştir.

• 1915 yılında, Edwin S. Porter ve W.E. Wadell tarafından ilk anaglifik (üç boyutlu görüntü sistemlerinde en eski ama aynı zamanda en kalitesiz görüntü sunan teknik) üç boyutlu film deneyleri yapılmıştır.

• 1916 yılında, Albert B. Pratt, kafaya yerleşik bir periskop ekranı (deniz ve kara savaşlarında harekâtı kolaylaştırmak maksadıyla kullanılan emniyetli mesafelerden hedefi görünmeden incelemeye yarayan optik bir alet) için patent almıştır.

• 1929 yılında, Edwin Link, sabit (iç mekân) bir konumda bir pilot yetiştirmek amacıyla mekanik bir uçuş simülatörü geliştirmiştir. Bu uçuş simülatörü, pilotların sanki uçuyormuş gibi hissettikleri yapay bir ortamda eğitim almasıdır. Uçuş simülasyonu "sanal gerçeklik" teknolojisinin erken bir yansıması olmuştur.

• 1946 yılında, Pennsylvania Üniversitesi'nde geliştirilen ilk elektronik dijital bilgisayar olan ENIAC ABD Ordusuna teslim edilmiştir.

• 1956 yılında, Morton Heilig, Sensorama'yı Cinerama'dan (çok geniş bir ekran olarak hareketli görüntü formatı) ilham alarak geliştirmiştir. Sensorama multimodal (çok modlu) bir deneyim görüntüleme sistemi olmaktadır. Kullanıcı, önceden kaydedilmiş deneyimi (örneğin Manhattan'dan bir motosiklet yolculuğu gibi) manzara, ses, koku, titreşim ve rüzgâr yoluyla algılamasını sağlamaktadır.

• 1960 yılında, Morton Heilig, HMD'lere (Başa Takılan Ekran-Head Mounted Display) çarpıcı bir şekilde benzeyen ve hatta görsel, duyusal ve koku alma duyularının kullanabilmesini sağlayan "Stereoscopic-Television Apparatus for Individual Use" isimli bir sistem için patent aldı.

• 1961 yılında, Philco mühendisleri Comeau ve Bryan, uzaktaki video kamera izleme sistemini takip eden, baş hareketlerini algılayan bir HMD oluşturdu. Telebulunuşluk konusundaki araştırmalarına dayanarak Telefactor Corp. Şirketini kurmuşlardır. HMD tabanlı bir telebulunuşluk sisteminin erken yansıması olmaktadır.

• 1963 yılında, MIT doktora öğrencisi Ivan Sutherland, Sketchpad uygulamasıyla dünyayı etkileşimli bilgisayar grafikleriyle tanıştırmıştır. Sutherland'ın çalışması, klavye girişine ek olarak, seçim ve çizim etkileşimi gerçekleştirmek için hafif bir kalem kullanmıştır.

• 1964 yılında, General Motors Corporation, otomotiv tasarımı için etkileşimli bir paket olan DAC (bilgisayar tarafından artırılmış tasarım) sistemi üzerine araştırmalar yapmaya başlamıştır.

• 1965 yılında, Ivan Sutherland, Uluslararası Bilgi İşlem Kongresi'nde sunumunda "ultimate display" kavramını açıklamıştır. Sutherland, kullanıcının fiziksel gerçeklik yasalarına uymasına gerek kalmadan, sanal dünyadaki nesnelerle etkileşime girebileceği bir ekran konsepti oluşturmuştur. Sutherland'ın ekran konsepti görsel uyarıcıları ve kinestetik (dokunsal) uyarıcıları içermektedir.

• 1966 yılında, Larry Roberts, MIT'in Lincoln Laboratuvarı'nda geliştirilen ultrasonik izleme yöntemlerini kullanarak üç boyutlu olarak izlenen bir kalem boyutlu bilgisayar giriş birimi "The Lincoln Wand" adlı çalışmasını yayımlamıştır.

• 1967 yılında, Fred Brooks, Chapel Hill'deki Kuzey Karolina Üniversitesi'nde Sutherland'ın "ultimate display" konseptinden ilham alarak, biyokimyacıların protein molekülleri arasındaki etkileşimleri "hissetmelerine" yardımcı olmak ve kinestetik (dokunsal) etkileşimin kullanımını keşfetmek amacıyla GROPE projesine başlamıştır. Kuzey Karolina Üniversitesi, sanal gerçeklik teknolojilerinin ve fikirlerinin geliştirilmesinde güçlü bir rol oynamaya devam etmiştir.

• 1968 yılında, Utah Üniversitesi bilgisayar bilimleri profesörleri David Evans ve Ivan Sutherland tarafından Evans ve Sutherland Computer Corp., kurulmuştur. Ivan Sutherland, "A Head-mounted Three-Dimensional Display" adlı makalesinde Harvard Üniversitesi'nde bir stereoskopik HMD geliştirmesini anlatmıştır. Ivan Sutherland, 1968 yılında bir başa takılan ekran (HMD) oluşturmuştur. HMD, stereoskopik görsel görüntüler, mekanik ve ultrasonik izleme ve sanal gerçeklik potansiyelinin bir gösterimini sağlamaktadır.

• 1972 yılında, Atari tarafından geliştirilen Pong oyunu, tüketici pazarına gerçek zamanlı olarak çoklu etkileşim sağlayan bilgisayar grafiklerini sunmuştur.

• 1976 yılında, Myron Krueger, Videoplace prototipi tamamlamıştır. Videoplace, kullanıcının hareketleriyle kontrol edilen sanal bir dünya oluşturma amacıyla kameraları ve diğer giriş aygıtlarını kullanmaktadır.

• 1977 yılında, Commodore, Radio Shack ve Apple, evde kullanıma yönelik kişisel bilgisayarları piyasaya sunmuştur.

• 1979 yılında, Eric Howlett, küçük bir ekrandan geniş bir görüş alanı elde etmek için optikleri kullanarak LEEP (Large Expanse Enhanced Perspective) sistemini geliştirmiştir. AT&T Bell Labs'ta Gary Grimes "dijital veri giriş eldiveni arayüz cihazı" geliştirmiş. Bu eldiven aynı zamanda kullanıcının elinin genel yöneliminin yanı sıra parmaklardaki ve diğer el duruşlarındaki bükülme miktarını hissetmek için de ışık kullanmıştır.

• 1982 yılında, Kapaklı tarzdaki ilk dizüstü bilgisayar olan GRiD Compass piyasaya sunuldu, ardından ertesi yıl Gavilan SC'yi "dizüstü bilgisayar" olarak pazarlanan ilk taşınabilir bilgisayar oldu.

• 1984 yılında, Jaron Lanier tarafından VPL Research, Inc., görsel bir programlama dili oluşturmak için kurulmuştur. Şirket yakında bu çalışmayı, NASA VIEW laboratuvarından alınan hibeler kapsamında DataGlove ve EyePhones'u (sırasıyla 1985 ve 1989'da) oluşturmak için bırakmıştır. DataGlove, kullanıcının elinin duruşunu bilgisayara bildiren aletli bir eldivendir. EyePhones, LEEP optiklerle birlikte bir çift LCD ekran kullanan bir HMD olmaktadır.

• 1986 yılında, Thomas Furness VR ile ilgili insan faktörleri araştırmasını "The Super Cockpit and its Human Factors Challenges" yayınladı.

• 1989 yılında, VPL, sanal gerçeklik kavramını tanıtan eksiksiz bir VR sistemi (RB-2 (Reality Built 2)) duyurmuştu. Bununla birlikte kullanıcı VPL Eyephones ve Datagloves kullanmasıyla birlikte sanal bir dünya ile karşılaşarak etkileşime girmektedir. Division, Ltd., VR donanımı ve yazılımı pazarlamaya başlamıştır.

• 1990 yılında, Stanford doktora mezunu Jim Kramer, CyberGlove'u ticarileştirmek için Virtual Technologies, Inc.'i kurmuştur. CyberGlove, el bileğine göre parmakların göreceli konumunu ölçmek için gerginlik ölçerler kullanan bir eldiven cihazıdır. Sanal Teknolojiler daha sonra Immersion Corporation tarafından satın alındı ve daha sonra 2009'da CyberGlove Systems olarak bilinen ayrı bir kuruluşa geri verilmiştir. NASA VIEW projesinin öncü mühendisi Jim Humphries, 1990'da Fakespace Inc. Tarafından ticarileştirilecek olan BOOM'u tasarlayıp prototiplenmiştir. BOOM, VIEW projesi için Humphries tarafından tasarlanan ve prototiplenen birçok HBD'den (Head Based Display-Kafaya Yerleşik Ekran) biriydi.

• 1992 yılında SIGGRAPH '92 bilgisayar grafikleri konferansında, Chicago'daki Illinois Üniversitesi Elektronik Görselleştirme Laboratuvarı'ndaki Tom DeFanti, Dan Sandin ve ekibi tarafından CAVE sistemi geliştirilmiştir.

• 1995 yılında, Profesör Hiroo Iwata ve öğrencileri tarafından SIGGRAPH '95 konferansında "Virtual Perambulator" araştırma prototipi gösterildi. Cihaz, kullanıcı ayakları ile zemin arasında fiziksel olarak bir ortamda dolaşırken, aynı zamanda sanal olarak da yürüyebilmelerini sağlayan düşük sürtünmeli bir arayüz sağlamıştır.

• 1996 yılında, Avusturya, Linz'deki Ars Electronica Elektronik Sanat müzesindeki CAVE sistemi, insanların sanal dünyaları deneyimlemelerinisağlamak için sanal gerçeklik ortamında çalışan sanatçılara halka açık bir alan sunmuştur.

• 1997 yılında, Virtual Technologies, Inc., CyberGrasp el tabanlı kuvvet geri bildirim cihazını sunmuştur. Bu cihaz, VR sisteminin kullanıcının parmaklarını kapatma yeteneğini kısıtlamasına ve sanal bir dünyada dokunma ve kavrama duygusunu artırmasına olanak tanımıştır.

• 1998 yılında, Disney hem HMD hem de projeksiyon tabanlı görsel ekranları kullanarak çok sayıda VR cazibe merkezine sahip olan DisneyQuest aile macera merkezlerinin ilkini açmıştır.

• 1999 yılında, Illinois Üniversitesi'nden SCAPE projesi, retroreflektif (yansıtıcı) ekran yüzeyleri kullanarak çoklu kullanıcıların her birinin sanal dünyayı kendi görüş açılarından görmesini sağlayan projeksiyon tabanlı bir AR / VR ortamını göstermektedir.

• 2003 yılında, Linden Labs tarafından Second Life, paylaşımlı sanal dünya sistemi piyasaya sunulmuştur. Second Life, öncelikle bir oyundan ziyade sosyal bir buluşma alanı, yani kullanıcıların etkileşimde bulunabileceği bir "sanal alan" olmaktadır.

• 2007 yılında, AlloSphere, Santa Barbara'daki Kaliforniya Üniversitesi'nde açılmıştır. AlloSphere, bir podyumda kürenin ortasında "bekletilmiş" izleyicilerin bölümünde iki yarım küreden oluşan ilginç bir projeksiyon aracılığıyla yansıtılan bir VR ortamı olmaktadır.

• 2008 yılında, Apple, IMU tarafından geliştirilen akıllı telefonların üç boyutlu sahneleri görüntülemek için optikleri olan bir koruma ile birleştirilmesiyle oluşturulmuş bir VR sisteminin, "Ekranlı taşınabilir bir elektronik cihazı tutmak için başa takılan ekran aparatı" patentini almıştır.

• 2010 yılında, University College London (Londra Üniversitesi Akademisi), VR sistemlerini kullanırken daha doğal yürümeye izin vermek için sürtünmeli bir yürüme yüzeyi olan Wizdish'in kullanımını araştırmıştır.

• 2012 yılında, MxR Laboratuvarı'nda öğrenci stajyeri olan Palmer Luckey, Oculus Rift isimli düşük maliyetli HMD için başarılı bir Kickstarter kampanyası yürütmüştür. Bu Kickstarter kampanyasıyla finanse edilen ilk Oculus Rift Development Kit (DK-1) sanal gerçekliğe büyük ilgiyi ortaya koymuştur.

• 2013 yılında, Virtuix Omni, düşük maliyetli ve düşük sürtünmeli yürüme yüzeyine sahip olarak prototipten üretim aşamasına geçmeyi finanse etmek için başarılı bir Kickstarter kampanyası yürütmüştür. Virtuix Omni, özel ayakkabıların merkeze geri dönmesini, halka içinde kalırken yürüme algısını arttırmasını sağlayan eğimli kenarlara sahip bir halka platformu olmaktadır. Virtuix Omni, düşük sürtünmeli bir yüzey ve düşük sürtünmeli ayakkabılar kullanarak, kullanıcının sanal alanda sonsuz yürüyüş yapmasını sağlamaktadır. Bundan ayrı olarak, Leap Motion, çok düşük maliyetli, düşük menzilli bir parmak takip sistemi olmaktadır. Sadece 80 ABD doları karşılığında kullanılabilen Leap Motion kontrol cihazı, bir kullanıcının elinin parmaklarını eldiven veya işaret takmaya gerek kalmadan takip etmenin bir yolunu sunmaktadır. Bir HMD giyen kullanıcıların, sanal dünya ile karşılaştıkları sırada ellerini görmeleri sağlamaktadır.

• 2014 yılında, Kickstarter kampanyasıyla düşük maliyetli HMD'ler oluşturmak için kurulan Oculus VR, Facebook tarafından 2 milyar ABD doları karşılığında satın alınmıştır. Google, "Google Cardboard" olarak adlandırılan karton ve plastik optiklerden oluşturulan bir sanal gerçeklik başlığı üretmiştir. Samsung, Oculus VR ile birlikte, ticari bir HMD olan "Samsung Gear VR" yi duyurmuştur. Bununla birlikte, bu durumda, kasanın içine yerleştirilmiş ilave izleme teknolojisi, düğmeler ve giriş için küçük bir dokunmatik yüzey bulunmaktadır.

• 2015 yılında, New York Times, abonelerine, özellikle The New York Times gazetecileri tarafından oluşturulan 360 hikâye içeriğini görüntüleyebilecekleri bir Google Cardboard sağladığı bir anlaşmayı duyurmak için Google ile bir araya gelmiştir.

• 2016 yılında, Oculus VR, ilk tüketici odaklı VR teşhir ürününü (CV-1) ön sipariş sistemi aracılığıyla piyasaya sunulmuştur. İlk sistem, HMD, video tabanlı konum izleme için bir kamera ve kullanıcı girişi için takip edilmeyen bir Xbox oyun denetleyicisi içermektedir. HTC ve Valve, ilk tüketici odaklı VR ürününü (Vive) ön

sipariş sistemi aracılığıyla piyasaya sürmüştür. Daqri, "Akıllı Kask" larını endüstriyel kullanım için ticari olarak kullanılabilir hale getirmiştir. Sony, PlayStation kamera ve Move kontrol cihazlarıyla birleştirmek ve PlayStation 4 oyun konsolu ile birlikte kullanılmak üzere "PlayStation VR" başlıklı cihazını piyasaya sürmüştür.

Artırılmış Gerçeklik

Artırılmış Gerçeklik (AR) kavramı, ilk kez 1950'li yıllarda görüntü yönetmeni Morton Heilig'in sinemanın, izleyici tüm duyularını etkileyerek ekrandaki olaylara daha derinlemesine katılmasını sağlama potansiyelini keşfetmesiyle ortaya çıkmıştır (Carmigniani, 2011: 342).

Artırılmış Gerçeklik (AR) teknolojisi, sanal verileri gerçek dünya ile entegre eden bir teknolojidir. Bu teknolojinin kullandığı araçlar arasında multimedya, 3D modelleme, gerçek zamanlı takip ve kayıt, akıllı etkileşim, algılama teknolojileri gibi pek çok bileşen yer almaktadır. Temel işleyişi, metin, resim, 3D modeller, müzik, video gibi bilgisayar tarafından üretilen sanal içeriklerin, gerçek dünya üzerinde görsel olarak sunulmasını sağlamaktadır. Bu sayede, sanal bilgiler gerçek dünyadaki unsurlar ile birleşmekte ve gerçek dünyanın etkileşimli bir şekilde zenginleştirilmesi mümkün olmaktadır (Chen, 2019: 1). Milgram ve Kishino (1994) artırılmış gerçekliği *"Gerçek dünya nesneleri yerine dijital ortam ürünlerinin kullanıldığı gerçeklik ortamıdır"* olarak tanımlamaktadır. Azuma'ya (1997) göre ise, artırılmış gerçeklik "bir çeşit sanal çevredir ya da sanal gerçekliğin daha yoğun kullanılmış şeklini" ifade etmektedir. Artırılmış Gerçeklik, sanal verileri yalnızca kullanıcının yakın çevresine değil, aynı zamanda canlı video akışı gibi gerçek dünya ortamlarının farklı görünümlerine entegre ederek kullanıcı deneyimini zenginleştirmeyi hedeflemektedir. Artırılmış gerçeklik, kullanıcının gerçek dünya ile olan etkileşimini ve algısını geliştirmeye yardımcı olmaktadır (Carmigniani, 2011: 342).

Artırılmış Gerçeklik (AR) bilgisayar tarafından üretilen sanal bilgileri gerçek dünyaya entegre ederek bu dünyayı zenginleştirmeyi amaçlayan bir araştırma alanıdır. Azuma (1997: 2), AR sistemlerinin üç ana özelliğini şu şekilde tanımlar (Schmalstieg, 2011: 13):

1. Sanal görsellerin gerçek dünyaya dahil edilmesi,

2. Dijital verilerin üç boyutlu olarak kaydedilmesi,
3. Gerçek zamanlı etkileşimin sağlanması.

Mobil bilgisayar teknolojilerindeki gelişmeler, bilgiye erişimi kolaylaştırırken, birçok sektörde yaratıcı düşünceye sahip profesyoneller, bu yenilikleri uygulamak için yenilikçi yöntemler arayışına girmektedir. Eğlence, sağlık, havacılık ve otomotiv gibi endüstriler, bu teknolojilerin sunduğu fırsatlardan faydalanmaktadır. Aynı şekilde, mimarlık, mühendislik ve inşaat sektörleri, proje süreçlerini iyileştirmek ve görselleştirmek için giderek daha fazla bilgisayar destekli teknolojilere yönelmektedir. Karmaşık yapı bilgilerini görsel hale getirmek, projelerin daha anlaşılır olmasını sağlamakla kalmaz, aynı zamanda paylaşılan bir vizyon ve tutarlı bir anlayış oluşturulmasına da katkı sağlamaktadır. Artırılmış Gerçeklik (AR) bu alandaki önemli teknolojilerden biridir ve araştırma aşamalarında, projelerin görselleştirilmesi için büyük avantajlar sunmaktadır. Ancak Artırılmış Gerçeklik (AR), sadece bu sektörlerle sınırlı kalmaz; sağlık, eğitim, savunma, seyahat, emlak, otomotiv, müzecilik, reklam, pazarlama, dijital oyunlar ve eğlence gibi farklı alanlarda da teknolojinin ilerlemesiyle birlikte giderek daha yaygın bir şekilde kullanılmaktadır (Bingöl, 2018: 48). Artırılmış gerçekliğin kullanım alanlarına dair bazı görseller aşağıda yer almaktadır.

Görsel 1.3. MagicBook & Col-AR Mix uygulamaları örneği
Kaynak: (Durna, 2021: 37).

Col-AR Mix adlı uygulama, MAG teknolojisi kullanılarak geliştirilmiş bir boyama uygulamasıdır. Bu uygulama eğitim ve eğlence amaçlı tasarlanmıştır.

Kullanıcılar, etkileşimli 3D modellerle öğrenebilmekte veya oyunlarla eğlenebilmektedir (Durna, 2021: 35). Magicbook ise, artırılmış gerçeklik (AR) teknolojisini kullanarak eğitim materyallerini dijitalleştiren bir araçtır (Durna, 2021: 37).

Yuen ve diğerleri (2011: 127) çalışmalarına göre, Artırılmış Gerçeklik (AG) uygulamalarının eğitim üzerindeki katkıları şunlardır:

1. Öğrencileri çeşitli ders materyallerini keşfetmeye teşvik eder,
2. Öğrencilerin motivasyonunu artırır,
3. Gerçek hayatta deneyimleyemeyecekleri dersleri veya konuları sanal ortamda deneyimlemelerini sağlar,
4. Öğrenci ve öğretmen arasındaki etkileşimi güçlendirir,
5. Öğrencilerin yaratıcılıklarını ve problem çözme yeteneklerini geliştirmelerine katkı sağlar,
6. Her öğrencinin farklı öğrenme tarzları ve hızları vardır; bu uygulamalar sayesinde öğrenciler, kişisel öğrenme yöntemlerini daha etkin şekilde yönetebilir,
7. Otantik, etkileyici ve motive edici bir öğrenme ortamı sunar.

Görsel 1.4. Artırılmış gerçeklik ortamı İkea AG uygulaması örneği

IKEA, artırılmış gerçeklik uygulaması IKEA Place ile kullanıcıların evlerinde iç mekân düzenlemelerini sanal ortamda denemelerine olanak tanımaktadır. Apple ARKit teknolojisiyle geliştirilen IKEA Place, kullanıcıların "ilham alın ve parmağınızla farklı ürünleri, stilleri ve renkleri keşfedin" yaklaşımını

benimsemektedir. Uygulamada, kullanıcılar önce istedikleri ürünü seçmekte, ardından bu ürünün yerleştirileceği alanı belirler ve sanal olarak ürünü bu alana yerleştirebilmektedirler. Sonrasında, seçilen ürünün gerçeğiyle birebir örtüşen 3D görseli belirlenen alanda gösterilmektedir. Uygulama, ürünleri dijital ortamda ölçeklendirerek %98 doğruluk oranıyla çalışmaktadır. Bu sayede, bir ürün satın alırken ölçü alma ihtiyacı ortadan kalkar, kullanıcılar herhangi bir ölçüm aracı kullanmadan doğru yerleşim sağlayabilmektedirler (https://shiftdelete.net/ikea-ar-uygulamasi-85130).

Görsel 1.5. Artırılmış Gerçeklik oyun örnekleri
Kaynak: (İçten ve Bal, 2017: 126).

Artırılmış gerçeklik oyunları, oyunun görsel ve işitsel unsurlarını kullanıcının gerçek dünyasıyla gerçek zamanlı olarak entegre etmektedir. Bu alandaki devrim niteliğinde bir örnek olarak kabul edilen Pokémon GO, akıllı telefonun kamera, cayroskop, saat ve GPS gibi sensörlerini kullanarak konum tabanlı artırılmış gerçeklik deneyimi sunmaktadır. Oyunda, gerçek çevrenin bir haritası ekranda gösterilir ve çimlerin hışırtısı bir Pokémon'un varlığını işaret etmekte; kullanıcı, dokunmatik ekrana dokunarak Pokémon'u yakalayabilmektedir. Artırılmış gerçeklik modu sayesinde, Pokémon'lar gerçek dünya görüntüsünde sanal olarak görünmekte ve oyuncu, bu sanal karakterlerle etkileşime girebilmektedir (Bingöl, 2018: 51).

Görsel 1.6. Turist uygulaması
Kaynak: (İçten ve Bal, 2017: 125).

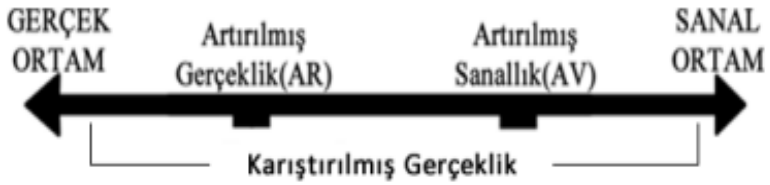
Yukarıdaki görsel de soldaki yerleşim merkezi, sağdaki arkeoloji alanında kullanılmış konum ve tanılama tabanlı izleme yönteminin uygulama görüntüsü yer almaktadır. Bu uygulamalar sayesinde önemli binaların ve tarihi mekanların tanıtımı, gerçek zamanlı yol tarifi işlemleri kolaylaşmakta ve daha etkili hale gelmektedir (İçten ve Bal, 2017: 125).

Görsel 1.7. Artırılmış Gerçekliğin Mimaride Kullanımı
Kaynak: (Doğan, 2016: 125).

Artırılmış gerçeklik sistemleri, tasarımcılara, işçilere, müşterilere ve potansiyel işverenlere projeleri gerçeğe dönüştürmeden önce sanal bir ortamda gezme ve tasarlanan veya inşa halindeki tesisleri/ binaları görüp deneyimleme imkânı sunmaktadır. Bu sayede, projelerin tüm aşamaları sana olarak gözlemlenebilir ve daha iyi bir anlayış geliştirilmesine olanak tanımaktadır (Behzadan, 2008).

1.1.4.8.1. Sanal Gerçeklik ve Artırılmış Gerçeklik Arasındaki Fark

Sanal gerçeklik ve artırılmış gerçeklik zaman zaman karıştırılabilmektedir. Sanal gerçeklik terimi, *"bir kişinin içine daldığı bilgisayar tarafından oluşturulmuş, etkileşimli, üç boyutlu ortam"* olarak tanımlanmaktadır. Artırılmış gerçeklik, uygun bilgisayar arayüzleri aracılığıyla bir bilgisayar tarafından işlenen dijital bilgilerin gerçek dünyadan gelen bilgilerle gerçek zamanlı olarak harmanlanmasına olanak tanır. Şekil 1.17'de sanal gerçeklik ile artırılmış gerçeklik kavramları arasında Paul Milgram ve Fumio Kishino'nun (1994: 3) Gerçeklik – Sanallık Sürekliliği'nin yardımıyla açıklanabilecek net bir fark vardır;



Şekil 1.17: Milgram'ın gerçeklik-sanallık sürekliliği (Milgram's reality-virtuality continuum)

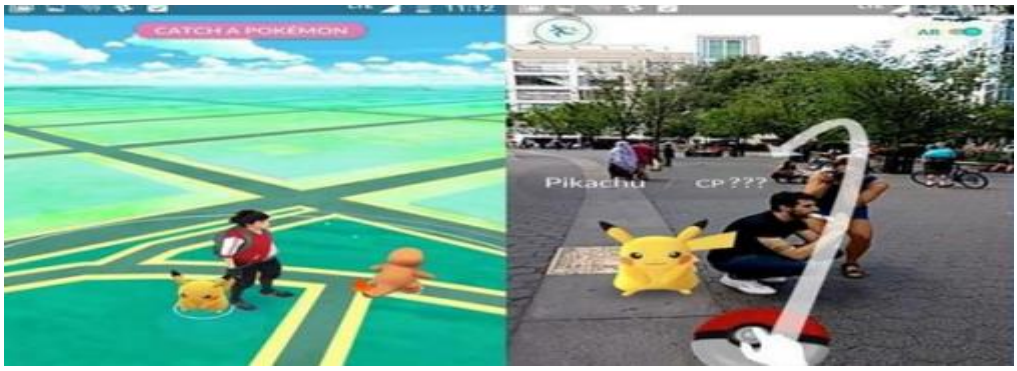
Gerçek dünya ile tamamen sanal bir ortam, bu iki uç nokta arasında bir süreklilik oluşturur ve bu aralıktaki bölge "Karma Gerçeklik" olarak adlandırılır. Artırılmış Gerçeklik (AR), bu spektrumda gerçek dünyanın dijital verilerle zenginleştirilmiş halini temsil eder ve genellikle gerçek dünyanın baskın olduğu uç noktaya daha yakındır. "Artırılmış Sanallık" ise, çoğunlukla sanal öğelerle oluşturulmuş ve bunlara gerçek dünya görsellerinin eklenmiş olduğu sistemleri tanımlamak içim Milgram tarafından kullanılan bir terimdir. Milgram ve diğerlerine (1995: 1) göre, sanal gerçeklik, kullanıcıyı tamamen sanal bir ortama daldırarak, çevresindeki gerçek dünyayı görmesini engeller. Bu genellikle bir gözlük takarak, kullanıcıyı tamamen farklı bir dünyada hissettirebilmekte ve etrafındaki gerçek dünyadan kopmasında neden olabilmektedir. Buna karşılık, artırılmış gerçeklikte, kullanıcılar bir bilgisayar, akıllı telefon, özel gözlük veya baş üstü ekran gibi bir cihaz aracılığıyla sanal öğelerin gerçek dünya ile birleştirildiğini görebilmektedir. Bu sayede, her iki dünyanın farkında olarak hem sanal hem de gerçek çevreyi deneyimleyebilmektedir (Amin ve Govilkar, 2015: 12). Uzun Hazneci'ye (2019: 500) göre sanal gerçeklikte, kullanıcılar mevcut fiziksel dünyadan tamamen koparak tamamen sanal bir ortamda var olmaktadırlar. Buna karşın, artırılmış gerçeklikte

kullanıcılar, gerçek fiziksel çevrelerine sanal öğelerin eklenmiş halini görmektedirler. Yani, sanal içerikler gerçek dünyanın üzerine yerleştirilmekte, ancak kullanıcılar çevrelerindeki gerçek dünyayı da aynı anda deneyimlemeye devam etmektedirler. Görsel 1.8 ve 1.9'de kavramlara ilişkin farklar sunulmuştur (Göçen, 2022: 101).

Görsel 1.8. Artırılmış Gerçeklik

Görsel 1.9. Sanal Gerçeklik

Artırılmış gerçeklik teknolojisi, kullanıcıyı tamamen gerçek dünyadan koparmak yerine, gerçek dünya ortamını temel almakta ve bu ortamı sanal öğelerle zenginleştirmektedir. Diğer tanımlamalarda da belirtildiği gibi, artırılmış gerçekliğin amacı gerçek dünyayı sanal nesnelerle entegre ederek daha etkileşimli ve bilgi dolu bir deneyim sunmaktır. Artırılmış Gerçeklik sistemlerinde kullanıcı, gerçek ve sanal nesneleri insan gözüyle ayırt edebilecek şekilde bir deneyim yaşamaktadır. Bu da sanal gerçeklik ile artırılmış gerçeklik arasındaki en temel farklardan birini ortaya koymaktadır (Durna, 2021: 27). Pokemon-Go oyununa ait örnek Görsel 1.10'da gösterilmiştir.



Görsel 1.10. Pokemon-Go oyununa ait örnek görsel

1.1.4.9. Siber- Fiziksel Sistemler

Siber-Fiziksel Sistemler (CPS) kavramı, hesaplama, ağ oluşturma ve fiziksel süreçlerin birleşimini ifade etmek amacıyla 2006 yılında ABD'de tanıtılmıştır (Törngren ve Sellgren, 2018: 478).

Siber-Fiziksel Sistemler (SFS), fiziksel dünya ve onun dinamik süreçleriyle sürekli bir etkileşim içinde olan, aynı zamanda veri erişimi ve işleme hizmetlerinin internet üzerinden sağlandığı, birbirleriyle etkileşim halinde çalışan hesaplama sistemleridir (Monostori, 2016). Geisberger ve Broy'a (1995: 9) göre, *"fiziksel dünya ile siber alanı internet ile birbirine bağlayan sistemlere siber-fiziksel sistemler (CPS-Cyber-Physical Systems)"* adı verilmektedir. Ayrıca, bu teknolojide sensörlerle desteklenmiş fiziksel faktörler, internet hizmetleri aracılığıyla kurulan iletişim sayesinde toplu hale getirilmekte, böylece belli amaçlar doğrultusunda nesnelerin etkileşimi sağlanmaktadır (Alçın, 2016: 23).

Bradley ve Atkins'in (2015) siber-fiziksel sistemlerin (CPS) gelişimini mümkün kılan önemli olay ve olguları içeren tarihsel dökümü Tablo 1.4'de derleyerek sunmuşlardır.

Tablo 1.4. Siber- Fiziksel Sistemlerin Gelişimi Olay/Olguları

Tarih	Olay/Olgu
1932	Nyquist, kontrol sistemleri konusunda frekans teknikleri geliştirmiştir.
1940- 1945	Örneklenmiş Veri Sistemleri Teorisi ortaya atılmıştır.
1945	İlk amplifikatör tasarımı yapılmıştır.
1946	İlk taşınabilir hücresel telefon geliştirilmiştir.
1946	İlk bilgisayar (ENIAC) bulunmuştur.
1950	Root Locus metodu geliştirilmiştir.
1954	Dijital Kontrol Sistemleri geliştirilmiştir.
1969	ARPANET (internetin ilk hali) geliştirilmiştir.
1973	Gerçek zamanlı işleme sistemleri geliştirilmiştir.
1973	Optimal, adaptif, non-lineer kontrol sistemleri ile stokastik sistemleri geliştirilmiştir.
1990	Hibrit sistemler geliştirilmiştir.
1997	IEEE 802.11 Wifi standardı geliştirilmiştir.
2000	Ağ önceliği sistemi (QoS) başlatılmıştır.
2006	Siber- Fiziksel Sistem (CPS) kavramı ilk kez kullanılmıştır.

Kaynak: Bradley, J. M. ve Atkins, E. M. (2015). Optimization and Control of Cyber-Physical Vehicle Systems, Sensors, Sayı:15, ss. 23023'den dönüştürülmüştür.

Siber fiziksel sistemlerin temel bileşenleri arasında algılayıcılar, ağ altyapıları, veri tabanları, sunucular, yazılımlar ve kullanıcı ara yüzleri yer almaktadır. Bu sistemler, daha verimli operasyonlar, hızlı karar alma süreçleri ve gerçek zamanlı veri görüntüleme imkânı sunarak, çeşitli alanlarda önemli faydalar sağlamaktadır (Çalhan ve Cicioğlu, 2022: 1). Siber fiziksel sistemler büyük verilerin bilgiye dönüşmesinde sistematik biçimde çalışmakta, bu da optimum karar verme sürecine katkı sağlamaktadır (Lee vd., 2015: 3).

Siber Fiziksel Sistemler iki önemli unsurdan oluşmaktadır (Serinikli, 2018: 1612):

1. İnternet üzerinden belirli adreslerle birbirleriyle iletişim kuran nesneler ve sistemlerden oluşan ağdır.
2. Gerçek dünyadaki nesnelerin ve davranışların bilgisayar ortamında simüle edilerek oluşturulmuş sanal bir ortamdır.

Siber-fiziksel sistemler hızla gelişen bir alan olup, havacılık, otomotiv mühendisliği, sivil altyapı, enerji, sağlık hizmetleri, üretim, ulaşım, eğlence ve tüketici cihazları gibi birçok mühendislik disiplininde geniş bir uygulama yelpazesi sunmaktadır. Ayrıca, akıllı evler, akıllı şehirler ve akıllı ofisler gibi alanlarda da yaygın bir şekilde kullanılmaktadır (Stojmenovic ve Zhang, 2015: 1). Bu nedenle, siber fiziksel sistemler yalnızca üretim süreçlerinde değil, aynı zamanda ar-ge, tasarım ve pazarlama gibi süreçlerde de önemli bir rol oynamaktadır (Yüksekbilgili ve Çevik, 2018: 426).

1.1.4.10. Üç Boyutlu (3D) Yazıcılar

3D yazıcılar, bilgisayar destekli tasarım programlarıyla tasarlanmış herhangi bir datayı, bir kalıp veya model aracına ihtiyaç duymadan doğrudan makineye aktararak malzeme katmanlarını üst üste ekleyerek fiziksel modeller üreten cihazlardır (Özsoylu, 2017: 54). Başka bir deyişle, 3D yazıcılar, bilgisayar ortamında oluşturulmuş dijital tasarım dosyalarını fiziksel nesnelere dönüştüren cihazlardır. Bu süreç, 3D baskı olarak adlandırılmaktadır. 3D yapabilmek için öncelikle bir modelin tasarlanması gerekmektedir. Modelleme, 3D tasarım yazılımları ile sıfırdan yapılabileceği gibi, 3D tarama teknolojileriyle de gerçekleştirilebilmektedir.

Bilgisayar ortamında yapılan bu tasarım işlemi CAD (Bilgisayar Destekli Tasarım) olarak adlandırılmaktadır. Piyasada, farklı sektörler de yaygın olarak kullanılan birçok CAD yazılımı bulunmaktadır (Tonga ve Tonga, 2022: 55).

3D yazıcıların çalışma prensipleri temelde benzer olsa da kullanım alanı ve amacına bağlı olarak kullanılan materyaller ve yöntemler arasında farklılıklar bulunmaktadır. 3 Boyutlu yazıcıların farklı materyal ve yöntem uygulamaları (Erener ve Boz, 2021: 50);

- Steryolitografi (SLA),
- Katı Zemin Kürleme (SGC),
- Lamine Nesne İmalatı (LOM),
- Eriyik Yığarak Modelleme (FDM),
- Çok Jetli (Polyjet-Multijet) Modelleme (MJF),
- Seçmeli Lazer Sinterleme ve Ergitme (SLS/SLE),
- Elektron Işınlı Ergitme (EBM) olarak sınıflandırılmaktadır.

3D baskı teknolojisi, tasarımcıların hayal güçlerini sınırsız bir şekilde kullanmalarına olanak tanımakta ve pek çok karmaşık tasarımın bile kolayca hayata geçirilmesini sağlamaktadır. Bu yöntem, kalıp yapımı gibi geleneksel üretim sınırlamalarını ortadan kaldırarak tasarım sürecini daha özgür ve esnek hale getirmektedir. Tasarım doğru bir şekilde programlandıktan sonra, üretim süreci hızlı ve verimli bir şekilde tamamlanabilmektedir. Böylece, daha fazla tasarım yaratılabilmekte ve yenilikçi çözümler hızla hayata geçirilebilmektedir (Kaplan ve Coşgun, 2023).

3D baskı, sağlık, otomotiv, havacılık ve savunma endüstrilerinde ve diğer çoğu alanda sayısız uygulama bulan nispeten yeni, hızla genişleyen bir üretim yöntemini ifade etmektedir (Dodziuk, 2016: 282). Bunlara örnek olarak şunlar gösterilebilir (Boyutkat, 2021):

- NASA tarafından 3D yazıcı ile üretilen PUFFER adlı robot
- Uluslararası Uzay İstasyonu'ndaki astronot ve kozmonotlar için inek hücrelerinin üç boyutlu yazıcıyla çoğaltılması yoluyla üretilen biftek
- Otomotiv sektöründe üretilen yedek parçalar

- Havacılık sektöründe 3 boyutlu uçak iç mekân parçaları
- Sağlık sektöründe tıbbi cihaz, protez, implant, damar, doku ve hatta organ üretimi
- Mimarlık ve inşaat alanında 3D yazıcı ile üretilen ev
- Elektronik sektöründe 3D yazıcı ile üretilen anten, pil, devre kartı ve radar sistemler
- Moda sektöründe 3D yazıcı ile üretilen giysi ve ayakkabılar
- Enerji sektöründe 3D yazıcı ile üretilen enerji santrali parçaları
- 3D yazıcı ile üretilen tüketim malzemeleri ve tersine mühendislik uygulamaları.

1.1.4.11. Siber Güvenlik

Dünya genelinde ve Türkiye'de internet ve bilgisayar kullanıcılarının sayısı giderek artmaktadır. Türkiye İstatistik Kurumu'nun 27 Ağustos 2024' de yayınladığı rapora göre 2024 yılında Türkiye'de İnternet kullanım oranı 16-74 yaş grubundaki bireylerde 2023 yılında %87,1 iken 2024 yılında %88,8 olmuştur (TÜİK, 2024). Teknolojinin ilerlemesiyle birlikte, birçok iş ve faaliyet sanal ortama taşınmıştır. Bu sanal ortam, paylaşılan verilerin sürekli olarak kaydedilmesiyle hızla genişlemekte ve bu ağlar, çeşitli siber tehditlere maruz kalmaktadır. Bu durum, ağ güvenliğinin önemini giderek daha fazla artırmakta ve güvenlik önlemlerinin güçlendirilmesini zorunlu kılmaktadır (Önaçan ve Atan, 2016: 16).

Siber güvenlik, teknolojinin hızla ilerlemesi ve internetin yaygınlaşması ile dijitalleşmenin artması sonucunda ortaya çıkan bir kavramdır. 1991'de internetin sivil kullanıma açılması, sanal ortamda önemli değişikliklere yol açmış ve dijital üretimi hızlandırmıştır. Bu süreç, siber alanların güvenliğini sadece kurumlar için değil, aynı zamanda bireyler için de kritik bir konu haline getirmiştir. Bugün sıkça gündeme gelen bir kavram olan siber güvenlik, temel olarak dijital ortamda karşılaşılabilecek tehditlerin engellenmesi ve güvenliğin sağlanması anlamına gelmektedir (Bıçakçı, 2019: 2). Uluslararası Telekomünikasyon Birliği siber güvenliği*, siber ortamda, organizasyon ve kullanıcıların varlıklarını korumak için kullanılabilecek araçlar, politikalar, güvenlik kavramları, güvenlik önlemleri, kılavuzlar, risk yönetimi*

yaklaşımları, eylemler, eğitim, uygulamalar, altyapı ve teknolojilerin bütünü olarak tanımlamaktadır (ITU-T, 2014: 2). Tanım incelendiğinde, korunması gereken gruplar ve bu grupların varlıkları açıkça belirlenmiş olup, alınması gereken önlemler de net bir şekilde vurgulanmıştır.

Siber güvenlik, bireyler ve ailelerin yanı sıra kuruluşlar, hükümetler, eğitim kurumları ve işletmeler için önemli bir konu haline gelmiştir. Ailelerin, çocukları ve diğer aile üyelerini çevrimiçi dolandırıcılıklardan koruması büyük bir önem taşımaktadır. Finansal güvenlik açısından ise kişisel mali durumu etkileyebilecek finansal bilgilerin güvence altına alınması kritik rol oynamaktadır. İnternet, öğretim görevlileri, öğrenciler, personel ve eğitim kurumları için hem çok değerli hem de birçok çevrimiçi riskle birlikte birçok öğrenme fırsatı sunmaktadır. İnternet kullanıcılarının çevrimiçi dolandırıcılıklardan ve kimlik hırsızlığından korunma yöntemlerini anlamaları oldukça hayati bir konu olmuştur. Çevrimiçi davranış ve sistem korumasına dair doğru eğitim, güvenlik açıklarını azaltarak daha güvenli bir çevrimiçi ortam yaratılmasına yardımcı olabilmektedir. KOBİ'ler, sınırlı kaynaklar ve yeterli siber güvenlik becerilerinin olmaması nedeniyle çeşitli güvenlik zorluklarıyla karşı karşıya kalmaktadır. Teknolojilerin hızla yayılması, bu alanda kalıcı çözümler geliştirilmemesi nedeniyle siber güvenliği daha karmaşık hale getirmektedir. Ağları ve bilgileri korumak için çeşitli çerçeveler ve teknolojiler kullanmakta ve bu konuda sürekli olarak çözümler üretmeye çalışılmakta; ancak bu çözümler genellikle kısa vadeli koruma sağlamaktadır. Daha iyi güvenlik anlayışı ve doğru stratejiler, fikri mülkiyetin ve ticari sırların korunmasına yardımcı olurken, mali kayıplar ve itibar zedelenmesini de en aza indirmeye olanak sağlamaktadır (Goutam, 2015: 14).

Boyut ve şekil değiştiren siber tehditler, artık siber savaşa dönüşerek kritik altyapı ve sistemleri hedef almaktadır. Bu durum, ülkelerin sınırlarını koruduklari gibi dijital verilerini ve altyapılarını da güvence altına almalarını zorunlu kılmaktadır. Bu mücadelede bir yandan teknolojik gelişme, diğer yandan ise bireylerin eğitim ve farkındalık seviyelerinin artırılması önemlidir (CBDDO, 2024).

1.2. KOBİ'ler ve Dijital Dönüşüm

KOBİ'ler ülkemizde özellikle 1990'lı yıllardan itibaren ülke ekonomisinin büyük çoğunluğunu oluşturmakta ve gün geçtikçe ekonomi içindeki payını arttırmaktadır. "Ülkemizdeki toplam girişim sayısının %99,9'unu, istihdamın %76'sını, maaş ve ücretlerin %53'ünü, cironun %63'ünü, faktör maliyetiyle katma değerin (FMKD) %53,3'ünü ve maddi mallara ilişkin brüt yatırımın %53,7'sini KOBİ'ler oluşturmaktadır." (Kılıç vd., 2016: 52).

KOBİ tanımı, ülkeden ülkeye, hatta aynı ülke içinde bölgesel ve sektörel farklar gösterebilir. Ayrıca, farklı kurumlar aynı kavramı değişik şekillerde tanımlayabilir. Küresel ölçekte, KOBİ'ler ekonomilerin temel yapı taşlarından biri olarak kabul edilmektedir. Dünya genelinde küçük işletmeler, toplam işletmelerin büyük bir kısmını, yani %95'inden fazlasını oluşturmakta ve KOBİ'lerin istihdam yaratma oranı ise %80 seviyelerine kadar çıkmaktadır. Bu özellikleriyle, KOBİ'ler ülkelerin ekonomilerinde kritik bir rol üstlenir. Sonuç olarak, KOBİ'ler ekonomik kalkınma, istihdam artışı ve genel ekonomi açısından son derece önemli bir yer tutmaktadır (Taghiyev, 2019: 3).

KOBİ'ler işletme sahibinin aynı zamanda yönetici olarak görev yaptığı, genellikler yerel ölçekte faaliyet gösteren ve dış kaynaklardan bağımsız olarak sadece kendi öz sermayesiyle finansman sağlayan kuruluşlardır (Keskin ve Canbaz, 2014: 163).

KOBİ'lerde işletme sahibi, genellikle yönetim sürecinde doğrudan yer almaktadır ve işin her yönüne daha fazla sahip çıkmaktadır. Personel ile daha yakın daha az hiyerarşik ilişkiler kurulmakta, bu da bürokrasinin azalmasına yol açmaktadır. Küçük ölçekli olmaları nedeniyle, müşterilerle daha sıkı ilişkiler geliştirilmektedir. Düşük sermaye ile faaliyet göstererek istihdam yaratmaktadırlar. Tüketici taleplerindeki değişikliklere hızlı bir şekilde adapte olmaktadırlar. Denetim ve kontrol süreçleri daha basit olmaktadır. Sipariş bazlı çalışma modeli sayesinde stok maliyeti düşmektedir. Teknolojik değişimlere büyük yatırımlar yapmadıkları için bu değişimlere daha kolay uyum sağlamaktadırlar (Şahin ve Çankaya, 2017: 123).

Bu bölümde, öncelikle KOBİ'lerde dijital dönüşümün önemi, KOBİ'lerde dijital dönüşümün avantaj ve dezavantajları ve KOBİ'lerde dijital dönüşümün gelişimi ele alınmaktadır.

1.2.1. KOBİ'lerde Dijital Dönüşümün Önemi

KOBİ'ler, hem gelişmiş hem de gelişmekte olan ülkelerde ekonomik büyümeye katkı sağlamakta ve yeni istihdam olanakları yaratmaktadır. Bu yönleriyle KOBİ'ler, bir ülkenin iş sektörünün önemli bir parçasını oluşturarak sosyal ve ekonomik kalkınma da önemli rol oynamaktadır (Adewole ve Umoru, 2021: 196).

KOBİ'ler dünya genelinde ekonomilerin temel taşlarından biridir. Küçük işletmeler, birçok ülkede toplam işletmelerin %95'inden fazlasını oluşturmakta ve istihdam oranı %80 seviyelerine ulaşmaktadır. Bu durum, KOBİ'lerin ülke ekonomileri üzerindeki etkisini artırırken, aynı zamanda gelişmişlik, istihdam ve ekonomik büyüme açısında kritik bir rol oynamaktadır (Koyuncuoğlu, 2021: 113). Tanımı farklılık gösterse de KOBİ'lerin tanımlanmasında kullanılan ölçütler genel olarak "nitelik (kalitatif) ölçütler" ve "nicelik (kantitatif) ölçütler" olmak üzere iki gruba ayrılmaktadır (Mecek, 2020: 30). Nitel ve nicel açıdan yapılan tanımlamalarda kullanılan kriterler genel olarak şu şekildedir (Karayılmazlar, 2007: 156):

a) Nicelik yönünden

- *İşçi sayısı,*
- *Sermaye,*
- *Aktif toplamı,*
- *Toplam çevirici güç miktarı,*
- *Enerji kullanımı,*
- *Ciro (satış hasılatı),*
- *Makine parkı,*
- *Kapasite (üretim hacmi).*

b) Nitelik yönünden

- *Girişimcinin işletmede fiilen çalışması,*
- *İş bölümü ve uzmanlaşma derecesi,*

- *Sermayenin sınırlı oluşu, finansal yetersizlik,*
- *Yönetim tekniklerinin uygulanmaması veya yetersizliği.*

KOBİ tanımlamalarında kolay ölçülebilmesi ve objektif sonuçlar vermesinden dolayı genellikle niceliksel ölçütlerden yararlanılmaktadır.

Ülkelerin hem ekonomik hem de sosyal yapıları gereği her ülkeye özgü bir KOBİ tanımlamasından bahsetmek mümkün olmamaktadır. Bu nedenle tüm dünyanın kabul ettiği tek bir tanımlamadan söz edilememektedir. Ülkemizde, 25.05.2023 tarihli ve 7297 sayılı Resmî Gazete'de yayımlanan "Küçük ve Orta Büyüklükteki İşletmelerin Tanımı, Nitelikleri ve Sınıflandırması Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik" kararı ile önceden bir işletmenin KOBİ statüsünde sayılabilmesi için gereken 250 milyon TL limit, 500 milyon TL'ye çıkarılmıştır. KOBİ tanımı, "250 kişiden daha az çalışanı bünyesinde barındırdığı, yıllık net satış hasılatı veya mali bilançosundan birinin 500 milyon TL'yi aşmadığı işletmeler yönetmelikte "KOBİ" (küçük/orta ölçekli işletme)" olarak değiştirilmiştir.

KOBİ'ler dünya genelinde geniş bir istihdam sağlayarak ve gelir oluşturarak birçok ekonominin temel yapı taşını oluşturmaktadır (Shafi, Liu ve Ren, 2020). Benzer şekilde, örneğin Türkiye'de Sanayi ve hizmet sektörlerinde faaliyet gösteren 3 milyon 773 bin girişim KOBİ sınıfına girmektedir. KOBİ'ler 2022 yılında toplam girişim sayısının %99,7'sini oluşturmaktadır. KOBİ'ler istihdamın %70,6 'sını, personel maliyetinin %47,5'ini, üretim değerinin %36,3'ünü ve faktör maliyetiyle katma değerin %36,4'ünü oluşturmaktadır. Tüm bu veriler Türkiye genelinde KOBİ'lerin ekonomideki önemini göstermektedir (TÜİK,2022).

KOBİ'ler, hemen hemen tüm ülke ekonomisinde önemli bir rol oynamaktadır. KOBİ'ler, büyük işletmelerle benzer özelliklere sahip olmakla birlikte, bağımsızlıkları, işletme sahibinin hem girişimci hem de yönetici rolünü üstlenmesi, müşteriler ve çalışanlarla kurdukları yakın ilişkiler gibi belirgin özellikleriyle büyük işletmelerden ayrılmaktadır. Bu özellikler sayesinde KOBİ'ler daha esnek bir şekilde hareket edebilmekte, değişen koşullara hızlıca uyum sağlamakta, pazar boşluklarını değerlendirerek fırsatları zamanında yakalayabilmekte, müşteri ve personel ile daha güçlü ilişkiler kurabilmekte ve teknolojik yeniliklere hızlı adapte olabilmektedir (Erdil vd., 2003: 21). Günümüzün yoğun rekabet ortamında, KOBİ'lerin varlıklarını

sürdürebilmeleri, çevresel koşullara ve teknolojik gelişmelere uyum sağlamalarına bağlıdır. Bu bağlamda, ülke ekonomileri açısından büyük öneme sahip olan KOBİ'lerin günümüz rekabet koşullarında hem rakipleriyle hem de büyük işletmelerle rekabet edebilmeleri özellikle de uluslararası pazarlarda rekabet güçlerini artırabilmeleri için interneti etkin bir araç olarak kullanmaları artık bir zorunluluk haline gelmiştir (Marangoz ve İnak, 2019: 2). Bu nedenle, KOBİ'lerin verimliliklerini artırabilecek ve hayatta kalma şanslarını yükseltecek stratejilerin belirlenmesi büyük önem taşımaktadır. Teknolojiyi iş süreçlerine entegre eden Dördüncü Sanayi Devrimi, iş dünyasına yenilikçi teknolojiler sunmaktadır. Bu ileri teknolojiler, işletmelerin operasyonel süreçlerini köklü bir şekilde dönüştürmektedir (Chang vd., 2020: 1).

KOBİ'lerde dijital dönüşüm, iş yapma biçiminde ve temel yapılarında köklü değişikliklere yol açabilecek yeni süreçler ve mekanizmalar sunarak, birçok organizasyonda önemli dönüşümlere neden olmaktadır (Kraus vd., 2022: 1). Dijital dönüşüm, "mobil teknoloji, yapay zekâ, bulut bilişim, blok zinciri ve nesnelerin interneti (IoT) gibi yeni dijital teknolojilerin, iş süreçlerinde önemli iyileştirmeler sağlamak amacıyla kullanılması" olarak tanımlanabilir ve bu dijital teknolojilere geçiş, işletmelere yeni fırsatlar sunmaktadır (Omrani vd., 2024: 5030).

KOBİ'ler için dijitalleşme büyük bir potansiyel taşımaktadır. Bilgi odaklı süreçlerin dijital ortamda yönetilmesi, maliyetleri %90'a kadar azaltabilir ve geri dönüş sürelerini önemli ölçüde iyileştirebilir. Ayrıca, kâğıt tabanlı ve manuel işlemlerin yazılım sistemleriyle entegrasyonu, işletmelerin süreç performansını, maliyetleri ve riskleri daha etkin bir şekilde analiz etmelerini sağlayan veri toplama sürecini otomatikleştirir. Gerçek zamanlı raporlar ve gösterge panelleri, yöneticilere sorunlar büyümeden müdahale etme fırsatı tanır. Sabbagh ve diğerlerinin (2013) araştırmalarına göre, dijitalleşme ekonomik büyümeyi kademeli olarak artırır; dijitalleşmenin ileri düzeyde olduğu ülkeler, daha az dijitalleşmiş ülkelere kıyasla %20 daha fazla ekonomik fayda sağlamaktadır. Ayrıca dijitalleşmenin, işsizlik oranlarını düşürme, yaşam kalitesini iyileştirme ve vatandaşların kamu hizmetlerine daha kolay erişmesini sağlama gibi olumlu etkileri de gözlenmiştir (Parviainen vd., 2017: 64).

1.2.2. KOBİ'lerde Dijital Dönüşümün Gelişimi

Tüm dünyada geçerli tek bir KOBİ tanımından bahsetmek mümkün değildir. Bu farklılığın temel sebeplerinden biri, ülkelerin kalkınma seviyelerinin farklı olmasıdır. Ayrıca, sektörlerin kendine has özellikleri de tanımlama farklarının bir başka nedenidir. Farklı kültürlere ve sosyal yapılara sahip ülkelerin küçüklük ve büyüklük anlayışlarının farklı olması, çeşitli tanımların ortaya çıkmasında yol açabilmektedir. Aşağıdaki tabloda bazı ülkeler ve Avrupa Birliği'nin KOBİ tanımlarını belirlerken kullandıkları ölçütler yer almaktadır (Tekin ve Güngör, 2024: 11).

Tablo 1.5. Ülkelere göre KOBİ Sınıflandırması

Ülkeler	KOBİ Ölçeği	Çalışan Sayısı	Net Satış Hasılatı	Mali Bilançosu
Türkiye	Mikro Öçekli	< 10	≤ 10 Milyon TL	≤ 10 Milyon TL
	Küçük Ölçekli	< 50	≤ 100 Milyon TL	≤ 100 Milyon TL
	Orta Öçekli	< 250	≤ 500 Milyon TL	≤ 500 Milyon TL
İtalya	Mikro Öçekli	1-19	-------	-------
	Küçük Ölçekli	20-99	-------	-------
	Orta Öçekli	100-249	-------	-------
Almanya	Küçük Ölçekli	< 9	< 1 milyon €	-------
	Orta Öçekli	< 499	< 50 milyon €	-------
İngiltere	Mikro Öçekli	0-9	≤ 1milyon £	≤ 1milyon £
	Küçük Ölçekli	0-49	≤ 2.8 milyon £	≤ 1.4 milyon £
	Orta Öçekli	50-249	≤ 11.2 milyon £	≤ 5.6 milyon £
Azerbaycan	Mikro Öçekli	< 10	≤ 200 bin AZN	-------
	Küçük Ölçekli	< 50	≤ 3 milyon AZN	-------
	Orta Öçekli	< 250	≤ 30 milyon AZN	-------
Belarus	Mikro Öçekli	< 15	-------	-------
	Küçük Ölçekli	< 100	-------	-------
	Orta Öçekli	< 250	-------	-------
Gürcistan	Mikro Öçekli	-------	-------	-------
	Küçük Ölçekli	≤ 50	≤ 12 milyon GEL	-------
	Orta Öçekli	≤ 250	≤ 60 milyon GEL	-------
Avrupa Birliği	Mikro Öçekli	< 10	≤ 2 milyon €	≤ 2 milyon €
	Küçük Ölçekli	< 50	≤ 10 milyon €	≤ 10 milyon €
	Orta Öçekli	< 250	≤ 50 milyon €	≤ 43 milyon €
	Küçük Ölçekli	1-499	-------	İmalat

Amerika Birleşik Devletleri	Orta Öçekli	500-1500	-------	
	Küçük Ölçekli	1-99	-------	Toptan Ticaret
	Orta Öçekli	100-500	-------	
	Küçük Ölçekli	-------	< 2.5 milyon $	Perakende Ticaret
	Orta Öçekli	-------	2.5-21.5 milyon $	
	Küçük Ölçekli	-------	< 0.5 milyon $	Tarım
	Orta Öçekli	-------	0.5-9 milyon $	
	Küçük Ölçekli	-------	< 5 milyon $	Hizmet
	Orta Öçekli	-------	5-21 milyon $	
Japonya	Küçük Ölçekli	< 20	-------	İmalat
	Küçük Ölçekli	< 5	-------	Servis Hizmetleri
	Orta Öçekli	< 300	< 300 milyon ¥	İmalat,İnşaat,Ulaşım
	Orta Öçekli	< 100	< 100 milyon ¥	Toptan Satış
	Orta Öçekli	< 50	< 50 milyon ¥	Perakendecilik
	Orta Öçekli	< 50	< 100 milyon¥	Servis Hizmetleri

Kaynak : (Tekin ve Güngör, 2024: 13-14).

Günümüzün sanayi devrimlerinin son aşaması olan Endüstri 4.0, üretim, tüketim ve tedarik süreçlerinde köklü değişikliklere yol açan bir döneme işaret etmektedir. Önceki sanayi devrimlerinden farklı olarak bu süreç, herhangi bir ekonomik, politik ya da sosyal patlamanın sonucu değil, Endüstri 3.0'ın getirdiği yeniliklerin ve iyileştirmelerin doğal bir devamı olarak ortaya çıkmıştır (Bal ve Erkan, 2019: 626). Endüstri 4.0 terimi, 2011 yılında Hannover Ticaret Fuarı'nda sunulmuştur (Slusarczyk, 2018: 233). Endüstri 4.0, büyük ölçüde insan müdahalesine gerek duymadan kendi başına çalışan makineler ve üretim sistemlerine dayalıdır. Teknolojik ilerlemeler sayesinde üretim süreçleri, akıllı ve otonom hale gelmiş, makineler kendi kendini yönetebilecek kapasiteye ulaşmıştır. Endüstri 4.0'ın temel unsurları arasında büyük veri analitiği, otonom robotlar, artırılmış gerçeklik, 3D yazıcılarla eklemeli üretim, bulut bilişim, siber güvenlik, nesnelerin interneti, sistem entegrasyonu ve simülasyon teknolojileri bulunmaktadır (Bal ve Erkan, 2019: 626).

Son yıllarda birçok KOBİ, özellikle gelişmekte olan pazarlarda, dijital teknolojileri dijital olmayan geleneksel ürün ve süreçlerine entegre etmek için dijital teknolojileri benimsemektedir. Girişimlerde bilişim teknolojileri kullanım araştırması (2024), sonuçlarına göre İnternete erişim oranı; 10- 49 çalışanı olan girişimlerde %86,1, 50-249 çalışanı olan girişimlerde %87,9, 250 ve üzeri çalışanı olan girişimlerde

ise %92,6 olduğu bildirilmiştir (TÜİK, 2024). Son 50-60 yıl, teknoloji açısından son derece dinamik bir dönem olmuştur ve her 10 yılda bu gelişmelerin hızı giderek artmıştır. Dünya nüfusu hızla büyümüş, ekonomi genişlemiş, internet kullanıcı sayısı önemli ölçüde artmış, teknolojiye erişim daha ucuz ve yaygın hale gelmiştir. Dijital dönüşümün tarihsel gelişimi Tablo 1.6' de ayrıntılı bir şekilde sunulmaktadır (Türkyılmaz, 2024: 280).

Tablo 1.6. Dijital Dönüşümün Tarihsel Gelişimi

17. yy. (1679) - ***Leibniz ikili sayı sistemi"0-1"***
18- 19 yy. – ***Mekanik hesap makineleri Bilgi depolama yaklaşımları***
1947 – ***Bell laboratuvarı ilk transistörün icadı***
1950 – ***İnternetin resmi başlama tarihi***
1954 – ***Kentucky Louisville' de ilk defa maaş bordrosu ve üretim kontrol programlarını içeren iş bilgisayarı olan UNIVAC I adlı bilgisayarın kullanıma açılması***
1958 – ***Jack Kilby ve ekibin baş teknisyeni Tom Yeargan tarafından icat edilen ve teknoloji alanında çığır açan dünyanın ilk mikroçipi***
1971 – ***İlk mikrobilgisayar***
1972 – ***İlk dijital saat PULSAR***
1975 – ***İlk dijital Kamera (Steven Sasson)***
1976 – ***Apple I İlk kişisel bilgisayar***
1977 – ***İlk ATM (Citibank)***
1981 – ***IBM PC Microsoft İşletim Sistemi***
1982 – ***İlk CD (Ticari amaçlı kompakdisk)***
1989 – ***WWW (World Wide Web***
1990- 2000'li yıllar- ***İnternetin gelişimi – (VEDOP, MERNİS) Banka otomasyonları***
2000 – ***WEB 2.0 Nesnelerin İnterneti***
2004 – ***Facebook – Youtube - Wikipedia***
2010 – ***İnstagram – Blockchain ve kripto para – Hücresel taşıma sistemi***
2020 – ***Otonom Etkileşim ve Sanallaştırma***

Dijital dönüşüm, büyük şirketlerin yanı sıra KOBİ'ler için de önemli bir konu haline gelmiştir. Ancak, KOBİ'lerin dijitalleşme yolculuğu, her dönemde farklı bir hızla ve farklı araçlarla ilerlemiştir. 1980'ler dijitalleşmenin ilk adımları olarak nitelendirilen bir dönemdir. Bu dönemde bilgisayar teknolojileri hızla gelişmiş ve işletmeler bilgisayarları daha yaygın kullanmaya başlamıştır. 1990'lar, internetin hızla yayılmaya başladığı ve dijitalleşmenin KOBİ'ler için önemli bir fırsat haline geldiği dönemi işaret etmektedir. Bu süreç, KOBİ'lerin işlerini dijital ortama taşımalarına olanak tanıyan yeni araçların gelişmesini sağlamıştır. 2000'ler, internetin giderek daha

yaygın hale gelmesi ve dijital teknolojilerin işletmelerin günlük operasyonlarına entegre edilmesinin hızlandığı bir dönemdir. Bu dönemde, dijitalleşme özellikle internet üzerinden sunulan iş çözümleri ve yazılım uygulamaları üzerine yoğunlaşmıştır. 2010'lar dijital teknolojilerin hızla geliştiği ve büyük veri, yapay zekâ, mobil uygulamalar ve sosyal medya gibi kavramların KOBİ'lerin iş yapış şekillerinde belirgin bir yer kazandığı bir dönemi temsil eder. Bu dönemdeki teknolojik ilerlemeler, KOBİ'lere iş süreçlerini daha verimli hale getirme ve rekabet avantajı sağlama fırsatı sunmaktadır. 2020'ler dijital dönüşümün KOBİ'ler için sadece bir seçenek değil, bir gereklilik haline geldiği bir dönem olmuştur. Özellikle Covid-19 pandemisi ile birlikte hız kazanmış ve yaşanan bu salgın, dijitalleşmeyi hem gerekli hem de kaçınılmaz hale getirmiştir. Böylelikle işletmeler varlıklarını sürdürebilmek için dijital çözümleri hızla benimsemişlerdir.

1.2.3. KOBİ'lerde Dijital Dönüşümün Avantajları ve Dezavantajları

Son yıllarda, dördüncü sanayi devrimine dayalı kavramlar ve teknolojilerin gelişimi, endüstriyi önemli ölçüde dönüştürmüştür. Endüstri 4.0 kavramının temel dayanağı üretimi, bilişim teknolojilerini ve internet kullanımının entegre edilmesidir. Bu bağlamda, Endüstri 4.0 örgütlerin süreçlerini daha verimli ve yenilikçi üretim modelleri oluşturulmasına imkân sağlamaktadır (BMBF 2012).

Dijital dönüşümün en büyük faydaları, özellikle üretim alanında görülmektedir. Küreselleşmenin etkisiyle coğrafi sınırların ortadan kalktığı günümüzde, rekabet her zamankinden daha yoğun hale gelmiştir. Bu doğrultuda, Endüstri 4.0'ın sunduğu avantajlı yöntemlere başvurmak, işletmeler için bir seçenek değil, zorunluluk halini almıştır.

Aşağıda belirtilen unsurlar, dijital dönüşüm uygulamalarının üretim süreçlerinde sağladığı en önemli değişiklikleri ve etkileri göstermektedir (https://www.endustri40.com):

- Dijital dönüşüm uygulamaları, sistemlerin izlenmesini kolaylaştırarak olası arızaların erken tespit edilmesine olanak tanır.
- Üretim sistemleri ve bileşenleri, dijital dönüşüm sayesinde öz farkındalık kazanarak daha verimli ve otonom çalışır.

- Dijital dönüşüm, çevre dostu çözümleri teşvik eder, kaynak israfını en aza indirir ve sürdürülebilir üretim süreçlerinin önünü açar.
- Dijital dönüşüm sayesinde üretim süreçlerinde yüksek verimlilik sağlanır, operasyonel etkinlik artar.
- Üretim esnekliği, dijital dönüşüm ile önemli ölçüde artar, böylece talebe tam uyumlu üretim süreçleri ve çıktıları elde edilir.
- Dijital dönüşüm uygulamaları, üretim maliyetlerini azaltarak daha rekabetçi ve karlı operasyonlar yürütülmesini sağlar.
- Dijital dönüşüm sayesinde zaman yönetimi daha etkin hale gelir, süreçler hızlanır ve kaynaklar daha verimli kullanılır.
- Dijital dönüşüm, etkin dijital tedarik zincirlerinin kurulmasını sağlar, tedarik süreçleri daha şeffaf ve hızlı hale gelir (Tekin, 2018: 253).
- İnsan gücü gereksinimi azalırken, makineler ve otomasyon sistemleri daha fazla devreye girer, böylece üretim süreçlerinde verimlilik ve güvenilirlik artar.

Dijital dönüşüm, şirketlere daha fazla esneklik ve verimlilik kazandırarak üretim süreçlerini optimize etmelerini, yenilikçi ekosistemler oluşturmak için değer önerileri geliştirmelerini ve pazar taleplerine hızlı bir şekilde yanıt vermelerini sağlamaktadır. Ayrıca, dijitalleşme, KOBİ'lerin, gelişmekte olan ve gelişmiş ülkelerdeki uluslararası pazarlarda fırsatları etkin bir şekilde keşfetmelerine yardımcı olan güçlü bir araçtır (Feliciano-Cestero vd., 2023: 1). Dijital dönüşüm süreci, birçok yeniliği beraberinde getirmiştir; bu yenilikler pek çok avantaj sağlarken, aynı zamanda bazı dezavantajları da beraberinde getirmiştir.

Endüstriyel üretim sistemlerindeki değişikliklerle birlikte, nitelikli iş gücünün yetişmesi için eğitime daha fazla önem verilmesi gerekmektedir. Aksi takdirde, nitelikli iş gücüne olan ihtiyaç artarken, niteliksiz iş gücüne olan talep azalacak ve bu durum işsizlik oranlarını daha da artıracaktır. Endüstri 4.0 ile birlikte ortaya çıkan dezavantajlar şu şekilde sıralanabilir (Kasa ve Arslan, 2020: 1813);

- Nesnelerin İnterneti (IoT) güvenliği giderek daha büyük bir sorun haline gelmektedir ve ortaya çıkan büyük verilerin analiz edilmesi, daha karmaşık ve zorlu bir hale dönüşmektedir.

- Kurumların IT departmanlarındaki iş gücüne olan ihtiyaç, dijitalleşme ile birlikte azalacaktır.
- Endüstri 4.0'a geçiş, zaman alıcı ve maliyetli bir süreç olduğu için, bazı kurumlarda bu değişime karşı isteksizlik görülebilir.
- Tüm üreticiler, yükselen piyasa koşullarına bağlı olarak rekabetten etkilenmeye zorunlu olarak başlayacaktır.
- Üretim süreçlerinde siber-fiziksel etkileşimler nedeniyle siber güvenlik tehditleri ortaya çıkabilir.
- İnsan faktörünün üretim sürecinden büyük ölçüde çıkarılmasıyla, kalite sürdürülebilirliği daha da kritik bir hale gelecektir (Tonga ve Tonga, 2022: 45).

İKİNCİ BÖLÜM
SİBER GÜVENLİK VE KOBİLER

2.1. Siber Güvenlik: Kuramsal ve Kavramsal Çerçeve

20. yüzyılda bilgi paylaşımı geleneksel yöntemlerle yapılırken, 21. yüzyılda dijitalleşme bu süreci köklü şekilde değiştirmiştir. İnternet pek çok hizmet sektöründe; eğitim, sağlık, hukuk ve ekonomi gibi alanlarda bilgi paylaşımını sağlamaktadır. Küresel ölçekte bilgi alışverişini kolaylaştıran internet, sonuç olarak bilginin değerini de artırmaktadır. Aynı şekilde, fiziksel ortamdan sanal ortama geçiş süreci bilgiye erişim daha kolay hale geldikçe hızlanmıştır. Bu dijital değişim, bilgisayar teknolojilerindeki hızlı ilerlemelerle daha da ivme kazandırmıştır. Ayrıca internet iş dünyasından bireylerin kişisel yaşamlarından kadar her alanda etkisini göstermektedir. Sağladığı faydaların ve kolaylığın yanı sıra dijital ortam, kurumlar ve kişiler için çeşitli tehditlere de neden olmaktadır. Bu sebeple, geçmişteki geleneksel yollarla işlenen suçlar, günümüzde dijital teknolojilerin sunduğu imkanlar sayesinde kolayca işlenmektedir. Özellikle, çeşitli teknolojik cihazlar üzerinde bulunan internet bağlantıları, siber güvenlik sorunlarının ortaya çıkmasına neden olmaktadır.

Hem kamu hem de özel sektörde; ağların, dijital verilerin, kritik sistemlerin ve yazılımların korunmasında siber güvenlik büyük öneme sahip dijital otoritedir. Veri ihlallerini önlemek, sistemlerin sürekliliğini temin etmek, kişisel ve ticari bilgilerin güvenliğini sağlamak için bu önlemlerin alınması gereklidir. Siber güvenlik konusundaki kamu ve özel sektör çalışanlarının farkındalığını artırmak, bu alandaki bilgi seviyelerini yükseltmek için eğitimlerin sürekli verilmesi çok önemlidir. Çünkü siber güvenlik hem kesintisiz hizmet sunumunu güvence altına almak, hem bireysel verilerin korunması için kritik bir öneme sahiptir. Ayrıca, siber güvenlik iş süreçlerinde meydana gelebilecek ağ problemlerinin ve olası kesintilerin önlenmesinin yanı sıra, hassas bilgilerin izinsiz erişimlere karşı korunması için de kritik bir adımdır. Buna ek olarak, ağların güvenliğinin sağlanmasında, güvenlik açıklarının minimize edilmesinde ve dijital tehditlere karşı etkin önlemlerin alınmasında siber güvenliğin rolü büyüktür. Hem kamu hem de özel sektörün bilişim sistemlerine dijital ortamda meydana gelebilecek siber saldırılar, terör olayları ve doğal afetler gibi tehditler zarar verebilmektedir. Bu da ulusal güvenliği doğrudan etkileyen bir durumu meydana

getirmektedir. Bu nedenle hem kamu hem de özel sektörde bu tür tehditlerin önüne geçebilmek için siber güvenlik stratejilerinin güçlendirilmesi çok kritik öneme sahiptir. Bu kapsamda bu bölümde, dijital dünyada sistemlerin korunması ve veri güvenliği için kritik bir öneme sahip olan siber güvenlik kavramı detaylı bir şekilde açıklanmıştır.

2.1.1. Bilgi ve İletişim Teknolojileri (BİT)

Günümüzde bilgiye yaklaşımda, teknolojik gelişmelerle birlikte önemli değişiklikler yaşanmıştır. Bilgi edinme, işleme, depolama ve bu süreçlerin sonunda fayda sağlama örgütsel yaşamın vazgeçilmez bir parçası haline gelmiştir. Günümüzde örgütsel yapılar, her büyüklükteki işletme ve kurum tarafından bilgi ve bilgiye bağlı teknolojilerin kullanılması, bilginin yönetilmesi bir tercih olmaktan çıkarak gerekliliğe dönüşmüştür. Bu nedenle, yeni kurulan örgüt yapılarının, çağın gereksinimlerine uygun şekilde yapılandırılması zorunlu hale gelmiştir (Solmaztürk, 2021: 7).

Russell (1970: 20-26), bilgi ve bilmek kavramlarını bir araya alıp incelemiştir. Sonuç olarak bu alanda kesin bir tanım yapmanın zor olduğunu ve neyin bilgi olduğu sorusu üzerinde yoğunlaşmanın gerekliliğini bildirmiştir (Güngör ve Güney, 2017: 133). “Bilgi” kavramı en temel ve sade şekilde “gerçekler, bilgiler, anlayışlar veya becerilerin, öğrenme, deneyim, algılama veya keşif yoluyla edinilmesi sonucu zihinde oluşan birikimi” olarak tanımlanmaktadır (Kapan, 2024: 2). Nitel veya nicel herhangi bir bilgi doğrudan kullanılabilir halde bulunmamaktadır. Çünkü bilgi, bazı değerlerin bir araya getirilerek zihin süzgecinden geçirilmesi sonucu elde edilmektedir. Bu sebeple, bilginin elde edilmesi ulaşılması gereken en üst noktayı göstermektedir. Bu aşamada, bilgiyi oluşturma yazında (Ackoff, 1989; Wilson, 2000: 13; Rowley, 2007: 164) değerler zinciri, bilgi hiyerarşisi ya da DIKM (data, information, knowledge, wisdom) olarak ele alınmaktadır. Piramidin en alt kısmında veri üst kısmında bilgi yer alırken, enformasyon ise veri ile bilgi arasında bulunmaktadır (Solmaztürk, 2021: 9).

Şekil 2.1. Bilgi Hiyerarşisi
Kaynak: (Rowley, 2007: 164).

Veri (data): Bilgi hiyerarşisin en alt basamağı veridir. Genellikle veriler ham bir halde bulunur. Veri sadece vardır ve kendi başına herhangi bir anlam taşımamaktadır. Kullanılabilir ya da kullanılmaz olan veriler, varlığını sürdürebilmektedir. Ancak veri kendi başına hiçbir anlam ifade etmez. Genellikle bilgisayar dilinde, bir elektronik tablo veri ile başlamaktadır (Bellinger vd., 2004: 3). Genel olarak veri; temel olarak varlığı bilinen, işlenmemiş, ham haldeki çeşitli işaretler, sembol, rakam ve harfi temsil edilen gözlemler veya kayıtlar olarak tanımlanmaktadır (Oğuz,2009: 3).

Enformasyon (information): En temel manada, enformasyon, düzenlenmiş veri olarak tanımlanabilmektedir. Enformasyon; belli bir sorun etrafında, belli bir amaca yönelmiş ve birbiriyle ilişkili verilerden oluşmaktadır (Şahin, 2009: 12). Enformasyon iletişim olgusuna dayanmaktadır. Ayrıca, iletişim olgusu alınan mesajın enformasyon niteliği taşıyıp taşımadığını belirlemektedir. Genellikle enformasyon, bir belge veya buna benzer bir araç yardımıyla alınan bir mesaj olarak tanımlanmaktadır. Tanımın devamında şu ifadelere yer verilmiştir: *"Her mesajda olduğu gibi enformasyonda da bir verici ve bir de alıcı vardır. Enformasyonun amacı, alıcının bir konudaki düşüncelerini değiştirmek, değerlendirmesi ya da davranışı üzerinde bir etki yaratmaktır. Enformasyon alıcısını biçimlendirmek zorundadır ve onun bakış açısında*

ya da anlayışında bir fark yaratmalıdır. Bu bağlamda enformasyon fark yaratan veridir" (Yılmaz,2009: 99).

Bilgi (knowledge): Alavi ve Leidner (2001;109)**,** bilginin *"olaylar, gerçekler, süreçler, kavramlar, fikirler, yorumlar, gözlemler ve yargılar ile ilgili sahip olunan kişiselleştirilmiş enformasyon"* olduğunu ileri sürmektedirler. *"Bilgi bilenlerin beyinlerinde ortaya çıkar ve orada uygulamaya geçirilir. Kuruluşlarda genellikle yalnızca belgelerde ya da dolaplarda değil rutin çalışmalarda, süreçlerde, uygulamalarda ve normlarda kendini gösterir"* şeklinde tanımlamıştır. Ayrıca bilginin "*yalın olmadığını, çeşitli unsurların birbiriyle karışmasından oluştuğunu, belli bir biçime sahip olmakla birlikte esnek olduğunu, sezgiler işin içine girdiğinde ona sözcüklerle sahip olmanın ya da mantık terimleri kullanarak anlamanın zor olduğunu belirterek*, *bilgi insanların içindedir [zihnindedir], insanın karmaşık ve önceden bilinemez doğasının bir parçasıdır"* değerlendirmesinde bulunmuşlardır. Bu tanımlamalar bilginin hem bir birikim hem de bir süreç olduğunu göstermektedir (Yılmaz, 2009: 100). Bilginin birçok özelliği olduğu Stephen Parker (2000: 233) dile getirmektedir. Birçok yönden bilgiyi "suya'' benzetmektedir, çünkü;

- *Elde edilmesi kolay veya zor olabileceğini*
- *Birçok farklı kaynaktan geldiğini*
- *Kullanılabilmesi için:*
    - *toplanması*
    - *işlenmesi*
    - *depolanması*
    - *dağıtılması gerektiğini*
- *Birçok farklı amaç için kullanılabileceğini*
- *Çarpıtma veya yanlışlık nedeniyle 'kirlenebileceğini'*
- *'sızıntılar' nedeniyle kaybolabileceğini*
- *Akar- ancak sudan farklı olarak kendiliğinden değil; bilgi akışının, ihtiyaç duyanlara, ihtiyaç duyduklarında ulaşması için yönetilmesi gerektiğini belirtmektedir.*

Açık bilgi (explicit knowledge): Yapılan faaliyetlere yeni değerler ilave etmek ve yeni bilgiler üretmek ve için kolaylıkla erişilebilen, sınırlı, yasaklı veya gizli olmayan bilgilerdir (Odabaş, 2008: 4). Wyatt (2001: 6), açık bilgiyi: erişilebilir ortamlarda yer alan, ilişkiler, kurallar ve gerçekler gibi doğruluğunu tartışmaya ihtiyaç duymadığımız bilgi olarak tanımlamaktadır. Ayrıca, açık bilgi aktarılabilir ve ifade edilebilir bilgidir. Başka bir ifade ile açık bilgi; kolay anlaşılan, kaydı tutulabilen ve iletişimi sağlanabilen bilgidir. Daha çok açık bilgi, bir konu hakkında bilgini içermektedir. Bu nedenle yazılı olarak kolayca transfer yapılabilmektedir. Özellikle, geleneksel bilgi yönetim süreci teknolojileri ve sistem merkezli stratejiler ile açık bilgi kolaylıkla paylaşılabilmektedir (Fayganoğlu, 2019: 1070).

Örtük bilgi (implicit/ tacit knowledge): Doğrudan ifade edilmesi güç olan ve sezgisel bilgiyi ifade etmektedir. Genellikle deneyim ve keşif elde edilmektedir (Bozkurt, 2014: 511). Ayrıca, örtük bilgi; kişisel görüşlerle "bilme yolu (know-how)" ile tecrübelerle kişisel sezgilerle, inançlarla, duygularla ve değerlerle ilişkilidir (Fayganoğlu, 2019: 1070). Genel olarak örtük bilgi, kelimelerle ifade edilmesi ya da metne veya çizime dökülmesi zor olan bilgidir (Sungur, 2014: 670).

İnsanlık tarihini inceleyen yazarlar bu evreleri inceleyerek; ilkel toplumdan tarım toplumuna, tarım toplumundan sanayi toplumuna ve sanayi toplumundan bilgi toplumuna geçiş şeklinde sıralamaktadır. Bu geçişlerin seyrine bakıldığında; yerleşik tarım düzenine geçiş bin yıl sürerken, tarım toplumundan sanayi toplumuna geçişin üç yüzyıl sürdüğü gösterilmektedir. Son olarak bilgi toplumuna geçişin ise çok daha kısa bir zaman diliminde gerçekleştiği belirtilmektedir. Ancak bilgi toplumuna geçiş evresinin çok kısa olmasına rağmen bu yeni düzenin insanlık tarihinde çok büyük bir değişime neden olduğu söylenebilmektedir (Karbuz, 2019: 9). Hızlı bir değişimin yaşandığı ve küresel değerlerin ön plana çıktığı içinde yaşadığımız bu dönem; bilgi toplumu, bilgi çağı olarak tanımlanmaktadır. Toplumsal yapıların değişmesine ve yeniden şekillenmesine bilgi teknolojilerindeki hızlı gelişmeler sebep olmaktadır (Çalık ve Sezgin, 2005: 62). Bu zamanda, gerekli olan bilginin üretimi bireylerin kullanımı önemlidir. Bu toplumun başka bir özelliği ise öğrenen bireylerin olmasıdır. Bilgi toplumunda birey; bilgiyi anlamak, yorumlamak, geliştirebilme ve kullanmak gibi yeteneklere sahip olmalıdır (Karabulut, 2015: 13).

Bilgisayar, bilgi toplumunun gelişmesinin yolunu açan teknolojilerindendir. Bilgi toplumunun temel belirleyicisi ve tamamlayıcısı, bilgisayara dayalı enformasyon ağlarıyla veri bankalarından oluşan kamusal altyapıdır. Yenileyici teknoloji olan bilgisayar teknolojisi; insanın zihinsel emeğinin yerini alan ve bilgi toplumunda kalkınmanın temelini oluşturan ve onu güçlendiren en önemli teknolojidir (Olcay, 2022: 60).

Bilgi toplumunda bilginin temel özellikleri; iletişim ağları içinde bölünebilir olması, taşınabilir olması, paylaşılabilir olması, sürekli üretilmesi, sürekli artış göstermesi ile toprak, emek ve sermayeni ikame edebilmesi şeklinde özetlenebilmektedir (Ünal, 2009: 137).

İletişimin kolaylaşması ve bilgi alışverişi hızlanması teknoloji geliştikçe mümkün olmuştur. Bilgi, iletişim ve teknoloji arasındaki bu sürekli etkileşim sonucunda, "Bilgi ve İletişim teknolojileri" çatı kavramı ortaya çıkmıştır. Uluslararası alanda İngilizce kısaltması ile kullanılagelen; "ICT" "Information and Communication Technologies" kavram, Türkçede uluslararası alan yazına içerik ve yapısal olarak uyumlu, işlek bir karşılık ve kısaltma bulmuştur: "Bilgi ve İletişim Teknolojileri: BİT" (İzci,2023: 19). Bilgi ve iletişim Teknolojilerinin kısaltması olarak kullanılan "BİT", çeşitli teknolojik araç ve kaynaklarının bilgiyi yaratma, depolama, yönetme, yayma ve iletişim amaçlı kullanılması olarak belirtilmektedir (Das, 2019: 97). Ayrıca BİT, bilgisayar ve iletişim teknolojilerinin birlikte kullanılmasıyla oluşturulmuş en yeni sistemlerdir. Buradaki Bilgi teknolojileri; bilginin toplanmasını, depolanmasını, işlemesini, ağlar aracılığı ile bir yerden bir yere iletilmesini sağlayan bilgisayar ve iletişim teknolojilerini de kapsayan tüm teknolojileri kapsamaktadır. Bu teknolojide, veri iletimi ve mikro elektroniklerin yanı sıra; televizyon, bilgisayarlar, mobil telefonlar, faks makineleri, bilgi ağları, videoteks software ve online tüm veri tabanları yer almaktadır. Mesajların bir yerden bir yere hızlı iletilmesine iletişim teknolojileri olanak sunmaktadır. Ayrıca, bilgisayar teknolojisi ise her alanda bilgi işleme ve hesaplama yeteneklerini milyonlarca kere artırmak imkânı sağlamaktadır (Özhavzalı ve Erduran, 2019: 145).

BİT'e, 20. yüzyılın sonlarında bilgisayar ve internet kullanımının hızla artması çok önem kazandırmıştır. Ülkeler BİT'i; daha az maliyet sarf ederek daha çok üretim

yapmak, verimliliklerini yükseltmek ve küresel dünyada pazar paylarını artırmak için daha etkin bir şekilde kullanmaya başlamışlardır (Akarsu vd., 2020: 310).

Günümüzde BİT birçok alanda; eğitim, üretim, mühendislik, savunma sanayi, ulaşım, bankacılık, iletişim, haberleşme, bilim, tıp ve ticarette yaygın bir şekilde kullanılmaktadır (Yılmaz, 2022: 31). Günlük yaşamda yer alan ve vazgeçilmez olan; bilgisayar, cep telefonları, telefon, telsiz ve uydu sistemleri ile ilişkin uygulamalar ve servisler BİT'i oluşturmaktadır. Bu nedenle BİT kavramı geniş bir kavram olup, çok disiplinli bir alanı kapsamaktadır (Magazzino vd., 2021: 1).

Bilgi ve iletişim teknolojileri olarak, bilgi ve iletişim teknoloji araçları sınıflanmaktadır Bilgi teknolojileri araçları; donanım, yazılım ve hizmet araçları olarak sınıflanabilir. İletişim teknolojileri araçlarını ise: donanım ve elektronik haberleşme araçları olarak alt sınıflara ayırabiliriz (TÜBİSAD ve Deloitte, 2018: 4).

Tablo 2.1. BİT Araçları

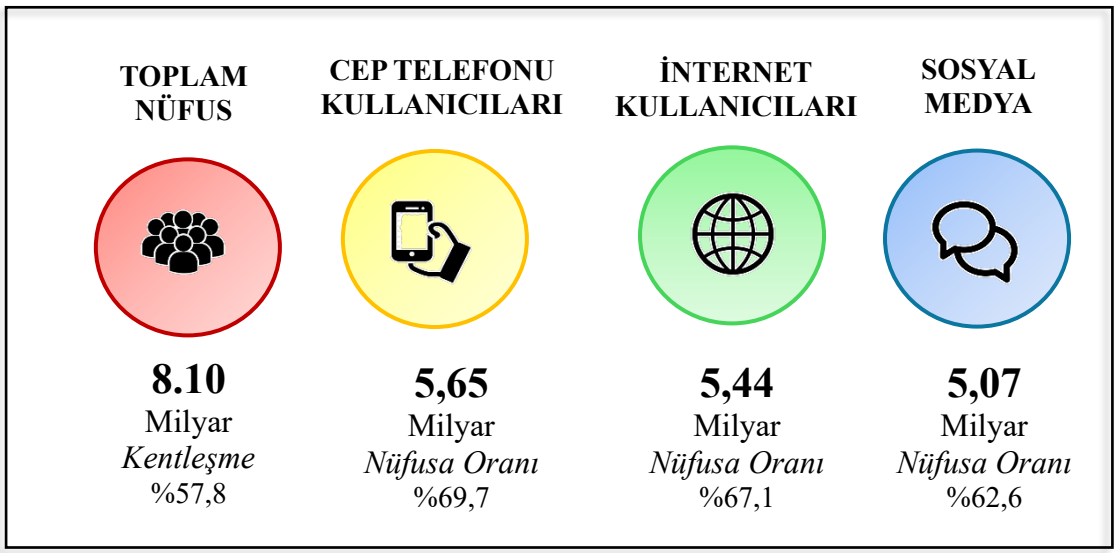
Kaynak: (TÜBİSAD ve Deloitte, 2018: 4).

Günümüzde insanlar ve kurumlar arasında oluşan iletişimlerdeki bilgi hacminin büyümesi BİT'in yaygın olarak kullanılmasının nedenlerinden biridir. Bilgi hacminde meydana gelen büyüme, onun anlaşılmasını ve kullanılmasını da zorlaştırmaktadır. Bilgi hacmi ile BİT ile arasında karşılıklı etkileşim bulunmaktadır. Bu etkileşim BİT'e duyulan ihtiyacın; bilgi hacminin büyümesiyle birlikte anlaşılmasının ve kullanılmasının zorlaşması sonucu artmasından kaynaklanmaktadır.

Oluşan büyük bilgi hacminden BİT vasıtasıyla, verimli bir şekilde faydalanmak ve doğru kararlar almak mümkündür. Bu nedenle bilginin üretilmesinde hızın önemli olmasının yanında bilginin iletilme süresinin kısalığı da çok önem arz etmektedir. Yeni bilgilerin üretilmesi, bilginin iletilmesindeki süre kısaldıkça daha da hızlanarak bilgi hacminin artması sağlanacaktır (İraz, 2004: 410).

2.1.1.1. Dünya'da Bilgi ve İletişim Teknolojilerinin Kullanımı

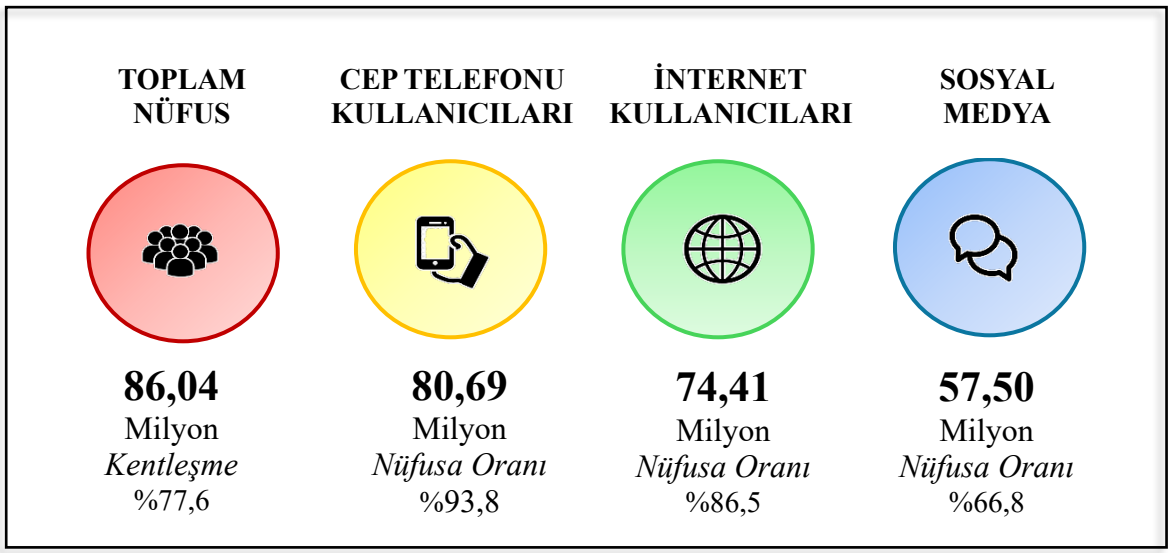
Nisan 2024' te yayımlanan verilere göre şu anda dünyada 8,10 milyar insan yaşamaktadır. En son raporlarda (2024 başlarında) ise dünya nüfusunun %69,7'sinin (5,65 milyar insanın) cep telefonu kullandığı bildirilmiştir. Son on iki ayda mobil kullanıcılara, 133 milyon yeni kullanıcı eklenmiş ve %2,4 oranında büyüme göstermiştir. İnternet kullanıcılarının ise 5,44 milyara çıktığı belirlenmiştir. Bu veriler de dünya nüfusunun yüzde 67,1'ine denk gelmektedir. Son veri analizleri internet kullanıcılarının sayılarının hızlı bir şekilde artmaya devam ettiğini göstermektedir. Bu veriler yıllık bazda %3,4'lük artışa işaret etmektedir (We Are Social, 2024).



2.1.1.2. Türkiye'de Bilgi ve İletişim Teknolojileri Kullanımı

Ocak 2024 itibarıyla Türkiye'nin nüfusu 86,04 milyon olarak bildirilmiştir. Türkiye nüfusunun %77,6'sı kent merkezlerinde yaşarken, %22,4'ü kırsal alanlarda yaşamaktadır. Son verilere göre 2024 yılı başında Türkiye'de toplam nüfusun yüzde 93,8'i (80,69 milyon insan) cep telefonu kullanmaktadır. Nüfusun

%86,5 ise (74,41 milyon insan) internet kullanmaktadır. Aktif sosyal medya kullanıcısı ise, 57,50 milyon insan (%66,8) olarak belirlenmiştir (We Are Social, 2024).



2.1.1.3. Siber Güvenlik ve BİT'in Tarihçesi

1837'den 1903'e kadar elektrik ve elektromekanik teknolojilerle iletişim kurma çabalarında, önemli ilerlemeler kaydedilmiştir. Bu dönemlerde, iletişimde kullanılan yöntemler ve teknolojiler hızla evrilmiş, pek çok yenilik birbirini izlemiştir. BİT'in tarihçesini pek çok bilim insanı, farklı olaylara bağlamaktadır. Ancak genel olarak 1837'de telgrafın icadıyla bu sürecin başlangıç olarak kabul görmektedir (Cridland, 2008: 1).

Dönemin önde gelen mucitlerinden Sir John Ambrose Fleming ile Nevil Maskelyne arasındaki mesleki rekabet, 1903 yılında İngiltere'de önemli bir noktaya ulaşmıştır. Güvenli radyo alıcısı ve vericisi sistemini geliştiren Guglielmo Marconi halka tanıtım yaptığı sırada, Fleming bu sistemin güvenliğini gizlice aşmıştır. Tanıtım esnasında Fleming kaynağı belirsiz mesajlar göndererek, teknoloji tarihinde ilk bilgisayar korsanlığı (hackerlik) girişimini yapmıştır (Güngör, 2015: 26).

ABD'li bilim adamları tarafından 1946 yılında silah ve nükleer hesaplamalar için elektronik veri işleme kapasitesine sahip ilk bilgisayar ENIAC (Elektronic Numerical Integrator and Computer) geliştirilmiştir. İlk bilgisayarlar olarak tanımlanan ENIAC ile matematiksel hesaplar yapılmaya başlanmış, bu hesaplamalar

sonucunda elde edilen veriler estetik amaçlar için kullanılmıştır (Çokokumuş, 2012: 53).

Polonyalı matematikçileri ve kriptoloji uzmanları olan Jerzy Różycki, Henryk Zygalski ve Marian Rejewski tarafından Enigma Şifreleme Sistemi'nin kırılması, bilgi güvenliği alanında kabul edilen dönüm noktalarından biridir. Bu kırılma İkinci Dünya Savaşı öncesinde yaşandığı için Almanların savaşı kaybetmelerinde önemli rol oynamıştır (Güngör, 2015: 26).

RAND Corporation adlı kuruluş tarafından altmışlı yılların başında Amerika Birleşik Devletleri'nde olası bir nükleer savaş sırasında, güvenli olarak askeri haberleşmeyi sağlamak amacıyla, bilgisayar ağı geliştirmek üzerine bir arge projesi geliştirilmiştir. İnternetin gelişimi için bu proje ilk adım olmuştur. 1969 yılında bunun devamı olarak ABD Savunma Bakanlığı tarafından ARPANET (Advanced Research Project Agency Network) adıyla bilgisayarlar arası ağ iletişimi başlatılmıştır (Yıldırım, 2014: 52).

Bilgisayarlar için kötü niyetli yazılımlar internetin icatı ve kullanılmaya başlanması ile ortaya çıkmış ve bilgisayarlarda hızla yayılmaya başlamıştır. ARPANET'te 1970'lı yılların başında "The Creeper'' virüsü ilk olarak tespit edilmiştir (Eken, 2013: 513). İletim kontrol protokolü'nün (TCP) dört uyarlaması 1978'e kadar oluşturulmuş ve denenmiştir. Bu küme 1980'de sabitleşmiş ve ARPANET'e bağlı bilgisayarlar arasındaki iletişimi kolaylaştırmıştır. İletim Kontrol Protokolü/İnternet Protokolü (TCP/IP) olarak bilinen yeni protokole bütün ARPANET kullanıcıları 1983'te geçiş yapmıştır. Aynı yıl TCP/IP, ARPANET'i de içeren Savunma Bakanlığı internetinde kullanılmak üzere standartlaştırılmıştır (Haki, 2007: 5).

Morris virüsü, 1988 yılında Rober Tappan Morris tarafından eğlence amaçlı yazılmıştır ve tarihte bilgisayarlarda ilk hizmet engelleme saldırısı olarak bilinmektedir. "Morris solucanı'' olarak da bilinen bu dijital virüs, Morris'in kodlama sırasında yaptığı bir yanlış sonucu ortaya çıkmıştır. Bu program sadece birkaç gün içinde günümüz İnternetinin öncüsü olan Arpanet'i dolaşmış ve internete bağlı olan bilgisayarların %10′unun ağlarını çalışmaz hale getirmiştir (Atasever vd., 2019: 240).

Önemli siber saldırı faaliyetlerden birisi, 1999 yılında dünya çapında bilgisayarlara sızan Melissa virüsüdür. Döneminde 80 milyon dolarlık zarara neden olan dijital virüs, Davis Smith tarafından kötücül yazılımlar aracılığı ile yayılmıştır (Garber, 1999: 17). "World Wide Web" in 1990'larda kurulması ile akademik alanın dışında pek çok kullanıcının birbiriyle bağlantı kurması mümkün olmuştur. Bu gelişimler sonucunda bilginin her bir bireyin bilgisayarından erişebilir olması fikrini doğurmuştur. Bu teoriye dayanarak bilgisayar kullanımının askeriyeden hükümetlere, özel şirketlerden bireylere kadar yayılım sağlanmıştır (Gündoğdu, 2023: 1327).

İnternet sayesinde 2000'li yılların başından itibaren bilgisayar ağları hem birbirleriyle hem de bunların kullanıcılarıyla etkileşime girmiş ve bunun neticesinde internet büyük bir siber uzay dönüşmüştür. Günümüzde internet teknolojileri insan yaşamına inanılmaz fırsatlar sunarak ve yaşamı her yönüyle daha da kolaylaştırmaktadır. Ancak internet teknolojileri diğer yandan da saldırgan kişi veya grupların hedeflerine ulaşmaları için elverişli bir zemin hazırlamıştır. Bu nedenle internet üzerinden yapılan siber saldırılarda adeta patlama yaşanmıştır (Güngör, 2015: 30).

Siber güvenlik alanında 2010'lar önemli değişimlerin ve dönüşümlerin yaşandığı bir dönemdir. Bu dönem aynı zamanda tehditlerin daha karmaşık ve yaygın hale geldiği karmaşık bir süreci ifade etmektedir. İran'ın nükleer tesislerine yönelik Haziran 2010'da gerçekleştirilen Stuxnet saldırısı da endüstriyel kontrol sistemlerinin korunmalarına rağmen saldırıya uğrayabileceğinin gösteren önemli bir siber saldırıdır. ABD'de meydana gelen geniş çaplı DDoS (Dağıtık Hizmet Dışı Bırakma) saldırısı da önemli örneklerden biridir. IoT cihazlar aracılığıyla yapılmış bu saldırı en büyük siber saldırılardan biri olarak tarihe geçmiştir (Gönen vd., 2021: 1148).

"WannaCry" adlı siber saldırı 12 Mayıs 2017 tarihinde gerçekleşmiş ve siber saldırı riskinin etkisini açıkça gösteren önemli bir örnektir. Ağırlıklı olarak Avrupa ülkelerini etkilemiş bu saldırı, birçok kullanıcıyı ve kurumu hedef almıştır. Bir fidye yazılımı olan "WannaCry", birçok bilgisayarı etkileyerek dosyaları şifrelemiş ve fidye talep etmiştir. Bu saldırı, siber riskin gerçek bir tehdit olduğunu ve küresel çapta ciddi etkilere yol açabileceğini bir daha göstermiştir. 2017 yılında ortaya çıkan diğer bir fidye yazılımı ise BadRabbit yazılımıdır. Bilgisayar sistemlerine sızan bu siber saldırı,

dosyaları şifreleyen ve ardından fidye talep eden bir saldırı türüdür. Özellikle Rusya, Ukrayna ve Türkiye gibi ülkelerde BadRabbit fidye yazılımı, yaygın olarak etkili olmuştur (Solmaz,2023: 3)**.**

Teknolojik ilerlemelerin toplumsal yapıyı dönüştürmesi ve dijitalleşmenin hızla ivme kazanması beraberinde çeşitli siber tehditleri de gündeme getirmektedir. Özellikle küresel ölçekte fidye yazılımları, kişisel veri kayıpları ve kimlik avı gibi siber saldırılar giderek daha da sık görülmektedir. Bu tehditlerin çeşitliliği ve olası etkilerini engellemek için, güvenlik ihlallerinin minimize edilmesi, etkili ve kapsamlı stratejilerin geliştirilmesi zorunlu hale gelmiştir. Bu nedenle, dijital ekosistemde güvenliğin sağlanması yalnızca kurumsal düzeyde değil, aynı şekilde topluluklar ve bireyler için de hayati bir önem arz etmektedir. Modern toplumların karşı karşıya olduğu risklere karşı dayanıklılık geliştirilmesinde dijital altyapıların güvenliğinin güçlendirilmesi en temel unsurdur.

2.1.1.4. BİT'in İşletmelere Faydaları

KOBİ'ler; Orta, küçük ve mikro işletmeler, iş yaratarak ve insanların çoğunluğunun gelir seviyelerini artırarak ekonomilerde önemli rol oynarlar. Bu işletmeler inovasyonun itici güçleri olarak tanımlanmakta ve ekonomik büyümeye hizmet etmektedir. Ayrıca KOBİ'ler, eşit gelir dağılımı sosyal hedefine hizmet eder. Ancak, günümüzde bu işletme kategorileri pek çok fazla zorlukla karşı karşıyadır. Yaşanan zorlukları en minimuma indirmek için, rekabet gücünü ve verimliliği artıracak BİT'lerin benimsenmesi de dahil olmak üzere çeşitli çözüm stratejileri önerilmektedir. Geniş yelpazedeki bilgisayarlı bilgi ve iletişim teknolojileri BİT'ler olarak tanımlanmaktadır. Bu teknolojiler; kablolu veya kablosuz internet, elle tutulan cihazlar, dizüstü bilgisayarlar, masaüstü bilgisayarlar, düzenleyici ve elektronik tablo gibi iş üretkenliği yazılımları, veri depolama, ağ güvenliği ve kurumsal yazılım gibi ürün ve hizmetleri içermektedir (Ongori ve Migiro, 2010: 93). KOBİ'lerin günümüz bilgi tabanlı ekonomisinde, rekabet avantajı sağlayacak hizmetler sunmalarını verecek süreçleri benimsemeleri önemlidir. Kurumsal performans üzerinde BİT'nin önemli bir olumlu etkisi olduğu ispatlanmıştır. Bu nedenle KOBİ'ler için hayati öneme sahiptir (Apulu ve Latham, 2010: 4). Günümüzde ekonominin tüm sektörlerini ve insan faaliyetlerinin tüm alanlarını kapsayan BİT örgütsel verimliliği ve işletme

operasyonlarını artırarak yaşam standardını iyileştirebilir (Udo ve Edoho, 2000: 329). KOBİ'ler arasında BT'lerin bir adım değişikliği yaratma ve onları daha rekabetçi hale getirme, aynı zamanda yenilikçiliği teşvik etme potansiyeline sahip olduğu söylenebilir. Dünya ekonomileri BT'lerdeki ilerlemelerin artan entegrasyonuna doğru ilerlemeye devam ettikçe, KOBİ'lerin hem bölgesel hem de uluslararası pazarlara katılarak bu faydaları elde etmeleri muhtemeldir. Küreselleşme çağında KOBİ'ler tarafından BT'lerin benimsenmesi, hayatta kalmaları için kritik öneme sahiptir (Sołek-Borowska, 2018: 214).

Bilgi ve İletişim Teknolojileri (BİT), Fullanteli ve Allegra'ya (2003: 45) göre, işletmelere rekabet güçlerini artırmak için geniş bir yelpazede olanaklar sağlar. BİT'ler işletmelere aynı zamanda; yeni danışmanlık modları, sürekli eğitim ve uzaktan danışmanlık gibi uzmanlaşmış bilgi hizmetlerine erişim mekanizmaları sunar. Ayrıca, BİT'ler vasitesiyle kuruluşlar gerçek zamanlı bilgi alışverişinde bulunabilir iş ortakları, tedarikçileri ve müşterileriyle daha yakın ilişkiler kurabilir. Bu zaman anında müşteri geri bildirimi, şirketlerin değişen müşteri taleplerine hızlı tepki vermesini ve yeni pazar nişlerini tanımasını kolaylaştırır. Bu da, BİT'nin sunduğu potansiyelleri kullanabilen kuruluşların Bilgi Yönetimi, Tedarik Zinciri Yönetimi ve Müşteri İlişkileri Yönetimi gibi yenilikçi süreçleri daha etkili bir şekilde yönetebileceği göstermektedir.

Sin Tan ve diğerlerine (2010) göre ise BİT benimsenmesinin en yaygın yararları arasında şunlar yer alır:

- Tedarikçiler ve müşteriler ile iletişimde düşük işletme maliyeti;
- Tedarikçiler tarafından daha iyi iletişim yoluyla malların teslimatında artan hız;
- Daha iyi koordinasyonu yoluyla değer zincirinde firmaların verimlilik artışı;
- Ticaret ortakları arasında daha yakın çalışma ilişkisi;
- Müşterileri ile etkili iletişim aracı;
- İşletmeyi yeni iş fırsatlarına açan daha büyük piyasa riski;
- Tedarikçiler ve müşteriler ile bilgi alışverişini geliştirerek pazar bilgisine daha fazla erişim;
- İşletmeleri yönetme ve organize etmenin yeni yollarını kolaylaştırma açısından
- Gelecekteki bir araç olarak görmek.

Tablo 2.2: Literatürde İnternet Tabanlı BİT'lerin Yararları

Yazar(lar)	BİT Benimsemenin Sağladığı Yararlar
Walczuch vd. (2000: 566)	1. Mesafeyle ilgili engellerin ortadan kalkması 2. Geliştirilmiş firma imajı 3. Tüm dünyada sürekli reklam 4. Artan satışlar 5. Bilgi toplamanın etkinliği 6. Daha fazla müşteri hizmeti 7. Artan müşteri memnuniyeti 8. Uluslararası pazarlara ulaşma imkânı 9. İş ortamının daha iyi bilinmesi 10. Konum genelinde bilginin kullanılabilirliği 11. Müşteriler ile ilgili daha iyi bilgi sağlama 12. Artan verimlilik 13. Daha iyi tedarikçi hizmetleri ve desteği 14. Daha hızlı ve/veya daha esnek malzeme teslimatı 15. Tedarikçiler edinmede daha düşük maliyet
Khatibi vd. (2003: 81)	1. Geliri artırmak 2. İşletme maliyetini azaltmak 3. Müşteri hizmetlerini artırmak 4. Tedarikçilerle ilişkilerde verimlilik artırmak 5. Bilgi akışını artırmak 6. Şirket markasını ve kurumsal imajını geliştirmek 7. Müşteri sadakatini elde tutmayı artırmak 8. İş süreçleri akışını iyileştirmek
Jones vd. (2003: 4)	1. Maliyet tasarrufu 2. Zaman tasarrufu 3. Geliştirilmiş bağlantı 4. Kalite iyileştirmeleri 5. Stratejik iyileştirmeler 6. Yeni pazarlara erişim
Yeung vd. (2003: 229)	1. Müşterilerle gelişmiş bilgi alışverişi 2. Geliştirilmiş müşteri hizmetleri 3. Geliştirilmiş müşteri sadakati ve elde tutma 4. Tedarikçilerle daha iyi bilgi alışverişi 5. Web tabanlı satın alma yoluyla düşük maliyet 6. Uluslararası pazarlara maruz kalma 7. Firma bilgilerinin korunma maliyetinin düşürülmesi
Alam vd. (2005: 191)	1. Küresel pazara ulaşabilme 2. Zaman engellerinin olmaması 3. Geliştirilmiş görüntü 4. Düşük maliyetli iletişim 5. Müşteriler ve tedarikçiler ile doğrudan bağlantılar 6. Gelecekteki iş araçları

Kaynak: (**Sin Tan vd., 2010: 31-32).**

2.1.2. Bilgi Güvenliği

Organizasyonların sahip olduğu en değerli üretim faktörü günümüzün artan rekabet koşulları çerçevesinde bilgi haline gelmiştir. Son yıllarda organizasyonlara

sürdürülebilir rekabet avantajı sağlayan bilginin yönetilmesi de üzerinde en çok durulan konulardan biridir (Atılgan, 2009: 204).

Verinin belli bir anlam ifade edecek şekilde düzenlenmiş hali bilgi olarak tanımlanmaktadır. Veri ve ilişkili olduğu konu bilgi üretecek şekilde bir araya getirilir. Bilgi, işlenmiş veri olarak da ifade edilebilmektedir. Shannon tarafından *"bir konu hakkında var olan belirsizliği azaltan bir kaynak"* olarak tanımlanmıştır. Sonuç olarak, veri üzerinde yapılan uygun bütün işlemlerin (varsayımlar, formüller, mantığa dayanan dönüşüm, basitleştirmeler ve ilişkiler) çıktısı, bilgi olarak tanımlanabilmektedir (Canbek ve Sağıroğlu, 2006: 166).

Bilgi aynı zamanda, eylem veya karar için ilgili çıkarım, anlam veya girdi içeren bir mesajdır. Bilgi hem tarihsel (yeniden yapılandırılmış resim ve işlenmiş veri) hem de güncel (iletişim) kaynaklardan gelmektedir. Bilginin amacı özünde karar almak veya sorunları çözmek için bir fırsatı değerlendirmeye yardımcı olmaktır (Liew, 2013: 50). Çeşitli formlarda mevcut olan bilgi, farklı bilgi türleri bir organizasyon için değişik değerler taşıyabilmektedir. Bilginin bütünlüğü, kullanılabilirliği ve gizliliğine yönelik tehditlerin etkisi ise, söz konusu bilginin organizasyonun misyonuna ve doğasına bağlı olarak farklılık gösterebilmektedir.

Birçok ortamda bilgiler bulunabilmekte, işlenebilmekte ve iletilebilmektedir. Genel olarak sahip olunan bilgilerin temelde hangi platformlarda bulunduğuna ya da bulunacağına yönelik çalışanlara bilgilendirmeler yapılmaktadır. Bilginin yer aldığı belli başlı ortamlar aşağıda yer almaktadır (Şahinaslan, 2009: 191);

• **Fiziksel ortamlar;** Tahta, pano, kâğıt, dolaplar, faks, Çöp/Atık kâğıt kutuları

• **Elektronik ortamlar;** CD, e-posta, Disk, USB, Disket, Bilgisayarlar, mobil iletişim cihazları vb. manyetik ortamlar.

• **Sosyal ortamlar;** Muhabbetler, telefon görüşmeleri, toplu taşıma araçları ve yemek araları vb. sosyal aktiviteler.

• **Tanıtım platformları;** Eğitimler, reklamlar, internet siteleri, sunular, broşürler, video ya da görsel ortamlar.

Daha çok bilginin depolanmasına ve taşınmasına bilgi teknolojilerinde yaşanan gelişmeler, imkân vermektedir. Her geçen gün küçük ama marifeti büyük, çok fonksiyonlu teknolojik cihazlar sayesinde daha fazla bilgi elektronik ortama aktarılmakta, işlenmekte, depolanmakta, hizmete sunulmakta ve taşınabilmektedir. Elektronik ortamlar üzerinde bilginin yoğun kullanımı ve hareketliliği günümüzde kurumlar, şirketler ve bireyler açısından çeşitli güvenlik risk ve sorunlarını da beraber getirmektedir. Bu durum teknolojik ilerlemelere paralel olarak her geçen gün artış göstermektedir. Bu nedenle kurumlarda bilgi güvenliğinin sağlanması kurumun güvenilirliği, imajı ve faaliyetlerinin devamı açısından oldukça önemli bir hale gelmektedir (Şahinaslan, 2009: 597).

Genel olarak bilgi güvenliği; bilgi varlıklarının bütünlüğünü, erişebilirliğini ve gizliliğini tanımlamaktadır (Brykczynski ve Small, 2003: 12).Bilgi güvenliği, "*bilginin bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda, istenmeyen kişiler tarafından elde edilmesini önleme olarak"* ifade edilmektedir. Bilgisayar teknolojilerinde güvenliğin amacı ise "*kişi ve kurumların bu teknolojilerini kullanırken karşılaşabilecekleri tehdit ve tehlikelerin analizlerinin yapılarak gerekli önlemlerin önceden alınmasıdır*" (Canbek ve Sağıroğlu, 2006: 169).

Caballoro Bilgi güvenliğini (2013: 1) "*tüm organizasyonun güvenlik sorunlarını yalnızca bir tür saldırıyı hafifletmeyi amaçlayan teknik kontrollere dayanarak değil, kendi stratejik yönlendiricilerine dayanarak çerçevelemesi ve çözmesi gerektiği anlamında bir iş sorunu olarak*" tanımlamaktadır.

Bilgi güvenliğine yönelik çeşitli tehditlere maruz kalan internet ve bilgisayar kullanıcıları için bilgi güvenliği (InfoSec) günümüzde büyük bir endişe kaynağıdır. Her gün bilgisayar korsanları, virüsler, casus yazılım, zombi ağları, spam ve bilgi güvenliğine yönelik diğer birçok tehdit nedeniyle milyonlarca güvenlik olayı yaşanmaktadır (Huang, 2010: 221).

Bilgi güvenliğinin amacı; erişilebilirliğini sağlayacak, bilginin bütünlüğünü koruyacak altyapıyı hayata geçirerek, kişisel bilginin mahremiyetinin korunmasını sağlamak, müşteri ve personel bilgilerinin gizliliğini koruyarak kurumsal itibarı

artırmaktır. Kullanılan bilgi sistemlerine (yazılım, donanım) bilgi işleme faaliyetlerine yönelik güvenlik kontrolleri uygulanmalıdır. Bu kontroller sayesinde bilgi varlıklarının çalınması, kaybı, hasarı, kuruluşun faaliyetlerinin kesintiye uğraması ve tehlikeye girmesi engellenmektedir. Çoğu organizasyon, bilişim teknolojilerinin sağladığı imkanlar ve kolaylıklar sebebiyle faaliyetlerini gerçekleştirmek için bilgi teknolojilerini kullanmasını zorunlu hale getirmiştir. Bu teknolojilerde meydana gelebilecek güvenlik risklerine karşı bilişim sistemlerine bağımlılık arttıkça duyarlılık da artmaktadır (Acılar, 2009: 30).

Bilgi sistemlerinde bilgi güvenliği konusunda zafiyet oluşturan, virüsler, solucanlar, Truva atları, arka kapılar, mesaj sağanakları, kök kullanıcı takımları, telefon çeviriciler, korunmasızlık sömürücüleri, klavye dinleme sistemleri, tarayıcı soyma ve casus yazılımların yanında, reklâm, parazit, hırsız, püsküllü bela yazılım, tarayıcı yardımcı nesnesi, uzaktan yönetim aracı, ticari RAT, bot ağı, ağ taşkını, saldırgan ActiveX, Java ve betik, IRC ele geçirme savaşı, nuker, paketleyici, ciltçi, şifre yakalayıcılar-soyguncular, şifre kırıcılar, anahtar üreticiler, e-posta bombardımanı, kitle postacısı, web böcekleri, aldatmaca, sazan avlama, web sahtekârlığı-dolandırıcılığı, telefon kırma, port tarayıcılar, sondaj aracı, arama motoru soyguncusu, koklayıcı, kandırıcı, casus yazılım ve iz sürme çerezleri, turta, damlatıcı, savaş telefon çeviricileri ve tavşanlar adı altında ve her biri farklı amaçlara yönelik değişik yöntemler kullanan çok çeşitli kötücül yazılımın var olduğu da tespit edilmiştir(Canbek ve Sağıroğlu, 2006: 169).

Yaygın olarak kullanılan Gizlilik, Bütünlük ve Erişilebilirlik (CIA), popüler bir bilgi güvenliği modelidir. Güvenli yazılım oluşturmanın başlıca anahtarlarıdır. Güvenlikte temel bir model olan CIA üçlüsü, Şekil 2.2’te, gösterilmiştir. Genellikle, herhangi bir güvenli sistemin tasarlanmasında CIA üçlüsünün üç yönünün korunmasını sağlamak önemli bir adımdır (Al-Far vd., 2018: 1).

Şekil 2.2. Bilgi Güvenliği Modeli
Kaynak: (Al-Far vd., 2018: 1) *uyarlanmıştır.*

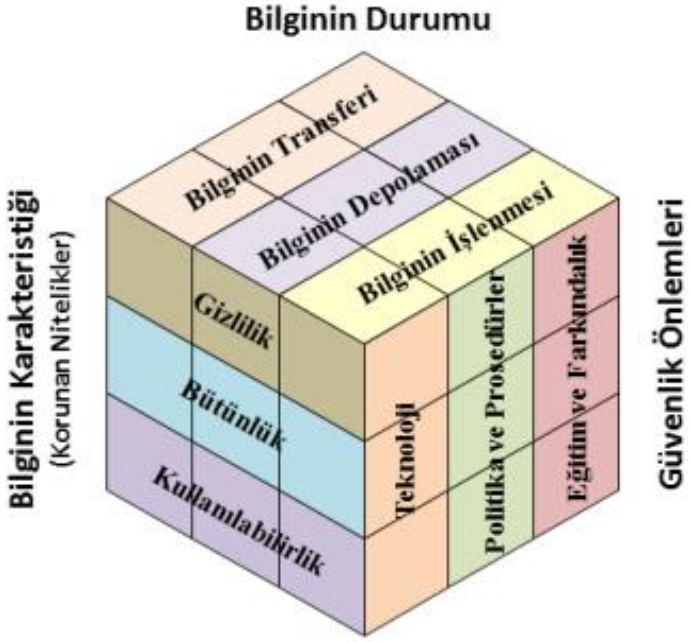
Utakrit tarafından (2021: 48) bilgi güvenliğinin üç temel boyutu aşağıdaki gibi ifade edilmiştir:

● **Gizlilik:** Gizli bir şekilde bilgilerin saklanması. Çok hassas ve özel bilgilere; ulusal kimlik numarası, doğum tarihi, vergi bilgileri ve sosyal güvenlik numarası gibi yalnızca yetkili kullanıcılar erişebilmektedir.

● **Bütünlük:** Doğru bir şekilde görüntülenen bilgiler hiçbir şekilde değiştirilmez. Bilgileri yalnızca yetkili kullanıcılar değiştirebilmektedir.

●**Erişebilirlik:** Genellikle müşterilere önceden bildirilen planlı bakım haricinde bilgiler, yetkili kullanıcılar için derhal erişebilir hale getirilmektedir.

Bilgi güvenliği ile ilgili CIA üçlüsünden farklı olan modeller de literatürde bulunmaktadır. McCumber (2004) modeli, çok detaylı ve boyutlu bakış açısı sunmaktadır. Bu model bilgi güvenliği politikası geliştirilirken kurumlar ve bilgi merkezleri için dikkate alınması gereken bir kuramsal modeldir. Bilgi güvenliğinin model üzerinde sağlanması ile ilgili olarak; bilginin üç farklı yüzü (karakteristiği/güvenlik servisleri, durumu ve güvenlik önlemleri) gruplandırılarak verilmektedir.



Şekil 2.3. McCumber Bilgi Güvenliği Modeli
Kaynak: (Henkoğlu, 2015: 32).

McCumber modelinde, bilgi güvenliğinin farklı boyutlarını gösteren gruplar da yer almaktadır. Modelin bir yüzünde gizlilik; bilgi güvenliğinin temel unsurları olarak kabul edilen kullanılabilirlik ve bütünlük ilkeleri ile bilgi karakteristiği adı altında toplanmıştır. Diğer yüzde bilginin durumu; bilginin işlenmesi, bilginin transferi ve bilginin depolanması ismiyle gruplandırılmıştır. Küpün son ve üçüncü yüzünde ise güvenlik önlemleri; politika, prosedür ve teknolojilerle farkındalık ve eğitim alanları başlığı altında toplanmıştır (Henkoğlu, 2015: 32).

Bilgi güvenliği için bilgi varlıklarının korunması gerekmektedir. Bilgi varlıkları; bir kuruluş veya kurumun katma değer sağlamak, rekabet oluşturmak, kar etmek, kurumsal sürdürülebilirliğini sağlamak amacıyla sahip olduğu veya sahip olması gereken teknoloji, ürün, organizasyon ve pazara ait bilgilerin tümü olarak isimlendirilebilmektedir. Fiziksel olarak bu bilgi varlıklarının korunması için fiziksel güvenliğin, gereken bilgilerin transfer edilmesini sağlanmak için iletişim güvenliğinin, bilgisayar ve ağ güvenliğinin sağlanması için bilgisayar sistemlerine erişimlerin kontrol edilmesi gerekmektedir. Farklı güvenlik türlerinin bilgi güvenliğini yüksek seviyede sağlayabilmesi için bu tamamının organize bir şekilde sağlanması gerekmektedir (Baykara, 2013: 238).

2.1.3. Siber Güvenlik

Özellikle son yıllarda BİT çeşitli yönleriyle çok gelişmiştir. BİT'in çok gelişmesi ve bireyler için ekonomik olarak daha kolay erişilebilir hale gelmesi, internetin tüm dünyada daha yaygın bir biçimde kullanımını neden olmuştur. İnternetin gündelik işleri; bilgiye erişim, bilgi paylaşımı, alışveriş ve iletişim gibi hızlı ve kolay hale getirmesi ile toplum için önemli bir ihtiyaç haline gelmiştir (Rahim vd., 2015: 607). Ancak internet sağladığı birtakım yararlar kadar, birçok tehdidi de bünyesinde barındırmaktadır. Teknolojik gelişmelerle birlikte saklanan veya elektronik ortamda bulunan kişisel bilgiler, siber saldırılar için önemli bir hedef haline gelmektedir (Kurnaz ve Önen, 2019: 83).

Bilgisayar bilimcileri tarafından ilk olarak 1990'lı yılların başında siber güvenlik terimi, bir ağa bağlı bulunan bilgisayarlarla ilgili bir dizi güven sorunlarını tespit etmek amacıyla kullanılmıştır (Hansen, 2009:1155). Schatz ve diğerleri, (2017: 66)' a göre, "*Siber güvenlik, siber uzay içerisindeki varlıkların, organizasyonların, insanların ve verinin, gizliliğinin, bütünlüğünün, erişilebilirliğinin korunması için kurumlar ve devletler tarafından takip edilen güvenlik risk yönetimi süreçleriyle ilgili yaklaşım ve aksiyonlardır*."

Bilgisayar korsanı saldırıları ve kötü amaçlı yazılımları gibi tehditlere karşı dijital sistemlerin korunmasını "Siber güvenlik" terimi ifade etmektedir. Genellikle siber saldırı riski taşıyan durumlar; bir şirketin hacklenebilmesi, bir bireyin bağlı cihazlarının saldırılması veya devlet tarafından yönetilen kritik altyapılara yapılan dijital saldırıları tanımlamaktadır. Hem kurumsal hem de bireysel düzeyde bu alandaki tehditler ciddi güvenlik sorunlarına neden olabilmektedir (Bay, 2016: 1).

Bilgi güvenliği kavramı ile siber güvenlik kavramı farklı zamanlarda sıklıkla birbirinin yerine kullanılmıştır. Ancak bu iki kavram arasında önemli farklılıklar vardır. Genel olarak bilgi güvenliği; bilginin erişilebilirliğinin, bütünlüğünün ve gizliliğinin sağlanması olarak tanımlanmaktadır (Solms ve Niekerk, 2013: 98). Siber güvenlik ise; siber uzayda (fiziki dünyadan bağımsız olarak, iletişim ve bilişim teknolojilerinin birbirine bağlı bulunduğu ve içerisinde farklı hakimiyet

mücadelelerini de barındırdığı soyut alan) yapılan siber saldırılara karşı kendini koruyabilme ve muhafaza edebilme yeteneğine odaklanmaktır (Kissel, 2013: 58).

Siber güvenlik özellikleri genellikle; uygulama güvenliği, kötü amaçlı yazılımlardan, virüslerden, saldırılardan veya dış tehditlerden korumak için prosedürel, donanım ve yazılım yöntemlerin kullanılmasını içermektedir. Özellikle siber güvenlik yazılım ve uygulama geliştirme sürecinde çok büyük önem taşımaktadır. Siber saldırılar ağlar üzerinden giderek daha fazla erişilebilir hale gelmektedir. Bu da yazılıma veya uygulama verilerine zarar verebilecek çok çeşitli tehlikelerin ortaya çıkmasına neden olacaktır. Bu nedenle yetkisiz kodların özel ve hassas verilere erişmek, değiştirmek, silmek ve çalmak için uygulamaları manipüle etmesini engelleyen rutin güvenlik işlemleri uygulanmaktadır. Genellikle bu önlemler; şifreleme veri doğrulama, güvenlik yamaları ve izin denetimi gibi önlemleri içermektedir. Karşı önlemler; uygulama güvenliğini garanti etmek için alınacak önlemlerdir. Yazılım için en önemli savunma yöntemi verilerin veya dosyaların yüklü programlar tarafından işlenmesini güvence altına uygulama güvenlik duvarıdır. Bireysel bir bilgisayar sisteminin IP adreslerinin internette doğrudan görünmesini sağlayabilen bir yönlendirici en yaygın donanım önlemidir. Şifreleme veya şifre çözme yazılımı, anti-virüs yazılımı, algoritmalar, biyometrik kimlik doğrulama sistemleri, casus yazılım algılama veya kaldırma güvenlik duvarları diğer geleneksel karşı önlemler arasında yer almaktadır (Buch, Ganda vd., 2017: 18).

Siber güvenliğin avantajları ve dezavantajları ise şu şekilde ifade edilmektedir (Buch vd., 2017: 21):

Siber güvenliğin avantajları

- Siber uzayın gelişmiş güvenliği
- Siber savunmada artış
- Siber hızda artış
- Şirket bilgilerini ve verilerini koruma
- Bilgisayarları ve sistemleri solucanlara, virüslere, casus yazılımlara ve kötü amaçlı yazılımlara karşı korur
- Kişisel özel bilgileri korur

- Kaynakları ve ağları korur
- Kimlik hırsızlığına ve bilgisayar korsanlarına karşı mücadele
- Bilgisayarın çökmesini ve donmasını en aza indirir
- Kullanıcılara gizlilik sağlar.

Siber güvenliğin dezavantajları

- Ortalama kullanıcılar için maliyetli olacaktır
- Güvenlik duvarlarını doğru şekilde yapılandırmak zor olabilir
- Güvenliği güncel tutmak için yeni yazılımı sürekli güncellemeniz gerekir.
- Sistemi eskisinden daha yavaş hale getirir.
- Yanlış yapılandırılmış güvenlik duvarları, güvenlik duvarı doğru şekilde yapılandırılana kadar kullanıcıların İnternet'te belirli eylemleri gerçekleştirmesini engelleyebilir.

Siponen (2001: 28), özellikle internet ortamında herhangi bir hizmetle veya BT ilgilenen tüm kullanıcıların en azından bir miktar siber güvenlik farkındalığına sahip olması gerekliliğini belirtmektedir. Hem kuruluşların içindeki hem de dışındaki kullanıcıların siber güvenlik konusunda bilinçli olması gerekmektedir. Yazılımsal ve donanımsal güvenlik sistemlerini içeren sanal dünyayı; siber ortama açık olan değerli bilgi ve sistem varlıklarının korunması amacıyla uygulanan risk yönetim faaliyetleri, eğitimler, kılavuzlar ve politikalar, kapsamaktadır. Bilgi, sayısallaştırılarak dijital ortama aktarılması sonucu üzerinde tutulduğu fiziksel ortamdan bağımsız hale gelmiştir. Ağ sistemleri üzerinden farklı alanlardaki veri sunucularına birden fazla kopya oluşturularak saniyeler içerisinde iletilmektedir. Siber güvenlik açıkları, bireysel, kurumsal ve ülkesel çapta telafisi mümkün olmayan kayıplara sebep olabilmektedir. Bu nedenle siber güvenlik önlemlerinin kamusal, askeri ve özel işletmeler başta olmak üzere ilgili tüm kritik bilgi ve altyapı sistemlerinde geliştirilmesi gerekmektedir (Şahinaslan, 2013: 3).

2.1.4. Siber Güvenlik Kavramları

Siber güvenlik kavramını daha iyi anlayabilmek için siber varlık, siber olay, siber uzay, siber zorbalık, siber savaş, siber casusluk, siber silah, siber terörizm, siber tehdit kavramları açıklanmıştır.

2.1.4.1. Siber Varlık

Siber uzay adı verilen yeni bir alan geleneksel alanlara ek olarak ortaya çıkmış ve hızla genişlemeye devam etmektedir. Bu bağlamda, "siber varlıklar" siber uzayda işlev gören dijital varlıklar olarak belirtilmektedir. Siber uzayda dijital olarak varlık gösteren ya tamamen bilgisayarlar tarafından sentezlenen tüm varlıklar siber varlıklardır. Siber varlıklar düşünsel, sosyal ve fiziksel alanlarla yakın bir ilişki içinde olan, hatta bu alanlarla entegrasyona sahip olan her türlü varlık olarak kapsamlı bir şekilde de tanımlanmaktadır (Dhelim vd., 2020: 5).

Siber ortamlarda bulunan; bilgiler, veriler, işlemler, araçlar, planlar, dokümanlar ve dokümante edilmiş düşünceler siber varlıkları kapsamaktadır. Siber varlıklar bir bilgisayar, ağ veya sunucu cihazı olabileceği gibi ulusal, kurumsal veya kişisel veriler de olabilmektedir. Siber ortamdaki varlıkları internete bağlı; cihaz, sistem, televizyon veya araç olabileceği gibi veri merkezi, veri kayıt sistemi, veri tabanı veya kullanılan yazılımlar, donanımlar ve süreçler oluşturmaktadır (Sağıroğlu ve Alkan, 2018: 24).

Fiziksel ve mantıksal siber varlıklar olmak üzere siber varlıklar iki kategoride sınıflandırmaktadır (Öztunç, 2022: 13);

1. Fiziksel Siber Varlıklar: Fiziksel bir kütlesi olan, çevre faktörlerinden etkilenme olasılığı olan, fiziksel olarak taşınabilen, fiziksel güvenlik önlemleri ile korunması gereken, fiziksel etkilere (hırsızlık, elektrik kesintisi, nem, yangın) maruz kalabilen varlıklar anlaşılmalıdır.

2. Mantıksal Siber Varlıklar: Bu varlıkların meydana gelmesinde rol oynayan bilgisayar kodları ve süreçleridir. Fiziksel siber varlıklar aracılığı ile işlenen bilgi, veri ve yapılandırma ayarları da mantıksal siber varlıklar olarak isimlendirilebilir.

2.1.4.2. Siber Olay

Türkiye'de siber olay anlayışı Ulusal Siber Güvenlik Stratejisi ve Eylem Planında (2020–2023); "*Bilişim ve endüstriyel kontrol sistemlerinin veya bu sistemler tarafından işlenen bilginin/verinin gizliliği, bütünlüğü veya erişilebilirliğinin ihlal edilmesi*" olarak tanımlanmaktadır. Siber olaylar; bilişim sistemlerine ve bu sistemlerin, bütünlüğüne, işleyişine ve işlevselliklerine yapılan saldırılar olarak tanımlanabilmektedir (Gençoğlu ve Sert, 2021: 472). Fiziksel veya mantıksal siber varlıklar, çeşitli şekillerde paydaş olduğu bir olayı ifade etmek için kullanılmaktadır. Endüstriyel ve bilgi kontrol sistemleri tarafından işlenen bilgi ve veri erişilebilirliğinin, bütünlüğünün veya gizliliğinin ihlali veya ihlal teşebbüsüne de siber olaylar olarak nitelendirilmektedir (Terlizzi vd., 2017, s.229).

Siber olaylara müdahale süreci ise aşağıdaki gibi gerçekleşir (Gençoğlu ve Sert, 2021: 472):

- **Siber Olayın Tespiti:** Tanı Konması.
- **Olayın Risk Tanımlanmasının Yapılması:** Çalışan sistemler ve Bilgi İfşası.
- **Siber Olay Müdahale Ekibine Bildirim Yapılması:** İlk bildirimin kurumsal Siber Olaylara Müdahale Ekibine (SOME) daha sonra Ulusal Siber Olay Müdahale Merkezine (USOM) bildirilmesi.
- **Siber Olaya Müdahale**
- **Teknik Analiz Saldırgan IP Tespiti:** Sistem log kayıtlarının örneklerinin alınması, vaka öncesi kayıtlar ile karşılaştırılması. Meydana gelen siber olay ile ilgili kanıt ve delillerin toplanması.
- **Önlem Alma:** Tespit edilen IP'lere karşı engelleme işlemi yapılması.

2.1.4.3. Siber Uzay

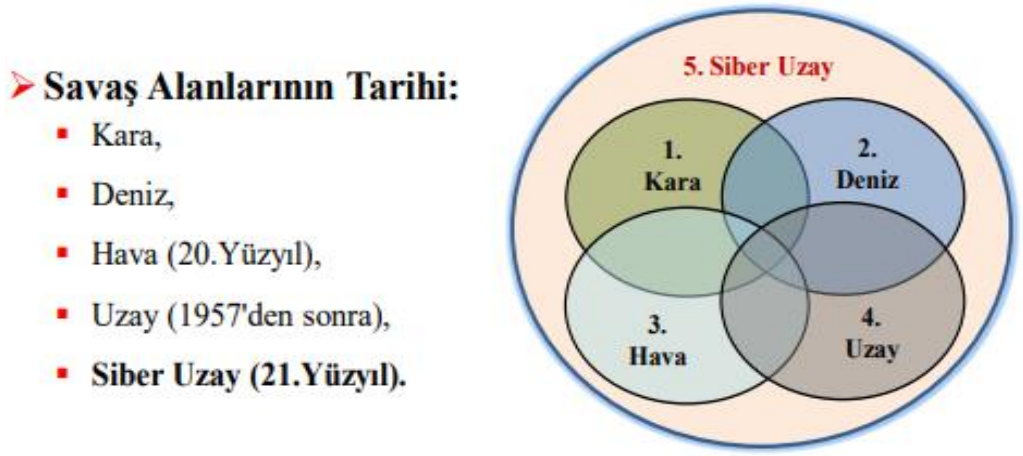
Amerikalı yazar William Gibson tarafından ilk olarak 1982'de yazılan "Burning Chrome" adlı kısa öyküde siber uzay ifadesi kullanılmıştır. Daha sonra yazar tekrar olarak 1984 tarihli "Neuromancer" adlı romanında siber uzay ifadesi işlenmiştir. Siber uzay kelimesi sonraki birkaç yıl içinde, çevrimiçi bilgisayar sistemleriyle belirgin bir şekilde ilişkilendirilmiştir (Seviş ve Seker, 2016: 1). Geçen yıllar boyunca

siber uzay kavramı birçok şekilde tanımlanmıştır. Yaygın olarak kabul gören tanıma göre siber uzay, "*bilgisayar ağları ve bu ağların barındırdığı hizmetler ile bilgilerden oluşan sanal dünyanın ortak adı*" olarak tanımlanmıştır (Haig, 2021: 93). Başka bir tanıma göre ise siber uzay, "*bilgisayar sistemleri tarafından yaratılan fiziksel olmayan alanı tanımlamak için kullanılan bir metafordur*" (Ottis ve Lorents, 2010: 268). Türkiye Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023); siber uzayı "*Doğrudan ya da dolaylı olarak internete, elektronik haberleşme ve bilgisayar ağlarına bağlı olan tüm sistem ve hizmetler*" olarak tanımlamaktadır.

David Clark'ın (2010: 1-4) siber uzay modellemesinde dört katman bulunmaktadır. Bu katmanlar sırasıyla; Fiziksel iletişim altyapı katmanı, mantıksal katman, bilgi katmanı ve kullanıcıların bulunduğu katmandır. Siber uzayın temeli siber uzayın fiziksel katmanıdır. Ayrıca, siber uzayın inşa edildiği fiziksel cihazlarda fiziksel katmandır. Siber uzay aynı zamanda, birbirine bağlı bilgi işlem cihazlarının bir alanıdır. Bu sebeple temelleri; internet ve diğer ağlar ve iletişim kanalları, süper bilgisayarlar ve şebekeler, PC'ler ve sunucular, sensörler ve dönüştürücülerdir. Bilgi işlem ve depolama cihazlarının; radyo iletimi yoluyla, iletişimler, kablolar veya fiberler üzerinden bir yerden bir yere fiziksel olarak taşınmasıyla yapılabilmektedir. Fiziksel katman belki de kavranması en kolay olanıdır. Çünkü fizikselliği ona sağlam bir konum duygusu verdiğinden elle tutulabilmektedir. Yeni mantıksal yapıların yaratılması ve birleştirilmesi siber uzayın doğasında vardır. Bu da fiziksel temellerin üzerinde çalışan yeni yeteneklerin ve hizmetlerin sürekli ve hızlı evrimiyle mümkündür. Bu nedenle, ikinci katmanda yer alan mantıksal katman, her birinde yeni yeteneklerin inşa edildiği ve bu yeteneklerin de bir sonraki yenilik için bir platform haline geldiği bir dizi platformu oluşturmaktadır. Üçüncü katmanda yer alan bilgi katmanı ise, siber ortamda iletilen, dönüştürülen ve saklanan bilgileri ifade etmektedir. Sonuncu katman olan kullanıcılar katmanı yer almaktadır. Bu katman; siber alana katılan, faaliyette bulunan, iletişim kuran, kararlar alıp planlar yapan, bilgi alışverişinde bulunan, hizmet ve yetenekleriyle siber alanın kendisini dönüştüren bireyleri tanımlamaktadır.

Siber uzay küresel bir sanal sistem içinde; bütün bilgi kaynaklarını, veri sistemlerini ve ağları bir araya getirmektedir. Bu açıdan bakıldığında insanoğlunun

varoluşundan başlayarak zaman içerisinde kara, hava, deniz ve uzay gibi kendine has gereklilikleri ve özellikleri bulunan dört savaş alanı olmuştur. Bu alanları da içerisine 21'inci yüzyıla gelindiğinde 5'inci harekât alanı olarak ifade edilmeye başlanan "Siber Uzay" da eklenmiştir (Şekil 2.4).



Şekil 2.4. Savaş (Harekât) Alanları
Kaynak: (Şenol, 2020: 18)

Siber uzay faydalar ve fırsatlar ile birlikte, risklerin ve tehditlerin de yer aldığı bir alan olarak bilinmektedir. Bu durum şirketlerin, grupların, bireylerin ve hatta devletlerin de güvenliğe siber uzaya karşı bakış açılarını değişime uğratmıştır. Temelde siber güvenliğin sağlanması siber uzayın korunması ile mümkün olmaktadır (Çokbildik, 2017: 153).

2.1.4.4. Siber Zorbalık

İnternet kullanımı günümüz toplumunda oldukça yaygın bir hale gelmiştir. Bunun bir sonucu olarak da sosyal medya araçları üzerinden insanlar birbirleri ile iletişim kurmaya başlamıştır. Son yıllarda özellikle çocuklar ve ergenlerde telefon, tablet ve bilgisayar kullanımı giderek artmaktadır. Şiddetin fiziksel dünyadan sanal ortama taşınmasına iletişime bağlı teknolojilerinin kötü niyetli ve hatalı kullanımı neden olmuştur. Bu da "Siber Zorbalık" adı verilen yeni bir kavramın doğurmuştur (Kestel ve Akbıyık, 2016: 845). Çeşitli araştırmacılar tarafından; internet zorbalık,

sanal zorbalık, dijital zorbalık, siber zorbalık, elektronik zorbalık, çevrimiçi zorbalık ve çevrimiçi zarar verme gibi kavramlarla tanımlanmaktadır (Aktepe, 2013: 32).

Bill Belsey tarafından 2003 yılında siber zorbalığın bilinen ilk tanımı yapılmıştır. Belsey, siber zorbalığı "*bir birey veya grup tarafından başkalarına zarar vermeyi amaçlayan, kasıtlı, tekrarlanan ve düşmanca davranışları desteklemek için bilgi ve iletişim teknolojilerinin kullanılması*" olarak adlandırmıştır (Tanrıkulu, 2015: 24). Birçok araştırmacı tarafından Belsey' in siber zorbalık kavramını ortaya atmasıyla kavram ele alınmış ve tanımlanmaya çalışılmıştır. Ybarra ve Mitchell (2004: 1308) siber zorbalık kavramı yerine "*internet tacizi*" kavramı kullanılmış ve bu kavram bireye yönelik çevrimiçi ortamda aleni olarak gerçekleşen eylemler olarak adlandırılmıştır.

Shariff ve Gouin (2005: 28), siber zorbalığı "*elektronik ortamlar aracılığıyla iletilen gizli, psikolojik zorbalık olarak"* tanımlamaktadır. (Smith vd., 2008: 376), Siber zorbalığın en yaygın kullanılan tanımına göre, "*siber zorbalık, iki veya daha fazla kişi arasında elektronik yollarla gerçekleştirilen, kasıtlı, tekrarlayan ve güç dengesizliği içeren saldırgan bir davranıştır*" Hinduja ve Patchin (2012: 88) siber zorbalığı kısaca "*bilgisayarlar, cep telefonları ve diğer elektronik cihazlar aracılığıyla kasıtlı ve sürekli biçimde gerçekleştirilen zarar verici eylemler*" olarak adlandırmıştır.

Siber zorbalık ifadesi yukarıdaki tanımlardan yola çıkılarak, internetin yanı sıra cep telefonları ve bilgisayar gibi elektronik cihazlar aracılığıyla gerçekleştirilen, bir bireye veya bir gruba yönelik olumsuz davranışlar olarak adlandırabilir. Bu tür davranışlara en çok; e-posta gönderme, arama yapma, mesaj gönderme, küçük düşürücü fotoğraf veya video paylaşma gibi eylemler gösterilebilir. Genellikle birini üzmek veya ona zarar vermek amacıyla kasıtlı ve tekrarlayan bir şekilde uygulanan; hakaret, küfür, tehdit veya taciz içeren kötü niyetli davranışları siber zorbalık kapsamaktadır. Siber zorbalık kavramına ilişkin farklı tanımlar literatürde bulunmaktadır. Ayrıca, farklı ölçütler temel alınarak siber zorbalık türlerinin de kategorilere ayrılmaya çalışıldığı görülmektedir. Zorbalık davranışlarının ölçüt olarak alınmasıyla siber zorbalık aşağıdaki türlere ayrılmaktadır (Willard, 2007: 5-11):

Parlama (Flaming): İki veya daha fazla birey arasında gerçekleşen kısa süreli ve hararetli bir tartışmadır. Genellikle parlama; kaba dil, kırıcı, hakaret, saldırgan ve bazen de tehditler içermektedir.

Taciz (Harassment): Bireysel bir hedefe tekrarlanan, sürekli olarak saldırgan mesajlar gönderilmesidir. Genellikle bu şekilde taciz mesajları; kısa mesaj, e-posta veya anlık mesajlaşma gibi kişisel iletişim kanalları aracılığıyla gönderilmektedir. Parlama türünden taciz türü sürekli olma ve zarar verme amacı taşıma yönüyle ayrılmaktadır.

Karalama (Denigration): Belirlenen bir hedef hakkında gerçek dışı, zalimce ve zararlı sözler paylaşılmasıdır. Bu zararlı sözler çevrimiçi olarak yayınlanabilir veya başkalarına gönderilebilir. Bu eylemleri göndermenin, yayınlanmanın amacı arkadaşlıklara müdahale etmek veya itibarını zedelemektir.

Başkasının kimliğine bürünme (Impersonation): Belirli bir hedefi kötü yansıtan, hedefin arkadaşlıklarını etkileyen içerikler paylaşan veya hedefin taklitlini kapsamaktadır. Hedefin kişisel profilinde, blogunda, Web sayfasında veya herhangi bir iletişim biçimi aracılığıyla bu eylemler yapılmaktadır.

İfşa ve Düzenbazlık (Outing and Trickery): İfşa, Bir bireye ait gizli sırların, özel görüntülerin, özel bilgilerin herkesin erişimine açılması veya başkalarına iletilmesi ifşa anlamına gelir. Özellikle bu durum, utandırıcı ve mahrem nitelikteki içerikler için geçerlidir. İfşanın bir uzantısı olarak Siber zorbalık da ortaya çıkabilir. Bir siber zorba, hedefini özel ve samimi bir iletişim ortamında olduğuna inandırarak, onun sırlarını öğrenebilir; bu bilgileri başkalarıyla paylaşabilir veya paylaşmakla tehdit edebilir.

Dışlama (Exclusion): Kasıtlı olarak birini internet ortamındaki gruptan çıkarmak veya bir gruba kabul etmemek söz konusu kişinin grup dışına itilmesi anlamına gelir. Bu durum, grubun dinamikleri içinde yer alan bir bireyin, belirli bir nedenle dışlanması olarak tanımlanabilir.

Israrlı Siber Takip (Cyberstalking): Hedef alınan bir kişiye zarar verme tehdidi içeren, son derece rahatsız edici, korkutucu ve saldırgan mesajların sürekli olarak iletilmesidir.

2.1.4.5. Siber Savaş

Ulus ya da devlet içerisindeki düşmanlar arasında meydana gelen, açıkça ilan edilmiş silahlı çatışmaları tanımlamak için savaş kavramı kullanılmaktadır. Rakip devletlerin siber ortamdaki siber saldırılarını ise siber savaşlar ifade etmektedir (Sandilaç, 2022: 180). Siber alana ilişkin mücadeleler için geniş ölçekli bir ifade olarak siber savaş kavramı kullanılmaktadır. Daha önce değinildiği gibi siber Savaş insanlığın kara, deniz, hava, uzaydan sonra 5. savaş alanı olarak kabul edilmektedir. Bazı kaynaklarda 5. boyut savaşlar olarak da tabir edilmektedir (Bayrak, 2020:28).

İngilizce karşılığı olan "cyberwar" olan siber savaşın, bazı sözlüklerde de "information war" teriminin yani "bilgi savaşı"nın eş anlamlısı olarak kullanılmaktadır ve "*elektronik iletişim ve internetin bir ülkenin iletişim sistemi, güç kaynakları, ulaşım sistemi ve benzeri sitemlerini bozması veya çökertmesi*" olarak tanımlanmaktadır (Sandilaç, 2022: 182). Başka bir tanıma göre, "*Siber savaş, devlet aktörleri (veya önemli bir devlet yönlendirmesi veya desteği alan devlet dışı aktörler) tarafından siber alanda gerçekleştirilen ve başka bir devletin güvenliğine yönelik ciddi bir tehdit oluşturan eylemlerle politikanın bir uzantısıdır veya bir devletin güvenliğine yönelik ciddi bir tehdide (gerçek veya algılanan) yanıt olarak gerçekleştirilen aynı nitelikteki bir eylem*" olarak tanımlanmaktadır (Stiennon, 2015: 8).

Siber savaşa genel anlamda, hedef seçilen ülke ve ülkelere yönelik askeri, politik ve ticari amaçlı örgüt, kurum, şirket ve bireylerden iletişim altyapılarına ve bilgi sistemlerine yapılan planlı ve koordineli saldırılara denilebilir (Güngör ve Güney, 2017: 139). Casusluk, manipülasyon, propaganda, iletişimin kontrol altına alınması, virüs ve Truva atlarıyla sistemlerin bozulması, siber bombalarla sabotaj, sistem kilitleme, dolandırıcılık, bilgi kirliliği gibi birçok alan siber savaşın oluşumuna katkı sağlamaktadır (Kara, 2013: 40**).**

2.1.4.6. Siber Casusluk

Günümüzde, internet ile günlük yaşamın iç içe geçtiği için internet üzerinden küçük ölçekli şirketlerin ve şahısların kullanıcı hesaplarının ve kimlik bilgilerinin ele geçirilmesi artık çok sık yaşanmaktadır (Yayla, 2014: 194). Bu kapsamda bir kişinin, organizasyonun, kurumun veya ülkenin hassas bilgilerini, siber ortamı araç olarak

kullanıp gizlice ele geçirmek siber casusluk olarak tanımlanmaktadır. Bu eylem, kolektif ya da bireysel olarak çıkar sağlamak veya parasal kazanç elde etmek için yapılmaktadır. Bir devlet tarafından organize olarak başka bir devlete zarar vermek amacıyla yapılan siber casusluk faaliyetleri siber savaşın nedeni olabileceği değerlendirilmektedir (Yayla,2013: 196).

Siber casusluk; siyasi, askeri ve ekonomik açıdan rakiplerine karşı daha önde olmak amacıyla bilişim sistemlerini yasaların izin vermediği şekilde kullanarak bir kuruluşa veya kişiye ait bilgilerin, sırların ele geçirilmesidir (Nickolov, 2008: 4).

Siber casusluk, önceleri kişisel maksatlar için yapılmıştır. Ancak zamanla bireysel çerçevesinden çıkmış askeri politik ve ekonomik avantaj sağlamak amacıyla devletler tarafından kullanılmaya başlanmıştır. Yasadışı faaliyet olarak yapılan siber casusluk rakip ülkenin bilgisayarlarına veya iletişim ağlarına yasal olmayan yollarla sızarak devlete ait gizli bilgilerin sızdırılması eylemi haline dönüşmeye başlamıştır. Bu da uluslararası aktörler açısından birimlerin ve kurumların oluşturulmasını gerekli kılmıştır. Oluşturulan birimler teknik içerikli önlemlerin yanında, casusluk faaliyetlerine ilişkin bir uzmanlaşmayı da beraberinde getirmiştir (Güntay, 2018: 89).

2.1.4.7. Siber Silah

Siber saldırı aracı olarak tercih edilen saldırı veya bir yazılımı aracını nitelendirmek için siber silah kavramı kullanılmaktadır. Ancak burada basit yapıda olan bir saldırı veya bir yazılım aracından değil de spesifik amaçları olan, gelişmiş tekniklerle üretilmiş ve karmaşık yapıya sahip bir saldırı yazılım aracından bahsedilmektedir (Çahmutoğlu, 2020: 7). Thomas Rid ve Peter McBurney'nin siber silah tanımını "*yapıları, sistemleri, canlı varlıkları tehdit etmek veya fiziksel, işlevsel veya zihinsel zarar vermek amacıyla kullanılan veya kullanılmak üzere tasarlanan bilgisayar kodu*" olarak tanımlamaktadır (Demircan, 2019: 8).

Üç ana başlık altında siber silahları toplamak mümkündür. Genel olarak bu silahlar sözdizimsel (syntactic), anlamsal (semantic) ve karışık (mixed) tipteki silahlar olarak adlandırılmaktadır (Brenner ve Goodman, 2002). Sözdizimsel silahlar DoS (Denial of Service) saldırılarını ve kötü niyetli yazılımları (Worms, Malicious Code, Trojan Horses ve Spyware) kullanarak bilgisayarların işletim sistemlerine zarar

verirler. Bilgisayarda karşımıza çıkan bilgilerin doğruluğunu değiştirerek bilgisayar kullanıcılarına kendini fark ettirmeden yanlış bilgi edinmelerini Anlamsal (semantic) siber silahlar sağlarlar. Hem sözdizimsel (syntactic) hem de anlamsal (semantic) silahların birlikte kullanılmasıyla karışık tipteki siber saldırı araçları oluşurlar. Bilgisayarın işletim sistemlerine zarar vermeğin yanı sıra, bu silahlar aynı zamanda bilgisayar kullanıcılarının elde ettiği bilgilerin doğruluğunu da değiştirirler. Bu nedenle karışık tipteki siber silahlar daha profesyonel saldırı aracı olarak tanımlanmaktadır (Gürkaynak ve İren, 2011: 270).

2.1.4.8. Siber Terörizm

Siber terörizm kavramının günümüzde çok sık kullanılmasına rağmen hangi tür eylemlerin dahil olacağı konusunda somut bir tanımlama bulunmamaktadır. İlk olarak 1980 yılında Güvenlik ve İstihbarat Enstitüsü (Institute for Security and Intelligence) araştırmacılarından Barry Collin tarafından siber terörizm kavramı kullanılmıştır. Siber terörizm, siber uzay ve terörizm terimlerinin birleştirilmesiyle yeni bir kavram olarak ortaya çıkmıştır (Yılmaz, 2020: 68). Ayrıca, siber terörizm, 21. yüzyılda iletişim ve bilgiye dayalı oluşumların kendi doğasına uygun olarak ortaya çıkardığı tehdit olarak tanımlanabilir. Bundan başka, Bilgi Toplumu, Bilgi Tabanlı Ekonomi, FTP tarzı örgütlenme, e-Devlet, Uluslararası Sivil Toplum Kuruluşları düzeni temsil ederken siber terörizm düzene yönelik tehdidi temsil etmektedir (Terzi, 2018: 89). Birçok araştırma siber terörizmi tanımlama üzerine yapılmıştır. Fakat uluslararası toplumun üzerinde uzlaştığı ortak bir siber terör tanımına ulaşılamamıştır. Kurumlara ve kişilere göz dağı vermek, siyasi ve sosyal mercilere, baskı oluşturmak amacıyla resmi kuruluşların bilgi ve veri tabanlarına, bilgisayarlarına ve network sistemlerine yapılan yasadışı tehdit ve zarar verici saldırılar siber terörizmi nitelendirmektedir. Saldırının siber terörizm olarak tanımlanması üzerinde durulması gereken önemli noktalardan biridir. Bir siber saldırının siber terörizm olarak tanımlanması için bireye ya da mala karşı şiddet içermesi veya en azından korku yaratacak kadar hasara yol açması gerekmektedir (Yılmaz, 2020: 70). Klasik anlamda terör eylemlerinin bilgisayar ve bilgisayar sistemleri kullanılarak icra edilmesi de siber terörizmi olarak tanımlanmaktadır. Denning'in makalelerinde yer alan siber terörizm tanımı da dikkate almaya değerdir (TASAM, 2004: 5):

"Siber terörizm, siber boşluk ve terörizmin bileşimidir. Siber terörizm, siyasi ve sosyal mercilere ve kişilere gözdağı vermek, baskı oluşturmak maksadıyla resmi birimlerin bilgisayarlarına, network sistemlerine, bilgi ve veri tabanlarına yapılan yasadışı tehdit ve zarar verici saldırılardır. Daha da ötesi, bir saldırının siber terörizm olarak tanımlanması için bireye ya da mala karşı şiddet içermesi gerekmektedir. En azından "korku yaratacak kadar hasara" yol açmalıdır. Siber terör ölümcül olan ya da fiziki hasara yol açan, şiddetli ekonomik kayba neden olan saldırılar olarak örneklenebilir. Kritik altyapı odaklarına yapılan ciddi saldırılar yarattığı etkiye göre siber terörizm olarak tanımlanabilir. Önemli olmayan servislere verilen rahatsızlıklar siber terörizm olarak tanımlanamaz."

Siber terörizmi Wiemann (2007: 220), "*enerji, ulaşım, ya da hükümet işlemleri gibi kritik ulusal altyapıları sabote etmek için bilgisayar ağlarının kullanımı"* olarak ifade etmektedir.

Siber terörizmi Lewis (2002: 1), "*kritik ulusal altyapıları (enerji, ulaşım, hükümet operasyonları gibi) kapatmak veya bir hükümeti veya sivil halkı zorlamak veya sindirmek için bilgisayar ağı araçlarının kullanılması*" olarak tanımlamaktadır.

Genel olarak toplarsak, aktörlerin ideolojik, siyasi ve sosyal hedeflerine ulaşmak için bilgisayar ve ilgili sistemleri yasadışı olarak kullanarak, bireylere ve mülklerine, ülkelerin kritik alt yapı sistemlerine yönelik zarar vermek amacıyla gerçekleştirilen şiddet veya şiddet kullanma tehdidi olarak siber terörizm kavramını tanımlayabiliriz.

Siber terörizmin harekât bulma süreci ve beslendiği nokta siber tehditlerle ilgilidir. Siber terörizmin kaynaklandığı noktalar bu kavrama dahildir. İnternete bağlanmayı sağlayan ve çevrimiçi saldırılara maruz kalmayı olanaklı kılan araçların oluşturduğu unsurlar siber tehditlerdir. Sanal ortamda siber tehdit yöntemleri ve ortaya çıkış süreci gerçekleşmesi maddi, manevi, fiziksel sonuçlar doğurmaktadır ve bu sonuçların geri dönüşü olmayabilir. Bu suçların etkileyici olmaları bireysel olmalarına, kurumsal bir etki oluşturmasına veya devlet gibi uluslararası aktörlere etki edişine göre farklılaşmaktadır. Sorunun küresel anlamda tartışılması da bu noktada başlamaktadır.

Devletler adına terörizmin takip edildiği boyut siber alana da taşmıştır ve bu durum ilgi uyandırmıştır (Güntay, 2017: 88).

2.1.4.9. Siber Tehdit

1990 yılında siber tehditler virüs olarak evrimleşmeye başlamıştır. Geçen on yılda solucan olarak büyüyerek; Gelişmiş Sürekli Tehdit, İçeriden Gelen Saldırı ve botnetler gibi tehditlere dönüştü. Modern teknolojinin getirdiği ilerleme nedeniyle şimdi tamamen yeni türde sorunlar ortaya çıkmıştır (Devi ve Mohankumar,2019: 2271)**.**

Bir veri iletişim yolu üzerinden yasa dışı yollarla bir bilgisayar ağına erişmeye yönelik kötü niyetli girişimler siber tehdit olarak tanımlanmaktadır. Bu tehditler; doğrudan veya dolaylı, kasıtlı veya kasıtsız, olabilir. Genellikle siber tehditler; virüs kodu yazarları, organize suç sendikaları, bilgisayar korsanları, endüstriyel casuslar, kinci davetsiz misafirler ve intikamcı çalışanlar tarafından yapılmaktadır (Almarabeh ve Sulieman, 2019: 1). Kötü niyetli saldırı olarak da siber tehdit tanımlanır. Siber tehditlerin amacı kişisel sistemlerin veya bir organizasyonun bütünlüğünü bozmak için siber-fiziksel bir sistemdeki güvenlik zayıflıklarını bularak sistem işleyişine zarar vermek veya onu devre dışı bırakmaktır (Singh ve Jain, 2018: 688).

Artık sadece siber tehditler bilgisayar sistemlerine verdikleri zararlar (sistemlerden bilgi çalma, sistemlere sızma ve sistemlere asılsız bilgi koyma) ile sınırlı kalmamaktadır. Bir ülkenin kritik olarak kabul edilebilecek askeri komuta ve kontrol sistemlerine, enerji ve ulaşım ağlarına, haberleşme sistemlerine ve bilgisayar sistemlerine zarar verecek ölçüde, asimetrik bir harp çeşidi olarak ortaya çıkmaktadır. Bu nedenle tüm dünya tarafından önümüzdeki yıllarda siber tehditlerin da önemli tehditlerden biri olacağı düşüncesi kabul edilmeye başlanmıştır. Bu kapsamda, gelecekte karşılaşılabileceğimiz tehditleri tahayyül edebilmek açısından geçmiş yıllarda yaşanan ulusal çaplı siber güvenlik olaylarının incelenmesi fayda sağlayacaktır (Aslay, 2017: 25).

Siber tehditler, siber ortamda bulunan verinin erişilebilirliğine, gizliliğine ve bütünlüğüne yönelik istenmeyen durumlara yol açabilme yeteneği sayesinde siber ortamdaki güvenlik açıklıklarını kullanma potansiyeline de sahip olabilmektedirler.

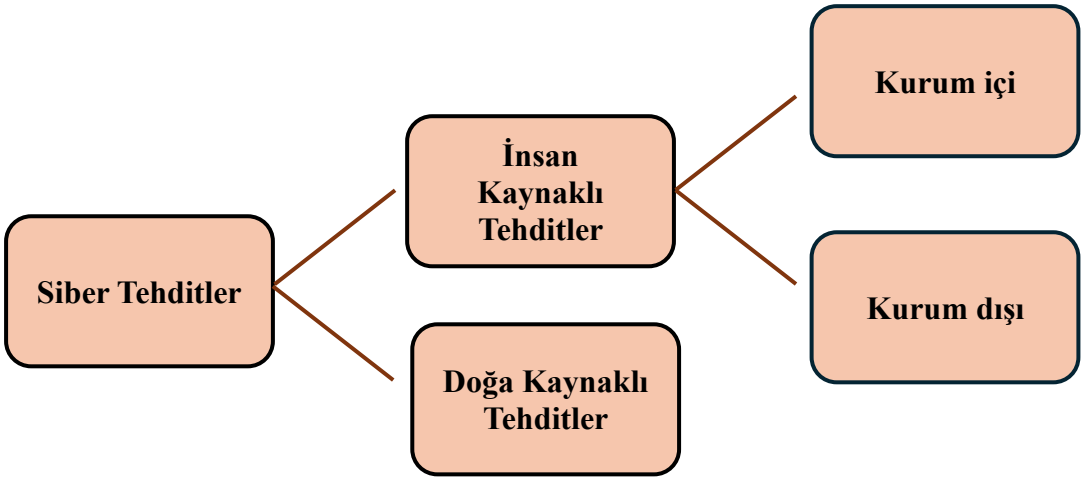
Kurumsal siber güvenliğe yönelik tehditleri "insan kaynaklı siber tehditler" ve "doğa kaynaklı siber tehditler" olarak iki ana kategoride incelmektedir (Yaşar ve Çakır, 2015: 491).

İnsan kaynaklı tehditler:

(1) Kurum içi: Casuslar, sistem yöneticisi hataları, art niyetli personel davranışları, eğitimsiz ve bilinçsiz kullanıcılar vb…

(2) Kurum dışı: Hırsızlık, casusluk, internet ortamından gelen tehditler ile yetkisiz ve izinsiz erişim vb. faaliyetler…

Doğa kaynaklı tehditler: Deprem, yangın, sel vb…



Şekil 2.5. Siber Tehditlerin Sınıflandırılması
Kaynak: (Yaşar ve Çakır, 2015: 492).

2.1.5. Siber Tehdit Yöntem ve Çeşitleri

Günümüzde bilişim teknolojilerinin hızla geliştiği için iletişim ve bilgisayar teknolojilerinin sunduğu olanaklardan en verimli şekilde yararlanabilmek için siber güvenliğin önemi giderek daha fazla anlaşılmaktadır. Bu nedenle, siber savunma ve güvenliğin daha etkin bir şekilde sağlanabilmesi için sürekli olarak araştırmalar yapılmaktadır. Siber güvenliğin sağlanması ve siber suçların önlenmesi için siber tehditlerin doğru bir şekilde tespit edilmesi ve tanımlanması çok büyük önem

taşımaktadır. Bu bölümde yaygın olarak kullanılan siber saldırı yöntemleri incelenmiştir.

2.1.5.1. Kötü Amaçlı Yazılımlar (Malware)

Saldırganlar tarafından özel bilgisayar sistemlerine erişim sağlama, hassas bilgileri toplamak ve bilgisayar işlemlerini bozmak için oluşturulan ve kullanılan yazılımlar, kötü niyetli (veya zararlı) yazılım ya da kötü amaçlı yazılım olarak tanımlanmaktadır. Ayrıca müdahaleci veya düşmanca yazılım çeşitli yazılım biçimlerini ifade etmek için kötü amaçlı yazılım genel bir terim olarak kullanılmaktadır (Miloševic, 2013: 1). Kötü amaçlı yazılımlar tarafından ağların gelişimi engellenir. Genellikle internet üzerinden çalıştırılan uygulamaları kötü amaçlı yazılımlar hedef alır. Günümüzde internet yaşamın hemen hemen her alanında hizmet kalitesini artırmak için kullandığından, bu kötü amaçlı yazılımların yarattığı olumsuz sonuçlardan kaçınılabilmesi için mümkün olduğunca erken tespit etme ve devre dışı bırakma ihtiyacı artmaktadır. (Tahir, 2018: 20). Kötü amaçlı yazılımlar; solucanlar, virüsler, casus yazılımlar, kök yazılımlar, reklam yazılımları ve Truva atları gibi çeşitli kategorilere ayrılmaktadır (Bazrafshan vd., 2013: 113). Aşağıda bu yazılımların kısaca tanımlamaları yapılmıştır.

Virüs: Bilgisayar virüsü veri ve yazılıma müdahale eden, kendi kendini kopyalayan ve bilgisayardan bilgisayara yayılan bir bilgisayar programıdır (Akinde vd., 2021: 51). Bilgisayar virüslerinin kısaltması olan virüsler, tartışmasız bilinen en eski kötü amaçlı yazılım türüdür. (Ngo vd., 2020: 798). Bazı virüsler sadece can sıkıcıdır. Ancak diğerleri ciddi hasara neden olabilir. Virüs yükünün içeriği, zararsızdan ölümcüle kadar her şey olabilen enfeksiyonun hedefi için koddur. Virüsler dosyaları önemli bilgileri çalabilir, değiştirebilir, silebilir, belgeleri elektronik posta (e-posta) yoluyla gönderebilir, istenmeyen uygulamaları yükleyebilir, çalıştırabilir ve hatta bir makinenin işletim sistemini (OS) çökertebilir. Çok sayıda virüs, yükün yürütülmesini tetikleyen bir koşul olan bir tetikleyiciye sahiptir. Bu tetikleyici çoğunlukla kullanıcının veya istemcinin etkileşimini içerir (örneğin, bir program veya yazılımı çalıştırma, bir belgeyi açma, bir e-posta ekine dokunma) (Akinde vd., 2021: 51).

Bulaşıcı mikroorganizmalar gibi bilgisayar virüs programları da oldukça küçüktür. Yalnızca birkaç satır program kodu kullanılarak temel bir virüs, yazılabilir. Bir virüs geliştirildikten sonra, enfekte diskler aracılığıyla dağıtılmış sistemler ya da telefon hatları üzerinden diğer bilgisayarlara aktarılabilir veya iletilebilir. Bilgisayar virüsleri mikrosaniyeler içinde çoğalabilir ve milyonlarca kilometre uzaklıktaki en büyük sistemlere zarar verebilir (Akinde vd., 2021: 51).

Solucanlar: Genellikle solucan ve virüs terimleri birbirinin yerine kullanılır. Fakat iki program türü arasında belirgin farklar vardır. Diğer bilgisayar sistemlerine girmek için bilgisayar kullanıcısından herhangi bir eylem gerektirmemesi bakımından solucanlar virüslerden farklanır. Başka bir deyişle, bir dosyaya bağlanmadan solucanlar bir bilgisayardan diğerine yayılabilir. Ayrıca, solucanlar virüslerden farklıdır. Çünkü virüslerden farklı olarak solucanlar bilgisayar sistemlerine ya da ağlarına girdikten sonra kendi başlarına hayatta kalabilir ve enfekte olmuş sistemlerde ve ağlarda çoğalırlar. Yukarıdaki ayrımlar göz önüne alındığında, solucanlar virüslerden daha büyük bir tehdit oluşturulabilmektedir (Ngo, 2020: 799).

Truva atları: Yararlı bir program gibi davranan Truva Atının, zararlı bir amacı vardır. Kendilerini çoğaltmayan bu programlar indirme gibi internet etkileşimiyle bir bilgisayara aktarılırlar. Kullanıcıların etkinliğini gözlemler, bulunduğu sistemdeki dosyaları ve özel bilgileri değiştirebilir, bozabilir, silebilir, ya da çalabilir (Idika ve Mathur, 2007: 5).

Reklam Yazılımları: Kötü amaçlı yazılım yüklendikten veya uygulama kullanıldıktan sonra otomatik olarak bilgisayara reklam oynatır, görüntüler veya indirir. Genellikle bu kod parçası özgür yazılıma gömülür. Birçok geliştiricinin internet kullanıcılarının etkinliklerini izleyerek reklam destekli yazılımları kötüye kullanması burada sorun oluşturmaktadır (Vinod vd., 2009: 74). Çoğu zaman reklam yazılımları oldukça can sıkıcıdır. Çünkü kullanıcının bilgisayarında kullanıcının izni olmadan reklam oynatır ve mevcut aktivitesini kesintiye uğratır. Reklam yazılımlarının temel amacı maddi çıkar elde etmektir. Diğer kötü amaçlı yazılımlar kadar zararlıdır (Tahir, 2018: 21).

Casus Yazılımları: Kişisel bir bilgisayara gizlice yüklenen ve kullanıcının izni olmadan bilgisayarla ne yaptığını kontrol eden ve kaydeden bir bilgisayar programıdır. Kök programları; bilgisayar korsanlarının kötü amaçlı şeyler yapmasına olanak sağlamak için işletim sisteminin bileşenlerinin etkisiyle ayarlanan programlardır. Bazen işletim sistemi çekirdeğini de etkilerler (Bazrafshan vd., 2013: 113). Saldırganlar, hassas verileri (örneğin, kullanıcı hesap bilgileri, oturum açma bilgileri) ve tuş vuruşlarını toplamak ya da kullanıcı etkinliklerini izlemek için casus yazılım kullanabilir (Ye vd., 2017: 4).

2.1.5.2. Oltalama (Phishing)

İnternet dünyasında kullanılan en yaygın ve tehlike oranı en yüksek olan saldırılandan birisi oltalama saldırılarıdır. İngilizce balık tutma ‘fishing’ anlamına gelen sözcükten esinlenerek türetilen bu kelime oltanın atılmasıyla en azından bir balığı avlayabileceğimiz düşüncesinden yola çıkılarak oluşturulmuştur (Turhan, 2006: 57). Oltalama (Phishing), saldırganlar tarafından internet kullanıcıların gizliliğini ihlal etmek amacıyla kullanılan ilk saldırı taktiği olarak tercih edilmektedir (Arshad vd., 2021: 163).

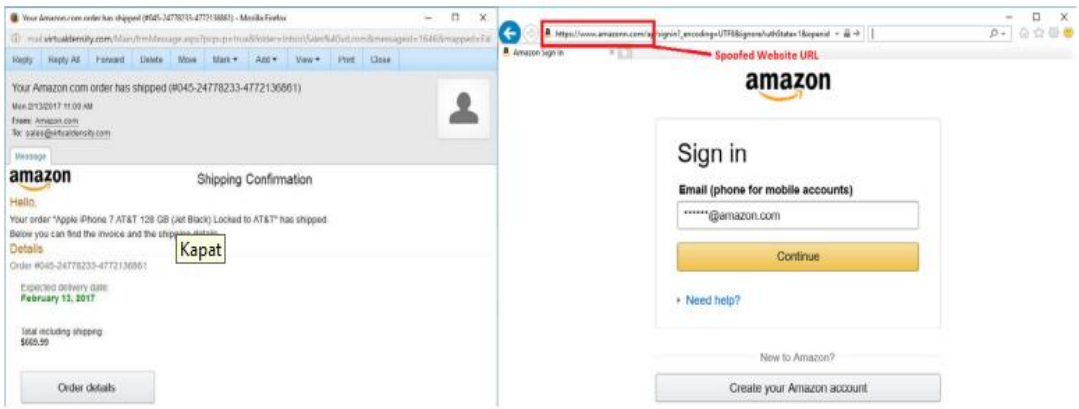
Oltalama veya kimlik avı saldırısı, internet kullanıcısının hassas verilerini ele geçirmek için çoğunlukla gerçek sistem kimliği görünümü alarak sahte e-mail, web reklamı, mesaj ve web sitesi şeklinde uyarlanan içeriğin hedefteki internet kullanıcısının kişisel e-mail adresine yollanan link gönderilmesiyle gerçekleşmektedir (Yalçın ve Avşar, 2018: 79).

Oltalama taktiğini kullanan saldırganlar, hedefin kişisel bilgilerini çalmak için birçok tarayıcıda varolan otonom doldurma işlevini kullanabilmektedir. Otomatik doldurma, bir sistem kullanıcısının kullanıcı ile ilgili depolanan verilere dayanarak web sitesindeki bir formu seri bir şekilde otomatik olarak doldurmasına imkân sağlayan bir işleve sahiptir. Oltalama saldırganları, sistem kullanıcısından ad ve e-mail gibi görünüşte basit ve sınırlı bilgiler isteyen sahte bir form tasarlayabilmektedirler. Fakat saldırganlar hedefteki kurban tarafından farkına varılamayacak form alanları ekleyebilmektedirler. Otomatik doldurma işlevi kullanıcı tarafından devreye sokulduğunda saldırganlar tarafından gizlenen bu form alanları otomatik olarak

doldurulmaktadır. Böylece hedefteki kurbanın iletişim bilgileri, adresi, şifresi vb. gibi önemli kişisel bilgileri oltalama saldırganının eline geçmekte ve kullanıcı bu durumun farkına varamamaktadır (Chiew, 2018: 5).

Oltalama saldırıları, görünüşte meşru olan bir e-mail oluşturarak içerisinde sahte bağlantılar veya kötü amaçlı içerik indirmeye yönelik tuzaklardan oluşmaktadır (Pajunen, 2017; 21). Oltalama da gönderilen içerik hükümetten, bankadan veya büyük şirketten çalışanın bilgilerinin teyit edilmesi amacıyla gelebilmektedir. Bu kurgulanmış siteler ve senaryolar gerçeğinden ayırt edilmeyecek şekilde tasarlanmakta ve tüm yasal haklara sahipmiş izlenimi vermektedir. Bazen son kullanıcıdan hesabın doğrulanması için giriş bilgilerini istemekte ve özenle hazırlanmış bir sayfaya yönlendirmektedir (Yalçın ve Avşar, 2018: 79).

İnternet kullanıcısı farkında olmadan bu bağlantılara tıklarsa, saldırgan kullanıcının sahte web sitesine girdiği bütün verilere ulaşmış olmaktadır. Bu e-postalar kusursuz derecede aldatıcı özellikte olabilmekte ve tecrübe sahibi kullanıcılar bile kandırılabilmektedir (Pajunen, 2017; 21). Şekil 2.6' de bu e-posta saldırısına yönelik örnek yer almaktadır. E-posta içerisinde yer alan bağlantı aslında gerçeği yansıtmayan düzmece bağlantı olup tıklandığı anda açılan web sayfası ile karşılaşılmaktadır. Bu web sayfası gerçeği ile birebir tasarlanmış biçimde görülmektedir. URL adresine dikkatle bakıldığında farklılıklar görülse de bu sayfa tecrübesiz kullanıcıyı yanıltıcı bir tuzak oluşturmaktadır.

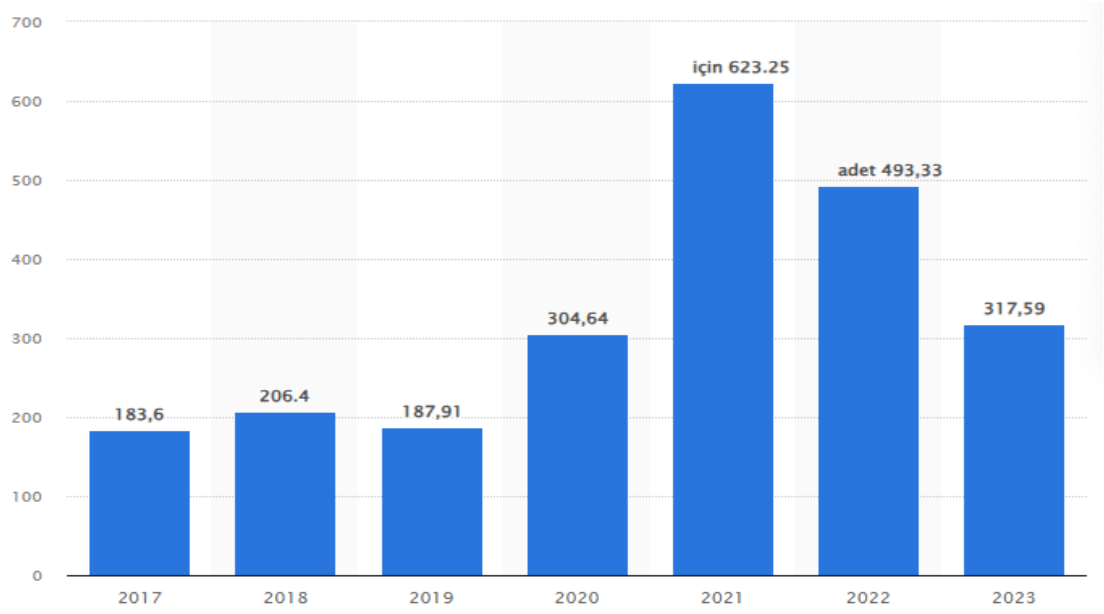


Şekil 2.6. Oltalama Saldırısında kullanılan e-posta ve web sayfası örneği
Kaynak: (Sahingoz vd., 2019: 346).

2.1.5.3 Fidye Yazılımları (Ransomware)

Fidye yazılımı, bir solucan gibi yayılan ve kullanıcıların sistemlerine sızarak erişimi sınırlayan ve engelleyen, sistem ekranını kilitleyerek kullanılmaz hale getiren veya bir fidye tahsil edilmedikçe kullanıcıların kişisel dosyalarını kilitleyen kötü amaçlı bir yazılımdır. Fidye yazılımları, genellikle yok edilemez şifrelemeden oluşmaktadır bu nedenle şifrenin çözülme ihtimali imkânsız hale gelmektedir. Saldırganlar çoğunlukla bir kuruluşun sistemlerine sızarak önemli iş verilerini şifrelemekte ve ardından "bitcoin" gibi dijital nakit formatlarından ödeme talebinde bulunmaktadır (Bartock vd.,2016: 30).

Bitcoin vb ödeme sistemlerinin hayatımıza girmesiyle birlikte ödemelerin bu platformlardan istenmesi güvenlik güçlerinin ve siber savunma departmanlarının görevini zorlaştırmıştır. Dijital nakit formatlarından önce fidye yazılımlarına yapılan ödemeler geleneksel para birimlerinden oluştuğu için saldırıyı gerçekleştiren kişi veya grupların tespit edilmesi daha kolay olduğu için saldırganlar açısından bu durum önemli bir problem olmuştur. Dünya genelinde fidye yazılımları en önemli siber tehditler listesinde ilk sıralarda olmaya devam ettiği; özellikle sağlık, telekomünikasyon ve finans gibi alanlarda fidye yazılım saldırılarının giderek arttığı tespit edilmiştir (Çelik ve Çeliktaş, 2018: 109). Grafik 2.1 de Dünya çapında fidye yazılım sayısına ilişkin bilgiler yer almaktadır.



Grafik 2.1 Dünya Çapında Yıllık Fidye Yazılımı Saldırısı Sayısı (2017-2023)
Kaynak: (Statista, 2025).

2023 yılı itibarıyla, dünya genelindeki kuruluşlar 317,59 milyon fidye yazılımı saldırı girişimi tespit etmiştir. Genel olarak bu sayı, 2022 yılının üçüncü ve dördüncü çeyrekleri arasında önemli bir azalma göstermiş ve sırasıyla yaklaşık 102 milyondan 155 milyon vakaya ulaşmıştır (Statista, 2024).

2.1.5.4. İstem Dışı Alınan Elektronik Postalar (Spam)

Spam, e-mail ve mesajlaşma teknolojilerinin kötü amaçlarla kullanılması ve kullanıcıların istemedikleri bir durum ile karşılaşmaları durumunu ifade etmektedir. İstem dışı alınan iletiler çoğunlukla ticari reklamlar şeklinde olmaktadır. Spam gönderimi gönderen açısından ufak maliyetli olsa da gönderimi alan taraflar için büyük kayıplara neden olmaktadır (Adır, 2019: 31).

Spam gönderimi genellikle reklam veya belirli bir siteye yönlendirme amacıyla gönderilmektedir. Bu işlem için e-posta adreslerinin elde edilmesi ise yasadışı yollarla veya adres sahibinin anlık dikkat kaybı ile gerçekleşmektedir (Naralan, 2002: 6).

Aldatıcı e-postaların içeriği birçok farklı şekillerde olabilmektedir. Bunlardan bazıları aşağıdaki gibidir (Marmara Üniversitesi, 2015):

- Gelen e-postalar yurtdışı kaynaklı ise yanlış dil bilgisi veya başka bir dilde yazılmıştır.
- “Hesabınız kapatılacak", “e-postalarınız silinecek”, "Ceza ödeyeceksiniz", "Kota Artırımı", "Kargonuz teslim edilemedi" gibi ibareler kullanılarak sizi ikna etmeye çalışan ifadeler içermektedir.
- E-postaya cevap vermek yerine, “Aşağıdaki linke tıklayarak bilgilerinizi güncelleyiniz" şeklinde tuzak sayfalara yönlendiren bağlantıları içerisinde barındırabilmektedir.

E-posta hizmetinin bu denli sık kullanımı, düşük maliyetli olması ve kısa sürede büyük çaplı kitlelere ulaşabilmesi spam probleminin ortaya çıkışında önemli rolleri oluşturmaktadır. Genellikle pazarlama ve reklam çalışmaları için gönderilen spam mesajlar, sahte ürün, siyasi ve dini ideolojilerin yayılması, güvenliğin tehdit edilmesi (casus yazılım, virüs ve trojan vb) gibi amaçlar taşımaktadır. Gönderilen spam e-postaların verdiği zararlar arasında (Öztürk, 2009: 123);

- Gelen e-posta mesajlarının kontrolü ve ayıklanması sırasında geçen zaman kaybı,
- Yüksek band genişliği ihtiyacı,
- Posta kutusunun depolama alanının dolması sonucunda gerekli e-postaların alınamaması,
- Para, zaman ve itibar kayıplarının oluşması,
- Spam mesajlarının fazlalığından kaynaklı önemli e-postaların gözden kaçması,
- Gerçekdışı ürün satışlarıyla kullanıcıların dolandırılması,
- Terör amaçlı propaganda faaliyetlerinde kullanılması,
- Sistemin gereksiz meşgul edilmesi sonucu hizmet veremez duruma getirilmesi,
- Bilgisayar ve sistem güvenliği için tehdit oluşturması,
- Casus yazılımlar ile kişisel verilere ulaşılması ve yasa dışı işlemlerde kullanılması, sayılabilir. Gerek kurumsal gerekse kişisel güvenlik için tehdit unsuru

olan bu tür mesajlar, maddi açıdan milyarlarca dolarlık para kaybına neden olurken kullanıcı yönünden e-posta hizmetine olan güveni de önemli oranda sarsmaktadır.

2.1.5.5. Tuş Kaydediciler (Keylogger)

Dolandırıcıların kullanıcı verilerini elde etmek için tercih ettikleri bir diğer yöntem tuş kaydedicilerdir. Tuş kaydedici, bilgisayarın klavye tuşlamalarından yola çıkarak bu vuruşları anlık olarak kopyalayan ve bu kopyalamaları kaydedip e-mail yoluyla saldırgan yazılımcının ele geçirmesine olanak sağlayan programlardır. Bu programın özelliği klavyede yazılan her şeyi kayıt altına almasıdır (Tunay, 2024: 171).

Tuş kaydediciler ve benzerindeki diğer kötü yazılımların ana temasını saldırı düzenleri oluşturmaktadır. Kötü amaçlı yazılım enfeksiyonlarının geneli geliştirme, dağıtım ve enfeksiyon ve yürütme basamaklarının bir dizi halinde mümkün olduğunca standart bir saldırı düzeni barındırmaktadır. Dağıtım ve yürütme, kötü amaçlı yazılımın bir ayağı olarak uygulanabilmekte ve bu sebepten ötürü tasarlanmasında ve geliştirilmesinde katkısı bulunmaktadır. Tuş kaydedici kötü amaçlı yazılımın yürütülmeye başlaması ve tuş kaydedicinin devreye girmesine ve bağlamına bağlı olarak çeşitli şekilde gerçekleşebilmektedir. Fakat bazı tuş kaydedici gerçekçi olarak iki durumu paylaşmaktadır (Tuli ve Sahu, 2013: 107):

(a) tuş vuruşlarını almak için kullanıcı giriş akışına bağlanma,

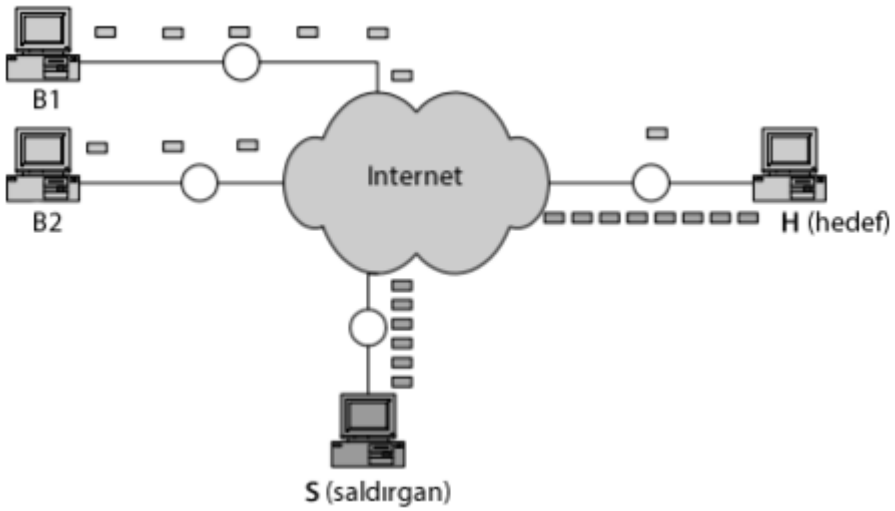
(b) verileri uzak bir konuma taşıma.

2.1.5.6. Hizmet Engelleme (DOS-DDOS) Saldırıları

İki tür hizmet engelleme saldırısı bulunmaktadır. Bunlar DOS (Denial Of Service- Servis Hizmet Reddi) ve DDOS (Distributed Denial of Service - Dağıtılmış Hizmet Reddi) saldırılarıdır. DoS saldırıları genelde bir iletişim ağında var olan kaynağın/kaynakların kötücül bir yaklaşımla kullanılarak sistemde yer alan bileşenlerin etkisiz hale getirilerek haberleşemez duruma getirilmesidir. Saldırının birden fazla noktadan organize olmuş bir şekilde gerçekleştirilmesine de DDoS saldırıları denmektedir (Arış vd., 2015: 1).

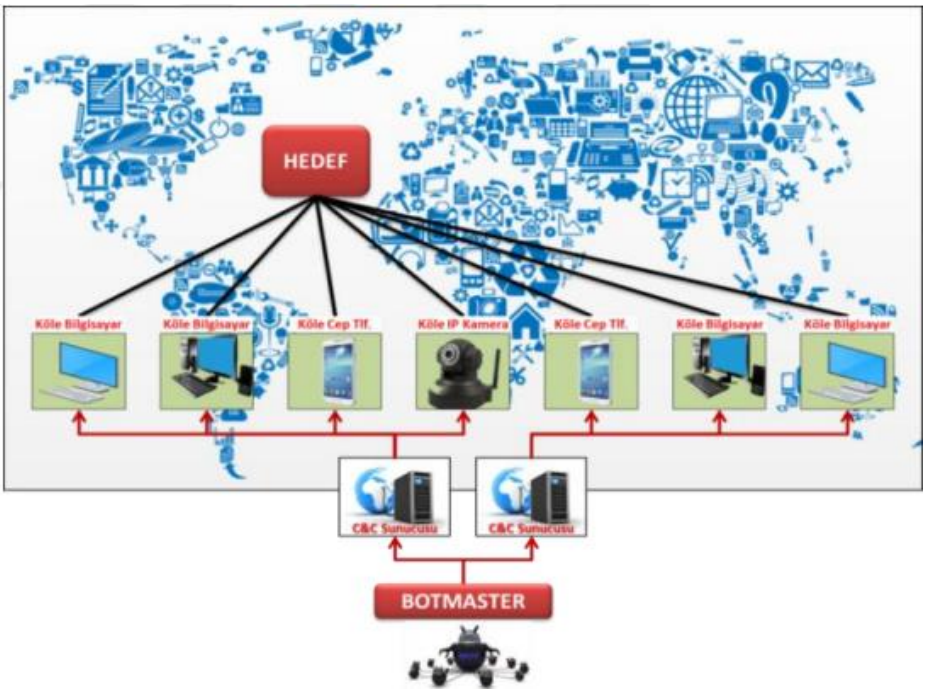
DoS sistemlere ya da servislere aşırı yük göndererek çalışamaz hale gelmelerini amaçlayan bir saldırı türünü ifade etmektedir. Bu saldırı türünde asıl hedef

internet uygulamasının kendisi değil uygulamanın içerisinde barındırdığı sunucu ve kaynaklardır. DoS saldırıları gerçekleştiğinde sistemler veya sunucular devre dışı bırakılabilmektedir. Bunun sonucunda uygulama sahibi kişi veya şirket maddi ve manevi kayıp yaşayabilmektedir. Şekil 2.7'de görüldüğü üzere DoS saldırıları bir merkezden başka bir merkeze direk yapılan saldırılar olarak adlandırılmaktadır (Çelikbilek, 2016: 2).



Şekil 2.7. DoS Atağı Senaryosu
Kaynak: (Çelikbilek, 2016: 2).

DDoS; İnternet üzerinden ele geçirilen birçok sistemden hedeflenen bir noktaya yapılan saldırı olarak tanımlanabilmektedir. DDoS saldırı çeşidinde farklı noktalardan sunucuya eş zamanlı olarak birçok sayıda veri paketi gönderilmektedir. Sunucu kendisine gönderilen paketleri işlerken kendi sistem kaynaklarını (işlemci, hafıza, bant genişliği) tüketebilmektedir. DDoS saldırılarının temel amacı hedef sistemin bant genişliğini ya da kaynaklarını (CPU, RAM, Disk) tüketmektir. Sonuç olarak sunucu veri paketlerine cevap veremez hale geldiğinde servis dışı kalmış olacaktır. Şekil 2.8'de DDoS saldırı senaryosu görülmektedir (Masum, 2017: 6).



Şekil 2.8. DDoS saldırı senaryosu
Kaynak: (Masum, 2017: 6).

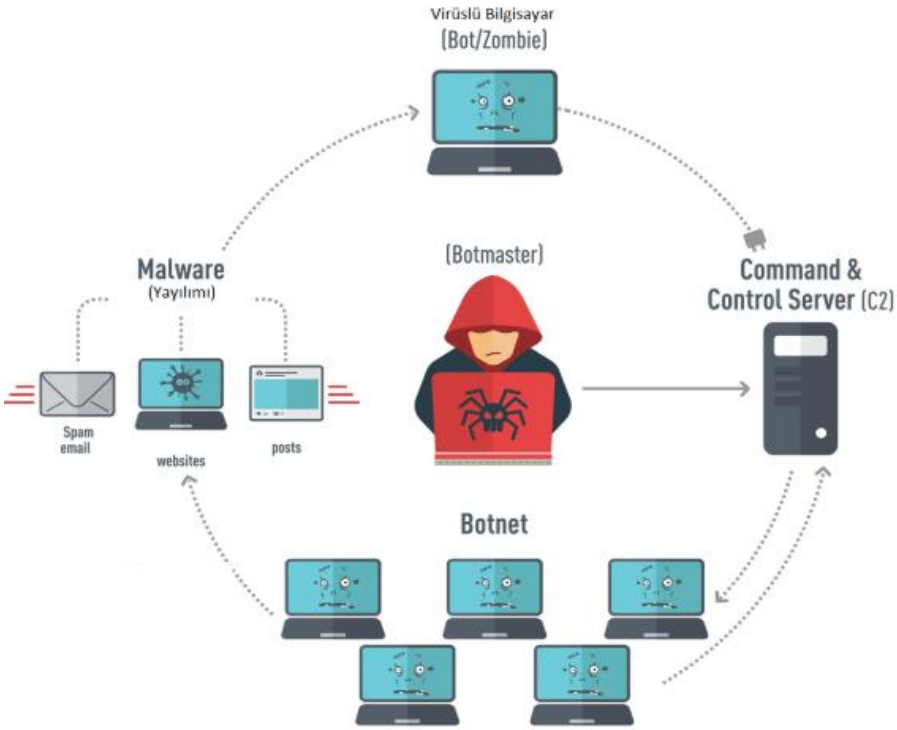
2.1.5.7. Botnet Saldırısı

Robot sözcüğünün kısaltılmışı olan "bot" sözcüğünden ve İngilizcede ağ anlamına gelen "net" sözcüklerinin bir araya gelmesiyle oluşmuş olan botnet (bot+net) sözcüğü, siber güvenlik literatüründe köleleştirilmiş, robotlaşmış veya kontrolü başkalarında olan yönetilen bilişim ağlarına verilen addır. Kullanıcıların farkında olmaksızın kötücül yazılımların yüklendiği, kontrol mekanizmasının saldırganlarda olduğu ve izinsiz kişilerce düzenlenen siber saldırıları gerçekleştirilen ve saldırının olmasına rağmen gerçekleştirilen siber suçun dahilinde olduğunun farkında olmayan donanımlara, sistemlere "zombi bilgisayar'' ismi verilmektedir. Siber faaliyet unsurlarının en ciddisi olan zombi bilgisayar ağı saldırıları, konumu belirsiz uzaktan yönetilebilen içerisine dahil olmuş binlerce bilgisayar ile yönlendirilen ve kontrol edilen sunuculardan meydana gelmektedir (Bozgeyik, 2018: 42).

Botnet saldırısı bir birey veya bir grup saldırgan tarafından koordine edilen ve internet üzerinden birbirine bağlanmış bilgisayarlar vasıtası ile gerçekleşmektedir. Bu saldırıya uğrayan bilgisayarlar, virüslü bir medya dosyasını veya bir spam e-posta

ekini açarak ya da zararlı bir web sitesine giriş yaparak enfekte olmaktadırlar (Kılınç ve Eyüpoğlu, 2023: 104).

Botnetler ya da zombi bilgisayarlar bu tehdit grubunun en tehlikeli olanları olarak kabul edilmektedir. Burada dikkat çeken nokta, bilgisayar kullanıcısının hiç farkında olmaksızın bilgisayarının kötü amaçlar veya ciddi suçlar işlenmesinde kullanılabilmesidir (Öğün ve Kaya, 2013: 155).



Şekil 2.9. Botnet Sisteminin İşleyişi
Kaynak: (Elmrabit vd., 2020: 28).

Bir botnet sisteminin işleyişi Şekil 2.9'daki gibidir. Öncelikle bot ağına girebilmesi için kullanıcıların elektronik posta, web sitesi veya gönderiler aracılığıyla cihazına zararlı yazılımların bulaşması gerekmektedir. Bu yöntemle birçok sayıda zararlı yazılım bulaşan bilgisayarlar bot ağını oluşturmaktadır. Botnet ismi verilen bu ağa bulaştırılan zararlı yazılım aracılığı ile botmaster denilen ve bu ağı yöneten siber saldırgan hedeflediği noktalara yönelik saldırılar gerçekleştirileceği zaman bu

bilgisayarları kontrol ederek komutlar vermekte ve dilediği gibi yönlendirmektedir (Eren, 2023: 60).

2.1.5.8. Sosyal Mühendislik (Social Engineering)

Sosyal mühendislik, kullanıcıların bilgi sistemlerini tehlikeye atmasını sağlama sanatı olarak ifade edilmektedir. Sosyal mühendisler teknik saldırılar yerine genelde bilgisine ulaşabilme potansiyeli fazla olan insanları hedefe alarak gizli bilgilerini ifşa etmekte veya etki ve ikna yoluyla planladıkları saldırıyı gerçekleştirmeye yönlendirmektedirler (Katharina Krombholz, 2015: 2).

Sosyal mühendislikte saldırganların öncelikli yaptıkları işlem hedefteki kişi veya kurum hakkında ayrıntılı bilgi elde etmektir. Sosyal mühendislik saldırılarının ilk adımı olan bilgi toplama süreci aylarda sürmekte ve beklediği bilinmektedir. Bilgi toplamanın yanı sıra doğru hedefi belirlemek de saldırının başarısı açısından oldukça önemlidir. Saldırganlar ikna edebilecekleri hedefleri özenle belirlemektedir. Ardından gerçekleştirilecek olan saldırı için gerekli özel bir planı oluşturmakta ve her ihtimali düşünerek alternatif planları da devreye sokmaktadırlar. Son aşamada ise saldırganlar bir senaryo üreterek ve kullanılacak araç ve gereçler, yazılımlar ve programları hedefin ilgi alanlarına göre düzenleyerek saldırıyı başlatmaktadırlar (Bozkurt, 2024: 47).

Sosyal mühendislik türleri, sürekli evrilen ve güncellenen bir yapıya sahip olup, uygulanan güvenlik önlemleriyle bile güvenlik açıklarını hedefleyen, net sınırları olmayan ve savunmasız alanları hedef alan sosyal mühendislik saldırıları, her zaman tam anlamıyla başarı sağlanmasını engellemektedir. Bu nedenle, her sistemde olduğu gibi güvenlik önlemlerinin de düzenli aralıklarla gözden geçirilmesi ve iyileştirilmesi gerekmektedir (Keskin ve Gözenman, 2019: 285).

2.1.5.9. SQL Enjeksiyonu (SQL Injection)

Günümüzde internetin hızla yayılmasıyla birlikte bireyler birçok işlemi çevrimiçi olarak gerçekleştirmektedir. SQL enjeksiyon saldırısı, veri tabanlarına saldırılar düzenleyerek bireylerin ihtiyaçlarını belirlemeye yönelik SQL sorgularını devreye sokan bir çeşit internet tabanlı saldırı taktiğidir (Avcı vd., 2021: 213). Bir diğer ifadeyle SQL enjeksiyonu, internet uygulamalarından elde edilen kullanıcı girdileri ile

yapılan SQL sorgularının manipüle edilmesi olarak tanımlanabilmektedir (Anley, 2002: 3).

Kullanıcıların etkileşimde bulundukları veri tabanlı web uygulamalarında, sorgu veya parametreler kullanılarak veri tabanı tablolarındaki bilgiler belirli kriterlere göre filtrelenerek uygulama ara yüzüne aktarılmaktadır. Aktarılan bu sonuç değerleri, uygulamanın tasarımına göre kullanıcıya veya yöneticiye belirlenmiş biçimlerde sunulmaktadır. SQL enjeksiyonu yöntemi tam bu işlemler gerçekleştirilirken yapılmaktadır. Saldırgan, web tarayıcı adres çubuğuna ya da uygulamada bulunan giriş kontrollerine kötücül kodlar ekleyerek, SQL enjeksiyon saldırısını gerçekleştirmektedir. Genel kullanıma açık olmayan ancak bu şekilde elde edilen bilgiler önemli ve gizli olabilmektedir. Saldırgan, sistem ve veri tabanı hakkında elde ettiği bu önemli bilgilerle SQL enjeksiyon senaryosuna farklı boyutlar oluşturarak, veri tabanında bulunan diğer bilgilere ulaşabilmektedir. Sonrasında elde ettiği bilgileri kullanarak, hedefini gerçekleştirmektedir (Demirol, 2013: 1).

2.1.5.10. İstismar Kiti (Exploit Kits)

Çağımızda yaygın bir şekilde kullanılan internet, siber saldırganlar tarafından web kullanıcılarına hiç olmadığı kadar tehditkâr olmakta ve Exploit Kit'ler (EK'ler) internet suçları için önemli bir yıkıcı güç unsuru olmaktadır (Süren, 2019: 3).

Exploit, saldırıyı gerçekleştirecek olan siber suçluların bir sisteme izinsiz erişim sağlamak için kullandığı güvenlik boşluklarından veya hatalardan faydalanan bir çeşit kötü amaçlı yazılımdır (Bayram vd., 2022: 179). Diğer bir ifadeyle, hedef sistem üzerindeki açıklıkları tespit edip bu açıklıkları kullanarak sisteme yönelik saldırılar gerçekleştirebilen exploit kitler, birçok fonksiyon ve yapılandırma seçenekleri sunan kullanıma hazır yazılımlardır (Yaşar, 2014 : 26).

Exploitler genel bir çerçevede değerlendirilecek olduğunda 7 ana başlıkta incelenmektedir. Bunlar (Ganal, 2016: 9);

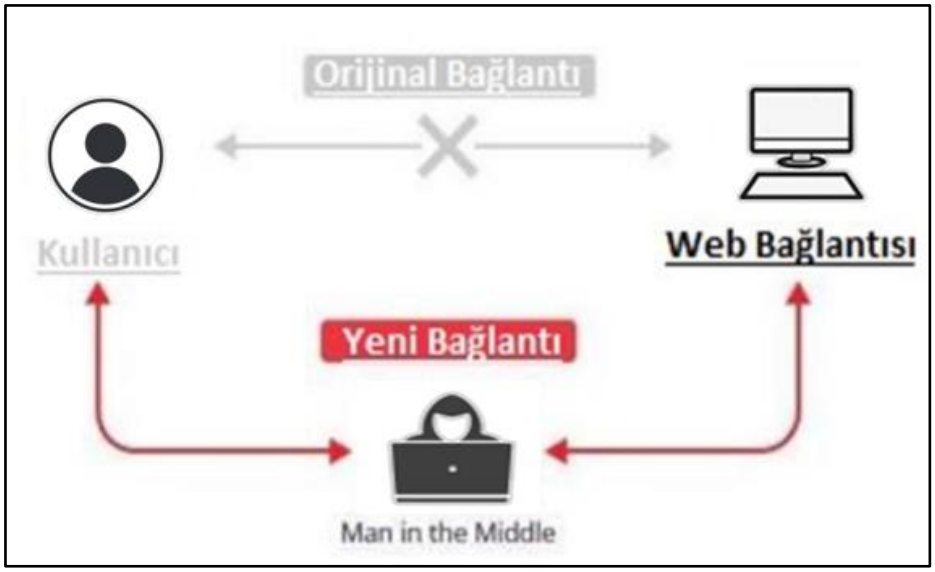
- Zero Day Exploit (Sıfırıncı Gün Exploitleri)
- Remote Exploits (Uzaktan Erişim Exploitleri)
- Web Application Exploits (Web Uygulamaları Exploitleri)
- Local Exploits (Yerel Exploitler)

- Privilege Escalation Exploits (Hak Yükseltme Exploitleri)
- Denial of Service Exploits (Hizmet Engelleme Exploitleri)
- PoC Exploits (Kavram İspat Exploitleri)

İnternete erişimi olan cihazlarda sıklıkla kullanılan uygulama, Ek'lerin hedefin sistemini kötü amaçlı yazılımla enfekte etmesi için zayıf hedefler olan tarayıcılardır ve oluşabilecek bir güvenlik boşluğundan faydalandıktan sonra, siber saldırganlar genellikle kullanıcının kişisel verilerini kötücül amaçlarda doğrudan kullanmak veya erişimi kısıtlamak için bilgileri çalmakta ve daha sonra kullanıcının şifresine ulaşabilmesi için gerekli olan şifre çözme rutinini etkinleştirmek için fidye talebinde bulunmaktadır. Bu durumdan daha da tehlikelisi, tehlikeye maruz kalan cihazlar herhangi bir geri dönütte bulunulmadan başka sistemlere saldırı gerçekleştirmek için kullanılmaktadırlar. Bu sebeple, günümüzde EK olgusu birçok güvenlik uygulayıcısı ve araştırmacısının öncelikli endişeleri arasında yer almaktadır (Süren, 2019: 3).

2.1.5.11. Ortadaki Adam Saldırısı (Man In The Middle)

Ortadaki adam saldırısı iki veya daha fazla uç nokta arasındaki iletişim ağını kötü amaçlı üçüncü bir tarafın kendini kamufle ederek gerçekleştirdiği bir saldırı biçimidir. Ortadaki adam saldırısını gerçekleştiren saldırganlar kurbanlar arasındaki iletişim hattını dönüştürebilmekte, kesebilmekte veya değiştirebilmektedir. Üstelik, hedefteki kurbanlar saldırganın farkına varamazlar. Bu sebepten dolayı iletişim ağının korunduğuna inanmaktadırlar (Conti vd., 2016: 2028). Şekil 2.10'da ortadaki adam saldırısının örnek bir şeması gösterilmektedir.



Şekil 2.10. Man in the Middle saldırısının örnek şeması
Kaynak: (Mallik, 2018: 110).

MITM saldırıları, iki veya daha fazla sistem arasındaki iletişim kanallarını kestikten sonra saldırganın kritik verilerin çok çabuk ele geçirmesine ve değiştirmesine olanak sağladığı için ağ güvenliği açısından ciddi tehdit unsuru oluşturmaktadır. Bu zaman zarfında kurban olup bitenden habersiz internete bağlanmayı sürdürür fakat sistemle iletişim kurulan bütün siteler saldırganlar tarafından da görünür durumdadır. Bu saldırı yöntemi, saldırganın kurbanların tüm konuşmalarını kontrol ettiği gizli bir dinleme türüdür (Dicle, 2022: 102).

2.1.5.12. IP Aldatmacası (IP Spoofing)

Bilgisayar ağlarında, IP adresi sahteciliği veya IP sahteciliği terimi, gönderenin kimlik bilgilerini saklamak veya başka bir bilgi işlem sistemini taklit etmek amacıyla sahte kaynak IP adresine sahip İnternet Protokolü (IP) paketlerinin oluşturulmasını ifade etmektedir. Sahtecilik saldırısında, saldırgan bir bilgisayara mesajın güvenilir bir sistemden geldiğini belirten mesajlar gönderir. Başarılı olmak için saldırgan önce güvenilir bir sistemin IP adresini belirlemeli ve ardından paket başlıklarını paketlerin güvenilir sistemden geliyormuş gibi görünecek şekilde değiştirmelidir. Özünde, saldırgan uzaktaki bilgisayarı ağın meşru bir üyesi olduğuna inandırarak kandırmaktadır (sahtecilik yapmaktadır). Saldırının amacı, saldırganın ana bilgisayara

kök erişimi elde etmesini sağlayacak bir bağlantı kurmak ve hedef sisteme bir arka kapı giriş yolu oluşturmaktır (Rashid ve Paul, 2013: 438).

IP aldatmacası sayesinde sisteme sızan korsan URL (Uniform Resource Locator- Birörnek Kaynak Bulucu) adreslerinin bir sahtesini hazırlayabilmektedir. Böylece orijinal siteyle aradaki fark anlaşılamaz hale gelmekte ve bu farkı anlayamayan kişi ve kurumların önemli bilgilerine ulaşılabilme imkânı doğmaktadır (Gürkaynak ve İren, 2011: 272).

2.1.5.13. Mantık Bombaları (Logic Bombs)

Mantık bombaları, bir programa kötücül bir kod parçasının dahil edilmesidir. Mantık bombaları çoğunlukla hedefte bulunan ağ veya bilgisayardaki verileri tamamen ortadan kaldırmak ve kullanılamaz hale getirmek için kullanılmaktadır (Çelik, 2013: 142).

Mantık bombaları virüs programı olmasının yansıra içerisine dahil olduğu bilişim sistemlerine yaratıcısının önceden belirlemiş olduğu özel durum oluşana dek veya önceden belirlenmiş ileri bir tarihte devreye girmesi için programlanması durumunda belirlenen bu ileri tarih geldiğinde devreye girerek sistemi deforme eden programlar şeklindeki kötücül yazılımlardır (Alioğlu, 2019: 16). Bu virüs devreye girdiğinde bilgisayardaki bütün veriler ve dosyalar yok olmakta ve dahası sistemi komple kullanılmaz hale getirebilmektedir. Mantık bombası olarak bilinen en popüler zararlı virüslerden biri ‘çernobil virüsü’dür. CIH (Çernobil Virüsü), 1998 yılında ortaya çıkmış, ana kartların Eprom (Erasable Programmable Read Only Memory) hafızasına veri yazarak kalıcı olarak donanıma zarar veren ilk virüs olmuştur (Alkan, 2023: 44).

2.1.5.14. Salam Tekniği (Salami Techniques)

Salam tekniği, çok fazla sayıda kaynaktan, az sayıda değerlerin transfer edilmesiyle gerçekleşmektedir. Tekniğin uygulanmasında genellikle truva atı programları kullanılmaktadır. Kaynağın çok fazla olmasından ötürü dikkat çekmeyecek düzeydeki değerlerin elde edilmesi haksız kazanç sağlamaktadır (Kızıltan, 2007: 25).

Salam tekniği (Salami techniques) genellikle bankacılık sektöründe kullanılmaktadır. Bu teknik hesapların virgülden sonraki son rakam veya son iki rakam tutarının başka bir hesaba aktararak haksız kazanç ele etme yöntemidir. (Aksoğan vd., 2019: 275).

Örnek bir olayda; bir banka memuru, bankanın elinde bulundurduğu milyonlarca mevduat hesabının dört ayda bir gerçekleştirilen faiz ödemelerinin dört ondalık kesir puanına kadar hesaplanabildiğini, sonra da aşağı veya yukarı yuvarlandığını tespit etmiştir. Bankanın bilişim sisteminde yer alan yazılım sayesinde bir doların 0,0075 kadar üstünde olan her rakam bir üst sente yuvarlanmakta ve mudiye ödeme gerçekleştirilmektedir. Bunun altında kalan rakamlar ise aşağı yuvarlanmakta ve bankanın hesabına eklenmektedir. Banka memuru yazılımın bu işlevini öğrenince, sistemin yaptığı işlemi değiştiren bir yazılım tasarlamış ve aşağı yuvarlanarak bankanın hesabına gitmesi gereken küsurat değerlerinin kendi açtığı bir hesaba gitmesini sağlamıştır. Banka çalışanının bu işlemi üç yıl süreyle uyguladığı ve bu süre içinde milyonlarca dolar tutarında hukuka aykırı yarar sağladığı belirtilmektedir (Bozkurt, 2024: 51).

2.1.5.15. Bukalemunlar (Chameleon)

Kendini gizleyerek normal bir program gibi işlevini sürdürürken arka planda birtakım aldatmacalar ile çok kullanıcılı sistemlerde kullanıcı adları ve şifrelerini taklit ederek saklı bir dosyaya kaydedip, sistemin geçici bir süreliğine bakıma alınacağına ilişkin bir uyarı göndermektedir. Bu esnada bukalemun programını kullanan kötü niyetli kişi saklanan bu dosyaya ulaşarak kullanıcı adı ve şifresini elde etmiş olur (Aslay, 2017: 26).

2.1.5.16. Çöpe Dalma- Atık Toplama (Scavenging)

Çöplenme veya atık toplama olarak adlandırılan yöntem, bilişim sisteminde gerçekleştirilen veri-işlem sonunda kalan bilgilerin depolanmasını ifade etmektedir. Bu bilgiler öncelikle, çıktı birimlerince oluşturulan ve sonrasında çöpe atılan kâğıt, mürekkep şeridi gibi malzemeler üzerindeki bilgilerin bir araya getirilmesiyle elde edilmektedir. Bir diğer teknik ise bilişim sisteminin hafızasında bulunan ve artık

gereksinim duyulmayan geri dönüşüme yollanmış bilgileri bazı yöntemlerle geri getirmektedir (Altunok ve Vural, 2011: 78).

Özellikle çöpe dalma tekniği denilen ve bozuk, hurda veya tamir edilmek üzere servise bırakılan bilgisayar ve cep telefonları kurcalanarak kullanıcının özel bilgilerine ulaşabilmektedir. Şirketler ve kurumlar bilgisayarlarını tamire vermeden önce önemli bilgileri veya ticari sırları çalınmasın diye harddiskleri sökmeli veya içeriği güvenli olarak silmelidir. Çünkü, harddisk üzerinden veri silerken sadece veriye erişim yolu silinmekte veri istenirse tekrar kurtarılabilmektedir (Bilek, 2012: 86).

2.2. KOBİ'lerde Siber Güvenlik

Türkiye'de genel olarak çalışan sayısı 250'yi aşmayan şirketler KOBİ olarak tanımlanmaktadır. KOBİ'ler ilerlemiş ve ilerlemekte olan tüm devletlerde fabrikaların %99' unu oluşturmaktadırlar ancak istihdam, ihracat ve yatırım alanlarında ise payları ise düşüktür (Ulusoy ve Akarsu, 2012: 105). Dünya Ticaret Raporu'na (2016) göre KOBİ'ler dünya ekonomisinin %90'ını, istihdamın %60'ını ve Gayri Safi Yurt İçi Hasıla (GSYİH)'nin %55'ini oluşturmaktadır. KOBİ'ler geçmişten bugüne ekonomik büyüme ve kalkınmanın itici gücünü oluşturmaktadır. KOBİ'ler ulusal ve küresel bağlamda ekonomik gelişimin, yeni iş imkanları sağlanmasının ve istihdamın en önemli oyuncularından birini oluşturmaktadır (KOSGEB, 2024: 7).

Dijital dünya, çevrimiçi platformlarda faaliyet göstererek erişimlerini genişletebilen KOBİ'ler için birçok fırsat sunmaktadır (Lloyd, 2020: 1). İnternet, kuruluşların birçok avantaj elde etmelerini sağlamaktadır. Özellikle işletmeler, küresel ölçekte yeni tedarikçilerle daha düşük maliyetler sağlamak ve yeni müşterilerle daha fazla satış yapabilmek amacıyla bağlantılar kurabilmektedir. Bu durum, iletişim giderlerinin azalmasına, daha yüksek verimlilik ve daha hızlı işlem süreçlerine neden olmaktadır. Ancak, tüm bu avantajlarının yanı sıra, işletmeler interneti kullanırken bazı önemli zorluklarla karşılaşmaktadır. Bu zorluklar arasında, siber saldırganlar, spam gönderenler ve suç örgütlerinin oluşturduğu tehditler ön planda yer almaktadır. Bu tehditler, çevrimiçi faaliyetleri güvenli ve verimli bir şekilde sürdürme konusunda işletmeleri ciddi şekilde zorlamaktadır (Arroyabe vd., 2024: 1).

Siber suçlardaki artış, tüm iş dünyasını etkilemiş ve özellikle KOBİ'ler daha fazla hedef alınan bir grup haline gelmiştir. KOBİ'lere yönelik siber saldırılardaki artışın sebeplerinden biri, bu işletmelerin genellikle zayıf kurumsal siber güvenlik önlemleriyle faaliyet göstermeleridir. Büyük işletmelerin aksine, KOBİ'ler, bilgi eksiklikleri ve uzmanlık yetersizlikleri, sınırlı farkındalık ve kaynak yetersizlikleri nedeniyle siber tehditlere karşı daha savunmasız bir durumdadır (Bada ve Nurse, 2019: 2). Siber tehditler tarafsızdır ve işletmeleri bir bütün olarak etkileyebilir. Ancak KOBİ'ler, daha büyük işletmelere kıyasla bazı belirli siber tehditlerden ve saldırılardan daha yoğun bir şekilde etkilenmeye eğilimlidir (Antunes, 2021: 224).

KOBİ'ler, sıklıkla siber saldırıların en fazla etkilenen mağdurları arasında yer almaktadır. Bu saldırılardan kaynaklanan zararları gidermek konusunda ciddi güçlükler yaşamaktadırlar. KOBİ'ler, genellikle sınırlı kaynaklara ve zayıf siber güvenlik alt yapılarına sahip oldukları için büyük işletmelere kıyasla daha kolay hedef haline gelmektedir. Büyük işletmeler ise son yıllarda karşılaşabilecekleri siber tehditlere karşı daha güçlü güvenlik önlemleri alarak, savunmalarını güçlendirmek amacıyla yatırımlar yapmaktadırlar.

2.2.1. Siber Güvenliğin KOBİ'ler İçin Önemi

Dijital teknolojiler ve yenilikler, işletmelerin iş süreçlerini, ürünlerini, hizmetlerini ve ilişkilerini derinden etkileyerek, iş yapma biçimlerini ve liderlik anlayışlarını yeniden şekillendirmelerini zorunlu kılmaktadır (Karimi ve Walter, 2015: 41). Dijital teknolojilerin benimsenmesi, yeni iş modellerinin geliştirilmesi, verimliliğin arttırılması ve daha iyi karar verme yeteneğine yol açmaktadır. Fakat bu faydalar, siber tehditlerden korunmak için gerek duyulan harcamalarla birlikte, bilinmesi gereken yeni riskler ve güvenlik açıklarını da beraberinde getirmektedir (Serac, 2023: 772).

Dijitalleşme, KOBİ'ler için verimliliği ve büyümeyi artırma, küresel ekonomi ile entegrasyonu sağlama ve dijital çağın gerekliliklerini hızlı ve etkili bir şekilde yerine getirme açısında önemli bir araç haline gelmiştir. KOBİ'ler, iş sürekliliklerini temin etmek, yeni teknolojilere uyum sağlamak, yeni rakiplerin pazardaki baskısını azaltmak ve değişen müşteri tercihlerini yönetebilmek amacıyla dijitalleşme çabalarını

hızlandırma gerekliliği ile karşı karşıya kalmaktadırlar (Yıldırım ve Durukan, 2023: 906). Kuruluşlar pazar erişimlerini genişletmek için interneti seçtikçe, kendilerini güvence altına almak için gereken adımlarla tanışmışlardır; kuruluş siber uzaya doğru büyüdükçe, oluşturulan veri miktarı muazzamdır. Dijital formattaki bilgiler "birbirine ağlı ağlar" aracılığıyla dünyayı dolaşır. Bu da bilgileri Truva atları, kötü amaçlı yazılımlar, kimlik avı ve diğer siber terör eylemleri gibi saldırılara ve hack'lere karşı savunmasız hale getirmektedir. Bilgi artık bir kuruluş için değerli bir varlık olarak kabul edilmekte ve bilgi kaybı, kuruluş için büyük mali kayıplara ve itibar kaybına yol açabilmektedir (Khan vd., 2020: 328).

Ponemon Enstitüsü tarafından yakın zamanda yapılan bir araştırma, KOBİ'lerin karşılaştığı siber güvenlik zorluklarına dair net bir çerçeve sunmaktadır. "KOBİ'lerde Küresel Siber Güvenlik Durumu" isimli raporda üst üste üç yıl, KOBİ'lerdeki güvenlik ihlallerinde önemli bir artış olduğu bildirilirken, aynı zamanda işletmelerin veri ihlallerini tespit etme süresinin de ortalama 197 gün sürdüğü belirtilmektedir (CyberMag, 2020).

Sage (Sage, 2023: 4) tarafından yapılan araştırmaya göre 2023 yılında dünya genelinde siber saldırılara maruz kalan KOBİ'lerin oranı %48 neredeyse her iki KOBİ'den birisinin siber saldırıya uğradığını gösteren rapora göre ankete katılan şirket yöneticilerinin büyük çoğunluğu siber tehdit ve saldırıları en büyük endişe kaynağı olarak aktarmaktadır.

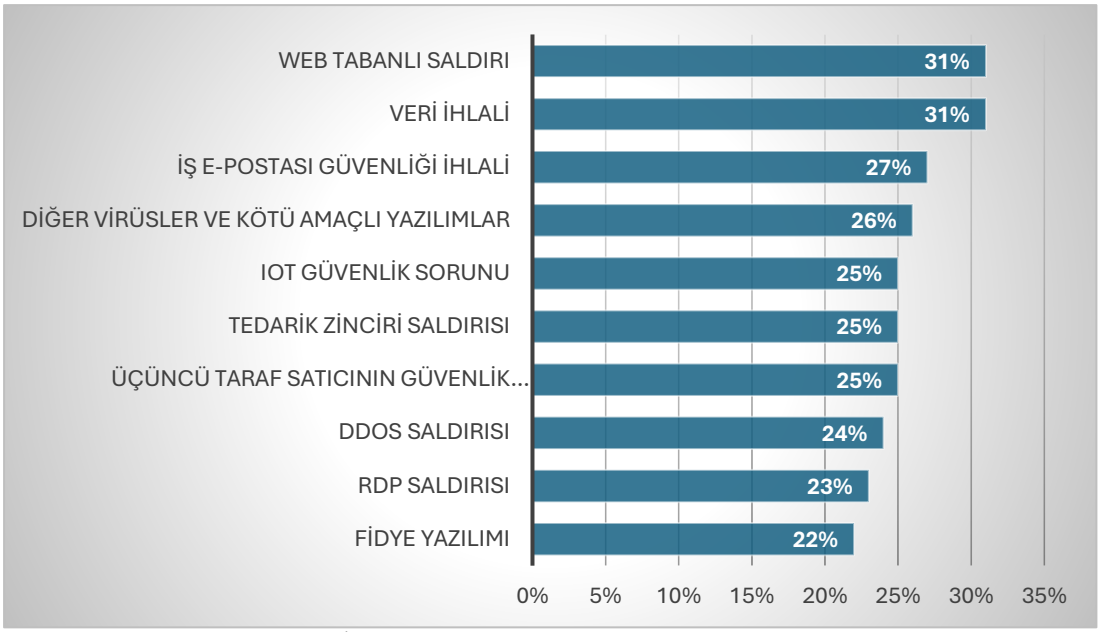
KOBİ'lerin sınırlı bir bütçesi olduğundan daha az uzmanlığa sahiptirler ve BT güvenlik politikalarını ve stratejilerini başlatma, kurma ve sürdürme konusunda daha az kaynak harcarlar (Khan vd., 2020: 329). Bundan dolayı Siber suçlular giderek daha zayıf savunmalara sahip oldukları düşünülen KOBİ'leri hedef almaktadır (Renaud ve Weir, 2016: 137). Bir KOBİ'de siber güvenlik politikasının uygulanması söz konusu olduğunda yönetimin desteği hayati önem taşımaktadır. Üst yönetim siber güvenlik politikasına uymazsa bu KOBİ'deki diğer çalışanlar üzerinde olumsuz bir etkiye yol açmaktadır. Üst yönetimin BT departmanına politikayı uygulamada yardımcı olması önemlidir. Politikanın uygulanmasında karşılaşılan bir diğer zorluk da iş ortamıdır. Her KOBİ'nin farklı bir iş ortamı vardır ve siber güvenlik politikası buna uygun olması gerekmektedir. İş hedeflerini desteklemek için gereken yeterli güvenlik uygulamasını

belirlemek gerekmektedir. Çok kısıtlayıcı bir siber güvenlik politikası KOBİ tarafından sağlanan hizmette verimliliğin azalmasına ve kalite eksikliğine yol açabilmektedir (Khan vd., 2020: 332). Bu bağlamda, siber güvenlik, işletmelerin faaliyetlerinin işlerliğini etkilemeden geliştirilmesine olanak tanıyarak dayanıklılığını garanti altına alan önemli bir unsur olarak ortaya çıkmaktadır (Arroyabe vd., 2024: 711).

2.2.2. KOBİ'lerin Karşılaştığı Siber Tehditler

Son yıllarda, internet teknolojilerindeki ilerlemelerle paralel olarak siber saldırı ve suçlarının büyük bir artış gösterdiği gözlemlenmektedir. Bu durum, işletmeler açısından ciddi bir güvenlik riski teşkil etmekte ve önemli bir tehdit oluşturmaktadır. İşletme yöneticileri ve yetkililerinin bu tehditlere karşı yeterli önlemler almadığı takdirde, işletmelerin sahip olduğu bilgi ve sermaye unsurları savunmasız hale gelmektedir. Türkiye'deki işletmelerin büyük bir kısmını oluşturan KOBİ'ler, siber saldırılara daha fazla maruz kalmakta olup, KOBİ yöneticilerinin bu saldırılara karşı önlem alması kaçınılmaz bir gereklilik haline gelmektedir (Eş ve Serdar, 2021: 133).

Konuyla ilgili önemli sonuçlar ortaya koyan bir araştırma sonucunda, KOBİ'lerin siber güvenliği üzerine odaklanan rapor yayımlanmıştır. Bu rapora göre, siber suçlular artık son derece hedeflenmiş ve karmaşık saldırılarla bireysel kuruluşlara yönelmektedir. Bu durum, özellikle KOBİ'ler için büyük bir tehdit oluşturmakta; zira bu işletmeler, algılanan güvenlik açıkları nedeniyle sıkça saldırıların başlıca hedefi haline gelmektedir (Eset, 2024: 5). Aşağıdaki tabloda KOBİ'lerin en yaygın olan siber güvenlik tehditleri yer almaktadır.



Grafik 2.2. KOBİ'lerin karşılaştıkları en yaygın siber güvenlik tehditler
Kaynak: (Eset, 2024: 5).

Grafik incelendiğinde en yaygın siber güvenlik ihlalleri veya olayları %31'lik bir oranla web tabanlı saldırılar ve veri ihlalleri olduğu görülmektedir.

Raporda da gösterildiği gibi KOBİ'lerin karşılaştıkları birçok siber tehdit bulunmaktadır. KOBİ'lerin çoğunluğu bu tehdit ve saldırılarla nasıl baş edeceklerini bilmemektedir. Bu nedenle, KOBİ'lerin risklerini arttıran faktörlerin değerlendirilmesi oldukça önemlidir. Aşağıdaki tabloda KOBİ'lerde siber saldırı risklerini arttıran 5 faktör yer almaktadır. Bunlar arasında, yetersiz güvenlik önlemleri en önemli neden olarak öne çıkarken diğer dikkat çeken faktörler arasında bulut uygulamaları ve hizmetleri, üçüncü taraf satıcılar, kritik veya yüksek öneme sahip güvenlik açıkları, sistem yanlış yapılandırması bulunmaktadır.

Şekil 2.11. Siber güvenlik olaylarına katkıda bulunan başlıca nedenler
Kaynak: (Eset, 2024: 5).

2.2.3. KOBİ'lerde Siber Güvenlik Tehditlerine Karşı Alınabilecek Önlemler

Siber saldırılar hızla artmaya devam etmektedir. Bu nedenle siber saldırıların neredeyse hergün gerçekleştirildiği böylesine zorlu bir ortamla başa çıkabilmek için savunma odaklı bir yaklaşım sergilenmesi gerekmektedir (Elradi vd., 2021: 57). KOBİ'lerde veri güvenliğini sağlamak ve olası siber tehditlere karşı korunmak için ilk adım, kurum çalışanlarına bilgi teknolojilerinin güvenliği konusunda eğitimler vererek farkındalık yaratmaktır. Çünkü bir güvenlik zincirinin en zayıf halkası insandır. Kurumlar, güvenlik tehditlerine yönelik önlemler alırken hangi verilerin veya bilgilerin, hangi tehditlerden ne ölçüde korunması gerektiğini belirlemeli, güvenliği sağlamak için gerekli adımları planlamalı ve alınacak önlemlerin finansal maliyetini göz önünde bulundurmak gerekmektedir (Vural ve Sağıroğlu, 2011: 90). Aynı zamanda, herhangi bir siber güvenlik saldırısından kendinizi korumak için yeterli siber güvenlik farkındalığına sahip olma zorunluluğu bulunmaktadır. Bu planlamaların yansıra alınabilecek diğer önlemler şunlardır Bunlar, aşağıdaki gibi sıralanabilir (Elradi vd., 2021: 57):

Yazılım

1. Bir güvenlik duvarı kullandığınızdan emin olun.
2. Antispam ve/veya antiphishing yazılımı kullanın.
3. Güvenilir, güncel, gerçek zamanlı engelleyici bir antivirüs kullandığınızdan emin olun.
4. Uzaktan oturum açan herkesin VPN üzerinden oturum açmasını zorunlu kılan bir politika uygulayın.
5. Tüm işletim sistemlerinin güncel ve yamalı olduğundan emin olun.
6. Taşınabilir cihazdaki cihaz yazılımları (işletim sistemi ve antivirüs), yeni sürümler ve yamalar kullanıma sunulduğunda otomatik olarak güncellenecek şekilde ayarlanmalıdır (Blanke ve McGrady, 2016: 19).

Yedeklemeler

1. Donanım tabanlı, yazılım tabanlı veya her ikisi de olan bir yedekleme çözümü uygulayın.
2. Yedeklendikten sonra verilerin güvenli, erişilebilir ve yedekli olduğundan emin olun.
3. Yedeklemelerinizin kurtarma işlevini düzenli olarak test edin.
4. Veriler otomatik günlük bir programla şirket sunucusuna veya bulut sağlayıcısına yedeklenmelidir. (Blanke ve McGrady, 2016: 19).

Veri hırsızlığını önleme

1. Sistemde ve ağda herhangi bir olağandışı trafiği tespit etmek için ağ analiz araçlarını kullanın.
2. Yetkisiz erişimi korumak için izin kullanın.
3. Verilerinizin kurcalanmasını zorlaştırmak için dosya veya sürücü şifreleme araçlarını kullanın.

Siber güvenlik farkındalığınızı zenginleştirin

1. Şüpheli e-postalardan ve bağlantılardan mümkün olduğunca uzak durun, güncel bir güvenlik yazılımı kullanın ve çevrimiçi olduğunuzda çok fazla bilgi vermeyin.

Şifreleme

1. Tüm cihazlar parola korumalı ekran koruyucularla güvence altına alınmalı ve belirli bir süre sonra otomatik olarak oturum kapatılmalıdır (Blanke ve McGrady, 2016: 19).

2. Her cihazda güçlü parolalar (8 karakter ve rakam kombinasyonu) kullanılmalı ve bu parolalar 6 ayda bir değiştirilmelidir.

3. 5 başarısız oturum açma girişiminden sonra cihaz kilitleme etkinleştirilmelidir.

4. Kullanıcıların veri tabanlarına ve ağlara erişimi dosya, alan ve klasör parolaları kullanılarak kısıtlanmalıdır.

5. Sistemlere erişim için 2 veya 3 faktörlü kimlik doğrulamayı kullanın.

6. Şifrenizi sık sık değiştirin (örneğin her 60 günde bir veya daha az) (Forte ve Power, 2007: 17).

7. Hiçbir uygulamada "Kimliğinizi ve şifrenizi kaydedin" özelliğini etkinleştirmeyin (evet, bu size zaman kazandıracaktır, ancak sisteminizi ele geçiren herhangi bir siber suçlu için de zaman kazandıracaktır).

Bilişim teknolojileri ile ilgili politika ve eğitim:

1. Çalışanlara yıllık bazda farkındalık eğitimi verilmesini zorunlu kılın (Blanke ve McGrady, 2016: 19).

Ağ güvenliği:

1. Kullanıcıların veri tabanlarına ve ağlara erişimi dosya, alan ve klasör parolaları kullanılarak kısıtlanmalıdır (Blanke ve McGrady, 2016: 19).

2. Güvenlik duvarı kurallarını uygulayın ve iş rollerine ve sorumluluklara göre kullanıcı erişim kısıtlamalarını yönetin.

E-posta güvenliği

1. İstenmeyen, sıra dışı olan her şey dahil olmak üzere tüm sahte mesajları, spam'leri, çevrimiçi dolandırıcılıkları, zincir mektupları vb. silin, özellikle de kişisel finanslarınız veya işiniz hakkında bilgi vermeniz isteniyorsa (Forte ve Power, 2007: 16).

2. Beklemediğiniz, tanımadığınız veya doğrulayamadığınız bir e-posta ekine tıklamayın, özellikle de tanımadığınız birinden geliyorsa. Tanıdığınız birinden

geliyormuş gibi görünse bile, bu o kişinin e-posta adres defterini kullanan bir solucan veya virüsün sonucu olabilir.

Fiziksel güvenlik önlemleri:

1. Bilişim sisteminin fiziksel güvenliği sağlanmalıdır. Sunucu veya veri tabanlarının bulunduğu oda herkese açık olmamalı ve havalandırması iyi olmalıdır. Ancak kullanım izni olanlar, sistemi kullanabilmelidir. İşletme içi ve gerekli görülürse işletme dışı bilgi ve/veya sistem yedeklemesi yapılmalıdır. Ayrıca, kesintisiz güç kaynağı kullanılmalıdır (Acılar, 2009: 8).
2. Küçük veya büyük işletmeler, bilgisayar kullandıkları ve İnternet'e bağlı oldukları müddetçe güvenlik riskleri ile karşı karşıyadır. Önemli olan, bu risklerin farkında olmak, gerekli yazılım ve donanım önlemlerini almak, çalışanları güvenlik tehditleri hakkında bilgilendirmek, devamlı olarak güvenlik tehditleri ile ilgili gelişmeleri takip ederek, en kötü durumlara karşı acil eylem planı ile hazır olmaktır (Keller vd., 2005: 7).

Günümüzde teknolojinin hızla ilerlemesi ve dijitalleşmemin giderek artan önemi KOBİ'lerin iş süreçlerine de entegre olmuştur. Dijital dönüşüm uygulamaları, işletmeleri maliyet, hız, esneklik gibi birçok yönden daha verimli hale gelmelerine olanak tanımaktadır. KOBİ'lerin dijital platformlarda veri akışı, e-ticaret işlemleri ve bulut tabanlı sistemlere yönelmesi siber tehditleri de beraberinde getirmektedir. Bu tehditlere karşı işletmelerin etkili siber güvenlik stratejilerini uygulamaya koymayı zorunlu hale getirmiştir. Bu nedenle, siber güvenlik artık sadece büyük ölçekli işletmeler için değil, KOBİ'ler için de kritik bir öncelik haline gelmiştir. KOBİ'lerin dijital altyapılarını güçlendirerek siber saldırı, veri ihlalleri ve fidye yazılımlar gibi tehditlere karşı önlem almaları uzun vadede sürdürülebilir büyüme elde etmeleri açısından büyük bir öneme sahiptir.

ÜÇÜNCÜ BÖLÜM
BİLİŞİM SEKTÖRÜNDE FAALİYET GÖSTEREN KOBİLERDE SİBER GÜVENLİK UYGULAMALARI ÜZERİNE BİR ARAŞTIRMA

3.1. Konya'da Bilişim Sektöründe Faaliyet Gösteren KOBİ'ler İle İlgili Genel Bilgiler

Küreselleşme süreçlerinin hız kazanması, piyasalardaki rekabetin daha da yoğunlaşmasına sebep olmuştur. Devlet müdahalesinin azalması, yabancı yatırımların ve mal ile hizmetlerin serbest dolaşımının önünü açarak firmaların daha düşük maliyetli ve kaliteli ürünler üretmelerini teşvik etmektedir. Artan rekabet ile birlikte kalite ve verimlilik önem kazanırken, bu durum teknolojik yatırımların artmasına yol açmıştır. Bu gelişmeler sonucunda, firmalar yeni finansal kaynaklar oluşturma gerekliliğiyle karşı karşıya kalmaktadır. Rekabetin her geçen gün daha da yoğunlaştığı bu ortamda, firmalar pazarda rekabet edebilmek için kendi güçlü yönlerini ön plana çıkararak alternatif stratejiler geliştirebilecektir (Aras ve Müslümov, 2002: 23).

Bilgi teknolojisi (BT) sektörü, yazılım, donanım ve yarı iletken cihaz üreticilerinin yanı sıra internet ve benzeri hizmetleri sunan firmalardan oluşmaktadır (Çalış ve Sakarya, 2023: 773). Öte yandan, bilişim sektörünün ülke ekonomilerinin büyümesine sağladığı katkı her geçen gün artmaktadır. Genel amaçlı bir teknoloji olarak, bilgi teknolojilerinin bir ülkenin ekonomik gelişimi üzerindeki etkisi, sadece bilişim sektörünü değil, aynı zamanda sektörler arası dışsallıklar ve yayılma etkilerini de kapsamaktadır. Bu bağlamda, bilgi teknolojilerinin gayri safi yurtiçi hasıla (GSYİH) büyümesine doğrudan katkısı, giderek daha belirgin bir hale gelmektedir (Şişman ve Şişman, 2019).

2023 yılı itibarıyla küresel bilgi ve iletişim teknolojileri (BİT) pazarının büyüklüğü, %1,1 oranında bir artışla 4,45 trilyon dolara ulaşmıştır. Ancak, bilgi teknolojileri pazarı aynı dönemde benzer oranda bir daralma yaşarken, iletişim teknolojileri pazarı %4,1 oranında bir büyüme göstermiştir. 2024 yılına gelindiğinde, küresel BİT pazarının 4,8 trilyon dolara ulaşması beklenmektedir. Bunun ardından, yıllık %9 oranında bir büyüme ile 2027 yılına kadar pazarın 6,2 trilyon dolara ulaşması öngörülmektedir.

Türkiye'de KOBİ'ler, tüm işletmelerin %98'ini ve toplam istihdamın %71'ini oluşturmaktadır. KOBİ'ler, yapılarındaki esneklik sayesinde değişen piyasa koşullarına ve teknolojik gelişmelere hızlı bir şekilde uyum sağlarlar. Yenilikçi yönetim anlayışları, KOBİ'lere hızlı karar alma ve bu kararları çabucak uygulama imkânı sunmaktadır. Küçük ölçekli üretim yapıları sayesinde, ürün farklılaştırması gerçekleştirebilen KOBİ'ler, büyük işletmelere ara malı temin ederek tedarik zincirinin tamamlanmasına katkı sağlamaktadır. Bu nedenle, KOBİ'ler sadece küçük ölçekli işletmeler olarak değerlendirilmemelidir. Aksine, ekonomik kalkınmanın önemli bir motoru olan KOBİ'ler, ülkelerin gelişim stratejilerinin vazgeçilmez bir parçasıdır. Faaliyet gösterdikleri bölgelerde istihdamı artırarak göçü engelleyen, girişimcilik potansiyelini harekete geçirerek kalifiye işgücü ihtiyacına önemli katkılar sunan KOBİ'ler, ekonominin dinamik unsurlarını oluşturmaktadır (Özçelik, 2023: 2).

Konya'daki KOBİ'ler, mevcut kaynaklarıyla üretim süreçlerini başarıyla gerçekleştirmiş ve ürettikleri ürünleri uluslararası pazarlara ihraç edebilecek düzeye ulaşmıştır. 2023 yılı itibarıyla Konya'nın ihracat hacmi, bir önceki yıla kıyasla %1,4 oranında bir artış göstererek 3.305 milyon dolar olarak gerçekleşmiştir. Böylece, Konya, tarihindeki en yüksek yıllık ihracat değerine ulaşmıştır. Bu performans, Konya'nın Türkiye'nin toplam ihracatındaki payını artırmasına olanak sağlamış ve il, en fazla ihracat yapan iller sıralamasında 10. sırada yer almıştır. Son 20 yıl göz önünde bulundurulduğunda, 2000'li yılların başlarında 100 milyon dolar seviyelerinde olan ihracat rakamı, 2023 yılı itibarıyla 3 milyar doları aşmış durumdadır (KTO, 2023).

Bilişim sektörü, günümüz dünyasında hayatın her alanında köklü değişiklikler yaratan dinamik ve hızla gelişen bir disiplin olarak karşımıza çıkmaktadır. Yazılım geliştirme, yapay zekâ veri analitiği ve bulut bilişim gibi alanlardaki ilerlemeler, bireylere daha akıllı, hızlı ve verimli çözümler sunma imkânı tanımaktadır. Ayrıca, dijital dönüşümün etkisiyle şirketler, küresel ölçekte rekabet avantajı elde etmek amacıyla bilişim teknolojilerini stratejik bir şekilde kullanmaktadır. Bilişim sektörü, aynı zamanda yeni iş kolları ve fırsatlar; toplumsal yapıyı dönüştüren güçlü bir itici güç olarak öne çıkmaktadır. Diğer sektörlerde olduğu gibi bilişim sektöründe güçlü ve zayıf yönler bulunmaktadır. Tablo 3.1' de Konya'da yazılım sektörüne ait swot analizi yer almaktadır.

Tablo 3.1 Konya'da Yazılım Sektörünün GZFT Analizi

Güçlü Yönler	Zayıf Yönler
• **Konya'da yazılım sektörünün gelişmesinde önemli katkısı olan üniversitelerin varlığı,** • **Konya'da Kurulu olan Teknokent bünyesinde çok sayıda yazılım sektöründe faaliyet gösteren firma varlığı,** • **Konya'nın yüksek genç nüfusa sahip olması,** • **Konya'da Güçlü bir sanayi altyapısının olması,** • **Güçlü ekonomik göstergeler ve büyüme eğilimi.**	• Kamu-Üniversite-Sanayi İşbirliği'nin yeterince gelişmemiş olması, • Ar-Ge ve inovasyona yönelik yatırımların ve çalışmaların yeterli olmaması, • Nitelikli işgücünün yetersizliği, • Fikri Mülkiyet Hakları ile ilgili ihlaller • Girişim sermayesi yetersizliği, • Müşterilerin ne talep ettiklerini bilmemeleri, • Takım çalışmasının yetersizliği • BT ile ilgili enformel eğitimlerin olmaması. •
Fırsatlar	**Tehditler**
• **Konya'nın son yıllarda yazılım firmaları sayısında hızlı bir yükseliş gözlemlenmesi,** • **Konya'da Nitelikli insan kaynağı varlığı ile şehir dışı yazılım firmalarının şube açma talebinin artması,** • **Konya'nın artan nüfusu ve sahip olduğu üniversitelerin geleceğe yönelik nitelikli işgücü bakımından bir potansiyel oluşturması,** • **Sektöre yönelik teşvik ve desteklerin varlığı,** • **Yeniliklere hızlı adapte olan tüketici,** • **Yenilikçi ürünlerin giderek artması,** • **Ucuz işgücü.**	• Yazılım sektöründe ithalatçı bir konumda bulunulması, • Ankara'nın Konya'ya yakınlığının, Ankara'yı daha cazip kılması ve bunun rekabetçiliğe olan etkisi, • Ar-Ge kültürünün istenilen düzeyde olmaması, • Fiyat odaklı yüksek rekabetten dolayı düşen kar marjları ve azalan yatırım eğilimi, • Makro ve mikro ekonomik belirsizlikler. • Ürün ve markalaşma konusunda geniş bir vizyon ortaya konmaması, • Beyin göçü • Piyasaların yeterince olgunlaşmaması.

Kaynak: (Erenler, 2019: 25).

Konya'da yazılım sektörü, üniversiteler ve Teknokent gibi önemli altyapılara sahip olup, genç nüfus ve güçlü sanayi altyapısı gibi avantajlarla desteklenmektedir. Bu unsurlar, sektöre güçlü bir ivme kazandırmaktadır. Ancak, kamu-üniversite-sanayi iş birliğinin yetersizliği, Ar-Ge ve inovasyon yatırımlarının eksikliği, nitelikli işgücü sıkıntısı ve fikri mülkiyet ihlalleri gibi zayıf yönler sektörü olumsuz etkilemektedir. Bununla birlikte, Konya'da yazılım firmalarının sayısındaki artış, nitelikli insan kaynağının varlığı ve şehir dışı firmaların yatırım yapma isteği, sektöre yönelik önemli fırsatlar sunmaktadır. Ayrıca, devlet destekleri, yenilikçi ürünler ve ucuz işgücü gibi faktörler sektörü destekleyen unsurlar arasındadır. Ancak, sektördeki ithalat bağımlılığı, Ankara'nın yakınlığından kaynaklanan rekabet avantajı, Ar-Ge kültürünün zayıf olması ve yüksek rekabet nedeniyle kar marjlarının düşmesi gibi tehditler bulunmaktadır. Bunun yanı sıra, beyin göçü ve piyasaların yeterince olgunlaşmaması da sektörü tehdit eden diğer faktörlerdir.

3.2. Konya'da Bilişim Sektöründe Faaliyet Gösteren KOBİ'lerin Kullandıkları Dijital Dönüşüm Uygulamaları

Günümüzde teknolojinin hızla ilerlemesiyle birlikte, bilgi teknolojilerinin işletmeler için kullanımı her sektörde ve her büyüklükteki firma için kaçınılmaz bir hale gelmiştir. Bilgi teknolojilerinin işletmelerin farklı alanlarında kullanımı, bilgisayarlar ve dijital sistemlerin ilk kullanımına dayanan bir süreçte sürekli olarak artış göstermektedir. Değişen ve gelişen rekabet koşulları, işletmelerin ihtiyaçlarının çeşitlenmesine ve artmasına yol açmıştır. Bu durum, firmaların farklı iş fonksiyonlarının etkin ve uyumlu bir şekilde bir arada yürütülmesini gerektiren bir ortam yaratmıştır. Çalışmaya katılan KOBİ'lerin dijital dönüşüm süreçlerinde kullandıkları uygulamalar hakkında kısa açıklamalar sunulmuştur. Söz konusu bu uygulamalar, KOBİ'lerin iş yapış biçimlerini dönüştürerek, teknolojinin sunduğu fırsatları en verimli şekilde değerlendirmelerine katkıda bulunmaktadır.

Enterprise Resource Planning (ERP): Kurumsal Kaynak Planlama (ERP) sistemi, bir şirketteki iş süreçlerini ve işlemlerini entegre etmek ve optimize etmek için tasarlanmış bir kurumsal bilgi sistemidir (Moon, 2007: 235). Kurumsal Kaynak Planlaması (ERP), İngilizce "Enterprise Resource Planning" teriminin kısaltması olup, işletmelerdeki farklı işlevlerin birleştirilerek merkezi bir noktadan izlenmesini sağlamaktadır. Daha geniş anlamıyla; satın alma, üretim, stok kontrolü, muhasebe, finans, kalite yönetimi, insan kaynakları, satış ve lojistik gibi alanlardaki verilerin tek bir veritabanında entegre edilmesini ve tüm organizasyon çapında bu verilere ulaşılmasını mümkün kılmaktadır. ERP sistemleri, her departman için gerekli bilgi akışını sağlayarak, işletmelerin verimli bir şekilde yönetilmesine olanak tanımaktadır (Çelebi ve Bulut, 2016: 167). ERP sistemini başarıyla uygulayan şirketler, ürün dağıtımını daha verimli hale getirme, bilgi yönetimini iyileştirme, müşteri memnuniyetini artırma gibi avantajlar elde etmektedir. Ayrıca, gelecekteki talepler yerine mevcut müşteri ihtiyaçlarına odaklanarak üretim yapabilme, envanterdeki malzeme miktarını azaltma ve ürün fiyatlarını hızlı bir şekilde belirleme gibi faydalar da sağlamaktadır. ERP, bir şirketin tüm departmanlarını bir araya getirerek, bütünsel bir bilgi yönetim sistemi sunmakta ve tüm iş süreçlerini kapsamaktadır (Acar vd., 2004: 3).

Zoho: Zoho, KOBİ'lere yönelik web tabanlı yazılımlar sunan bir uygulamadır. Bu uygulamalar arasında; kelime işlemci, elektronik tablo, sunum hazırlama, veritabanı yönetimi, müşteri ilişkileri yönetimi ve sipariş takibi gibi programlar bulunmaktadır. Zoho'nun internet tabanlı yapısı sayesinde, farklı bilgisayarlar ve işletim sistemleriyle uyumlu şekilde çalışabilmektedir. Ayrıca, Microsoft Office ve OpenOffice gibi uygulamalara ait dosya formatlarıyla da uyumludur. Kullanıcılar, Zoho platformunda çevrimiçi olarak belgeler ve sunumlar oluşturup düzenleyebilmekte, bu ürünleri birleştirerek, Zoho veya diğer bağlı depolama hizmetlerinde saklayabilmektedir. Ayrıca, kullanıcılar istedikleri zaman kişisel cihazlarıyla Zoho servisleri arasında veri senkronizasyonu yapabilmektedir (Sevli, 2011: 31).

Amazon Web Services (AWS): Amazon Web Services (AWS), 2006 yılında piyasaya sürülen ve bulut bilişim alanında öncü olan bir hizmet sağlayıcısıdır. AWS, yalnızca yüksek kaliteli bulut hizmetleri sunmakla kalmaz, aynı zamanda müşterilerinin verilerinin gizliliğini, bütünlüğünü ve erişebilirliğini sağlamak adına güçlü güvenlik önlemleri de sunmaktadır (Narula vd.,2015: 503). Bulut depolama, veritabanı hizmetleri, veri analizi, nesnelerin interneti, mobil bilişim ve kurumsal hizmetler gibi geniş bir yelpazede bilişim hizmetleri sunan AWS, organizasyonların daha hızlı büyümesini, maliyetlerini azaltmasını ve operasyonlarını ölçeklendirmesini mümkün kılmaktadır. Bu özellikleriyle AWS, sektördeki en köklü ve en yaygın kullanılan bulut platformalarından biri olarak dikkat çekmektedir (Mufti vd.,2020: 3).

Azure*:* Azure, Microsoft tarafından geliştirilen ve 140'tan fazla ülkede 54 farklı servis sağlayıcısı ile iş birliği yapan, bulut bilişim tabanlı bir çalışma platformudur. Azure, çok çeşitli bilişim hizmetleri sunarak, işletmelerin ve geliştiricilerin çeşitli ihtiyaçlarını karşılamaktadır. Microsoft Bilişsel Hizmetler, Azure platformu üzerinde yer alan ve yapay zekâ alanındaki sorunlara yönelik çözümler geliştirmeyi amaçlayan bir algoritmalar kütüphanesidir. Bu hizmet, dil işleme, makine öğrenimi, arama ve görüntü işleme gibi işlevleri içermektedir. Alanında derin uzmanlık gerektirmeden yazılım geliştiricilerin bu teknolojilerden faydalanabilmesi için tasarlanmıştır. Bilişsel Hizmetler, geliştiricilere API ve SDK formatında sunulmakta olup, kullanıcıların mevcut uygulamalarındaki problemleri çözmelerine

veya uygulamalarını daha akıllı halet getirmelerine olanak tanımaktadır. Bu API'lerde, uygulamanın nasıl kullanılacağı detaylı bir şekilde açıklanmakta, ancak arka planda çalışan algoritmaların detaylarına yer verilmemektedir (Yılmazer ve Solak, 2020: 3).

Github: GitHub, sürüm kontrolü ve işbirlikçi yazılım geliştirme amacıyla kullanılan web tabanlı bir platformdur. Geliştiricilere, yazılım projelerinin kaynak kodlarını yönetme ve paylaşma imkânı sunmaktadır. GitHub, sürüm kontrolü için dağıtılmış bir sistem olan Git'i kullanarak, yazılım geliştirme süreçlerinde kaynak kodundaki değişikliklerin izlenmesini sağlamaktadır. Çekme istekleri, dallanma ve sorun izleme gibi özellikler, GitHub'ı hem bireysel hem de takım projeleri için etkili bir araç haline getirmektedir. Ayrıca, GitHub, açık kaynaklı projelere katkı sağlamayı kolaylaştırarak, dünya çapındaki geliştiricilerin çeşitli projelere etkin bir şekilde iş birliği yapmalarını ve katkıda bulunmalarını mümkün kılmaktadır (Chacon ve Straub, 2014: 131).

Digital Ocean: DigitalOcean, 2011 yılında kurulmuş olan bir bulut hizmeti sağlayıcısıdır. DigitalOcean, PaaS olarak hizmet sunmaktadır. Kullanıcı dostu bir arayüze sahip olan DigitalOcean "Droplet" adı verilen sanal sunucular aracılığıyla, farklı ihtiyaçlara yönelik özelleştirilmiş sanal makineler oluşturulmasına olanak tanımaktadır. Bu sunucular, belirli gereksinimlere göre yapılandırılabilmekte ve esnek bir kullanım imkânı sağlamaktadır (Eren, 2017: 32).

Jira: Proje ve süreç yönetimi işlemleri için firmaların kullanmış olduğu pek çok uygulama vardır. Bu uygulamaların belki de en önemlilerinden bir Jira'dır. Kullanım kolaylığı, stabil oluşu ve çevik yöntemleri destekliyor olması, Jira'nın yazılım geliştirme dünyasının vazgeçilmez iş takibi uygulamaları arasında yer almasına yol açmıştır. Bunun yanında, Jira pek çok farklı sektörde de kullanılmaktadır. Jira çevik yazılım geliştirme projelerinin planlanması noktasında esnek bir yapıya sahiptir (Borandağ ve Yücalar, 2020: 5).

Slack: Slack, özellikle yazılım geliştirme ekipleri arasında hızla benimsenmiş, modern bir iletişim platformudur. Slack, ekip içi mesajlaşmayı ve iletişimlerin arşivlenmesini kolaylaştırmakla kalmaz, aynı zamanda harici hizmetlerle ve botlarla entegrasyonu da destekleyerek, kullanım alanını genişletmektedir. Bu entegrasyonlar,

yazılım geliştirme süreçlerinde giderek daha önemli bir dol oynamakta, ekiplerin verimli bir şekilde çalışmasına ve iş birliği yapmasına olanak tanımaktadır (Lin vd., 2016: 333).

Bitbucket: Bitbucket, yazılım geliştirme süreçlerinde kod depolama ve sürüm kontrolü sağlamak amacıyla kullanılan bir platformdur. Modern yazılım geliştirme yaklaşımlarına dayalı olarak, işlevsel, güvenilir, kullanıcı dostu, genişletilebilir ve entegre edilebilir sistemlerin oluşturulmasına olanak tanımaktadır. Bu tür sistemler, düşük risk ve kabul edilebilir maliyetlerle optimize edilmiş çözümler sunmaktadır. Atlassian Bitbucket, sürümlerin izlenmesi ve kontrol edilmesi için tercih edilen bir araçtır. Bitbucket, bir veya birden fazla dosyada yapılan değişiklikleri kaydederek, belirli bir eski sürüme dönmeyi, projenin önceki bir durumuna geri gitmeyi, zaman içindeki değişiklikleri incelmeyi, bir modülün çalışmayı durdurmasına neden olan değişiklikleri tespit etmeyi veya kodda oluşan bir hatanın kaynağını belirlemeyi mümkün kılmaktadır (Lavrov, 2017: 540).

3.3. Alan Araştırması

3.3.1. Araştırmanın Amacı

Bilişim teknolojilerinin hızla ilerlemesiyle birlikte bilgisayar ve internet kullanımının yaygınlaşması, bu araçları modern yaşamın ayrılmaz bir parçası haline getirmiştir. Ancak, bilişim ve internetin küresel ölçekte hızla yayılması, kullanıcılara bir yandan pratiklik ve özgürlük sağlarken, diğer yandan ortaya çıkan güvenlik açıkları nedeniyle sistemlerin kötüye kullanılmasına yol açabilmektedir (Aslay, 2017: 24). Son yıllarda siber saldırılar, yalnızca bireysel bilgisayarları hedef almakla kalmayıp, aynı zamanda devletlerin bilgisayar sistemleri, iletişim altyapıları, askeri tesisleri ve silah sistemleri, ulaşım ağları ve altyapıları, enerji sistemleri ile sağlık hizmetleri gibi kritik alanları da tehdit etmektedir. Bu bağlamda, siber tehditlerin önemi, önümüzdeki yıllarda da artarak devam edecektir (Aytekin, 2015: 19). Bu çerçevede, alınacak önlemlerin hızla planlanması, acil durum senaryolarının oluşturulması ve güçlü savunma sistemlerinin hayata geçirilmesi büyük bir önem arz etmektedir (Goodman, 2008: 28).

Bu araştırmanın temel amacı, Konya ilinde bilişim sektöründe faaliyet gösteren KOBİ'lerin siber güvenlik farkındalık seviyelerini belirlemek ve bu farkındalık seviyelerinin katılımcıların demografik özelliklerine göre farklılık gösterip göstermediğini incelemektir.

3.3.2. Araştırmanın Önemi

Günümüzde, siber saldırılar kurumlar ve şirketler için giderek daha karmaşık hale gelmekte ve bu durum ciddi güvenlik riskleri yaratmaktadır. Bu saldırıların olumsuz etkileri göz önünde bulundurulduğunda, bu tehditlere karşı etkili önlemler alınması gerektiği açıktır. Teknolojik gelişmelerin hızla ilerlemesiyle birlikte, siber korsanların daha gelişmiş yöntemler ve teknikler kullanabildikleri de gözlemlenmektedir. Bu nedenle, kurumların saldırılara maruz kalmadan önce ya da saldırı anında etkin bir şekilde yanıt verebilecek sağlam bir siber güvenlik stratejisine sahip olmaları büyük önem taşımaktadır. Bu bağlamda, siber güvenlik farkındalığının artırılması, güvenlik açıklarının önlenmesinde ve siber tehditlerle mücadelede kritik bir rol oynamaktadır (Karakaya, 2022: 2).

Bu araştırma Konya'da bilişim sektöründe faaliyet gösteren KOBİ'lerin siber güvenlik farkındalığı ile ilgili mevcut durumlarını incelemektedir. Bu bağlamda araştırma, işletmelerin siber güvenlik yönetimindeki karşılaştıkları sorunları belirlemek ve bu sorunlara yönelik çözüm önerileri geliştirmek açısından önemli bir yer tutmaktadır. Ayrıca, araştırma, ilgili literatüre katkı sağlama amacıyla da değer taşımaktadır.

3.3.3. Araştırmanın Sınırlılığı

Araştırmanın sınırlı bir zaman diliminde yapılması ve maliyet unsurları gibi kısıtlamalar nedeniyle Konya il merkezinde bulunan KOBİ'ler ile sınırlı tutulmuştur. Araştırma çerçevesinde, yüz yüze görüşmelerin gerçekleştirilebilmesi amacıyla Konya ilindeki KOBİ'ler arasından seçilen işletmelerle iletişime geçilmiştir. Örneklem grubunu yalnızca bilişim sektöründe faaliyet gösteren KOBİ çalışanları oluşturmuştur.

3.3.4. Etik Kurul Onayı

"Dijital Dönüşüm ve Siber Güvenlik: Konya'da Bilişim Sektöründe Faaliyet Gösteren KOBİ'ler Üzerine Bir Araştırma" başlıklı yüksek lisans tez çalışmasında bilimsel araştırma ve yayın etiğine uyulmuştur. Çalışma için Necmettin Erbakan Üniversitesi Sosyal Bilimler Enstitüsü'nden 05/01/2024 tarih ve 2024/13 sayı ile etik kurul izni alınmıştır.

3.3.5. Araştırmanın Yöntemi

Yöntem kısmında, tez çalışması kapsamında yapılan nicel ve nitel araştırmaya yönelik bilgiler bulunmaktadır.

3.3.5.1. Nicel Araştırma Yöntemi

Nicel araştırma yöntemleri, sayılara odaklanarak, özellikle kitlelerin ne söylediğini ne yaptığını ve ne düşündüğünü genelleştirmeye yönelik veri toplar ve analiz eder. Bu yöntemler, geniş bir örneklem üzerinden elde edilen verilerle, belirli eğilimleri ve ilişkileri ortaya koymayı amaçlar (Berber, 2017: 72). Bu araştırmada anket kullanılmasının sebebi; bilişim sektöründe faaliyet gösteren KOBİ çalışanlarının, araştırmacının kişisel eğilimlerinden etkilenmeden siber güvenlik konusundaki düşüncelerini açıklayabilmesi ve çok sayıda katılımcıdan kısa sürede bilgi toplanabilmesidir. Anket, genellikle bir sorgulama aracığı olarak tanımlanmakta olup, örneklemden elde edilecek verilere ulaşmak amacıyla kullanılan, standartlaştırılmış ifadelerden oluşan bir veri toplama yöntemidir (Ural ve Kılıç, 2013: 53). Bu araç, katılımcıların araştırılan konu veya olguya ilişkin düşüncelerini, eğilimlerini, beklentilerini, tercihlerini ve algılarını ortaya koyabilmek için uygulanmaktadır (Salı, 2018: 136).

3.3.5.1.1. Nicel Araştırmanın Hipotezleri

Araştırmanın hipotezleri, Konya ilinde bilişim sektöründe faaliyet gösteren KOBİ'lerin siber güvenlik farkındalık düzeylerinin, katılımcıların demografik özelliklerine göre farklılık gösterip göstermediğini incelemek amacıyla oluşturulmuştur.

H1: Çalışanların siber güvenlik farkındalık düzeyleri cinsiyete göre farklılık göstermektedir.

H2: Çalışanların siber güvenlik farkındalık düzeyleri yaşa göre farklılık göstermektedir.

H3: Çalışanların siber güvenlik farkındalık düzeyleri eğitim seviyesine göre farklılık göstermektedir.

H4: Çalışanların siber güvenlik farkındalık düzeyleri işletmedeki çalışma süresine göre farklılık göstermektedir.

H5: Çalışanların siber güvenlik farkındalık düzeyleri işletmedeki pozisyonuna göre farklılık göstermektedir.

3.3.5.1.2. Nicel Araştırmanın Evreni ve Örneklemi

Araştırmanın evrenini; Konya ilinde bilişim sektöründe faaliyet gösteren KOBİ çalışanları oluşturmaktadır. Araştırmanın örneklemini ise, anketi cevaplamayı kabul eden 228 KOBİ çalışanı oluşturmaktadır. Kolayda örnekleme yöntemi kullanılarak elde edilen örneklem grubu üzerinden gerçekleştirilmiştir. Kolayda örnekleme, araştırmacının erişimi ve kolaylığı doğrultusunda belirlediği örneklem grubuyla gerçekleştirilen bir yöntemdir (Burns ve Bush, 2015:226). Evrenin tamamına ulaşılamadığı durumlarda, evreni temsil edecek en iyi örneklem sayısına ulaşmak önemlidir.

Alanyazında, ulaşılması gereken örneklem büyüklüğü hakkında çeşitli ölçütler ve fikirler bulunmaktadır. Örneklemin büyüklüğü, faktör veya madde sayısı gibi bağıl ölçütlere göre tahmin edilebilmekle birlikte genelde örneklem büyüklüğünün ölçekte yer alan madde sayısının beş on katı civarında olması gerekmektedir (Kass ve Tinsley, 1979; Kline, 1994; Tavşancıl, 2005). Kline'e göre (1994) mutlak ölçüt olarak 200 kişilik örneklem yeterlidir fakat daha büyük örneklemler ile çalışmak daha uygun olmaktadır. Comrey ve Lee (1992) ise 100 kişinin zayıf, 200 kişinin orta, 300 kişinin iyi, 500 kişinin çok iyi ve 1000 kişinin mükemmel olduğunu ifade etmiştir. Buradan hareketle bu araştırmanın çalışma grubu; ölçülen özelliğin ranjını temsil edebilecek nitelikte bir örnekleme ulaşabilmek amacıyla, kolayda örnekleme yöntemiyle

belirlenmiş ve araştırmanın verileri, Konya ilinde bilişimde sektöründe faaliyet gösteren KOBİ çalışanlarında 228 katılımcıdan elde edilmiştir.

3.3.5.1.3. Nicel Araştırmanın Veri Toplama Araçları

Araştırma, veri toplama aracı olarak anket yöntemini kullanarak gerçekleştirilmiştir. Bilişim sektöründe faaliyet gösteren KOBİ çalışanlarının siber güvenlik farkındalıklarını ölçmeyi amaçlayan bu çalışmada, katılımcılara anket soruları yöneltilmiştir. Anket formu oluşturulurken Saeed (2023), Hasan ve diğerleri (2021), Ngoma (2019), Redekop (2016), Arpaci ve Sevinç (2022) çalışmalarından yararlanılmıştır.

Araştırma kapsamında kullanılan anket, iki bölümden oluşmaktadır. İlk bölüm, katılımcıların demografik bilgilerine ilişkin ifadeleri içermektedir. Bu bölümde, katılımcıların cinsiyet, yaş, eğitim durumu, işletmedeki çalışma süresi ve pozisyonu gibi kişisel özelliklerine dair sorulara yer verilmiştir. İkinci bölüm ise, katılımcıların "Siber Güvenlik Farkındalığı" düzeylerini ölçmeyi amaçlayan 32 maddelik bir ölçeğe dayalı ifadelerden oluşmaktadır. Araştırmada, katılımcıların cevapları 5 dereceli Likert ölçeği üzerinden toplanmıştır. Likert ölçeği, şu şekilde derecelendirilmiştir: 1 – Kesinlikle Katılmıyorum, 2 – Katılmıyorum, 3 – Kararsızım, 4 – Katılıyorum, 5 – Kesinlikle Katılıyorum.

3.3.5.2. Nitel Araştırma Yöntemi

Nitel araştırmayı, "*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 tanımlamak mümkündür (Yıldırım ve Şimşek, 2008, s. 39). Nitel araştırma yöntemi, araştırmacıya araştırma sürecinin her aşamasında esneklik sunarak, yeni yöntemler ve yaklaşımlar geliştirme imkânı tanımaktadır. Bu yöntem, araştırmanın kurgusunda yapılacak değişikliklerle uyumlu olup, genellikle keşfedici bir özellik taşır. Keşfedici özelliğe sahip araştırmalar, daha önce az çalışılmış konuları derinlemesine inceleyerek, bu alanlarda yeni bilgiler elde edilmesini sağlamaktadır (Neuman, 2012: 228). Bu araştırmada yarı yapılandırılmış mülakat tekniğinin kullanılmasının nedeni,

araştırmacının konuya dair derinlemesine bilgi edinmesi amacını taşımaktadır. Önceden belirlenmiş bir görüşme taslağına dayanarak gerçekleştirilen yarı yapılandırılmış mülakatlar, araştırmacıya daha sistematik ve karşılaştırılabilir veriler elde etme imkânı sağlamaktadır (Yıldırım ve Şimşek, 2004). Araştırmada kullanılan yarı yapılandırılmış görüşme tekniğinde, araştırmacıya görüşme öncesinde hazırladığı bir dizi soru rehberlik etmektedir. Bu görüşme yaklaşımı, görüşme sırasında irdelenecek bir sorular veya konular listesini kapsamaktadır (Yıldırım ve Şimşek, 2016: 130).

3.3.5.2.1. Nitel Araştırma Veri Toplama Aracı

Nitel araştırmalarda sıklıkla yararlanılan yarı yapılandırılmış görüşme tekniği kullanılarak, görüşme yapılan kişilerin olay ve olguları anlamlandırmalarını, duygu ve düşüncelerini anlamak ve daha derin bilgi edinmek amaçlanmıştır (Yıldırım ve Şimşek, 2011).

Nitel araştırmanın amacı doğrultusunda işletmelerin yöneticileri ve/veya müdürü siber güvenlik seviyelerini tespit etmeye yönelik 13 soruluk yarı yapılandırılmış görüşme formu hazırlanmıştır. Yarı yapılandırılmış görüşme soruları hazırlanırken alanyazın taraması yapılmış, uzman görüşü alınarak değerlendirilmiştir. Seçilen işletmelerin yöneticileri ve/veya müdürü ile yarı yapılandırılmış görüşmeler gerçekleştirilmiştir. Seçilen işletmeler, bilişim sektöründe tanınan, belirgin bir vizyon ve misyona sahip olup, yeniliklere açık olma özelliklerine dikkat edilerek belirlenmiştir.

Görüşme formu, aşağıda belirtilen başlıklar altında yer alan soruları içermektedir.

1. İşletmeniz kaç yıldır faaliyette bulunmaktadır?
2. İşletmenizdeki pozisyonunuz nedir?
3. İşletmenizde kaç çalışan var?
4. Dijital cihazları ve interneti kullanma konusundaki beceri düzeyinizi nasıl değerlendirirsiniz?
5. Hassas verilere erişiminiz sınırlı mı?
6. Verilerinize kimler erişim sağlayabilir?

7. İşlemenizde siber güvenlik farkındalığından kim sorumlu?
8. İşletmenizde siber güvenlik farkındalığı girişimlerinin amacı nedir?
9. Çalışanlarınıza rutin olarak ne tür siber önleme eğitimi ve öğretimi sağlıyorsunuz?
10. Bir siber saldırı meydana gelirse acil durum planınız ne olur?
11. Siber güvenlik konusunda en çok zorlandığınız şey nedir?
12. İşletmenizde güvenlik farkındalığını artırmak için geliştirmek istediğiniz teknikler nelerdir?
13. Siber güvenlik farkındalığında hangi özelliklerin iyileştirilmesi gerekiyor?

3.3.5.2.2. Nitel Araştırmanın Katılımcıları

Nitel araştırmanın örneklemi, olasılıklı olmayan amaçlı örnekleme yöntemidir. Olasılıklı olmayan amaçlı örnekleme yönteminde, mülakat gerçekleştirilecek katılımcıların araştırma konusu ile doğrudan ilişkili olup olmadıkları büyük önem taşır (Neuman, 2012: 320). Bu noktadan hareketle araştırmacının çalışmanın amaçlarına uygun olarak kendi kararına göre seçtiği amaçlı örnekleme yönteminden yararlanılmıştır.

Hennink ve Kaiser (2022: 9), yaptıkları araştırmada, nitel araştırma yöntemlerinden mülakat tekniği kullanılarak örneklem doygunluğuna ulaşabilmek için 9-17 kişi arasında belirlenen örneklem sayısının yeterli olduğunu belirtmişlerdir. Bu bulguya dayanarak, belirli koşullar altında, nitel araştırmalarda 18 kişilik bir örneklemin veri doygunluğuna ulaşmak için yeterli olabileceği ifade edilmektedir.

Araştırmada, Konya ilinde bilişim sektöründe faaliyet gösteren 707 KOBİ içerisinden 20 işletme yöneticileri ve/veya müdürü belirlenerek, görüşmeyi 20 işletme yöneticileri ve/veya müdürü gerçekleştirilmesi hedeflenmiştir. Uygulama aşamasında 2 işletme yöneticileri ve/veya müdürü araştırmaya katılmaktan vazgeçmiş, araştırma 18 yöneticileri ve/veya müdürü ile devam etmiştir.

Bilişim sektörü, hızla dijitalleşen dünyada büyük bir öneme sahiptir ve hem yerel hem de küresel ölçekte ekonomik ve toplumsal yapıları şekillendirmektedir.

Teknolojinin her geçen gün daha fazla hayatımıza entegre olmasıyla birlikte, bilişim sektörü büyük işletmelerin yanı sıra KOBİ'ler için de kritik bir işlev taşımaktadır. Özellikle Konya gibi gelişen illerde, bilişim sektörü, KOBİ'lerin sürdürülebilirliklerini ve rekabet gücünü artıran önemli bir alan olarak ön plana çıkmaktadır. Konya ili 2000'den 2023'e yapılan ihracat rakamı 39 kat büyümüştür.2023 yılında Konya, 3,36 milyar dolar ihracatla Türkiye genelinde 11. sırada yer almıştır. Bu rakam, 26 ilin toplam ihracatından daha fazladır. Konya, 180'den fazla ülkeye ihracat yapmaktadır. 2023 yılı sonu itibariyle Konya'da 752 adet yatırım teşvik belgesi düzenlenmiştir ve Türkiye'de 5. sıradadır (KTO, 2024). Konya'da bilgi ve iletişim sektöründe faaliyet gösteren girişimlerin sayısında sürekli bir artış gözlemlenmektedir. Konya ilinde bilişim sektöründe faaliyet gösteren girişimlerin sayısı 2019-2023 yılları arasında %88.02 oranında artmıştır (TÜİK, 2024). Bu da sektörün Konya'da önemli bir büyüme kaydettiğini göstermektedir. Bu bağlamda, sektördeki işletmelerin siber güvenlik farkındalık seviyelerini incelemek, dijital tehditlere karşı daha güvenli bir ortam oluşturulmasına katkıda bulunacak önemli bir adımdır.

3.3.5. Araştırmanın Analizi

Araştırma verileri, önce nicel yöntem kullanılarak daha sonra da nitel yöntem kullanılarak analiz edilmiştir. Nicel ve nitel verilerin analizinden aşağıda bahsedilmiştir.

3.3.5.1. Nicel Verilerin Analizi

Bu çalışmanın nicel bölümünde, 228 katılımcıya; 5 adet ***Demografik Bilgi*** ifadesi ve 5'li likert tipinde ***Siber Güvenlik Farkındalığı Ölçeği (SGFÖ)***'ne ait 32 ifade yöneltilmiş ve alınan cevaplar IBM SPSS Statistics 23 paket programında analiz edilmiştir.

Analiz süreci öncesinde ilk olarak, tanımlayıcı bulgulara bakılmış ve yorumlanmış, daha sonra ölçeğe verilen cevapların geçerliğine bakılarak Açımlayıcı Faktör Analizi (AFA) ve AFA bulgularına göre Doğrulayıcı Faktör Analizi (DFA) yapılmıştır. Faktör analizleri sonucunda elde edilen alt boyutlara göre güvenirlik değerlerine bakıldıktan sonra katılımcıların ölçekteki ifadelere verdikleri cevapların

normallik durumuna bakılarak ilişkisel analizlerde kullanılacak yöntemlerin parametrik veya parametrik olmayan yöntemler olmasına karar verilmiştir.

İlişkisel analizler sürecinde ise; iki gruptan oluşan kategorik değişkenler ile sürekli değişkenler arasındaki farklılaşmanın görülebilmesi için normal dağılım göstermeyen değişkenlerde parametrik olmayan yöntemlerden Mann Whitney U Testi, normal dağılım gösteren değişkenlerde parametrik yöntemlerden Bağımsız Örneklem T Testi kullanılmış, üç veya daha fazla kategorisi olan kategorik değişkenler ile sürekli değişkenler arasındaki farklılaşmanın görülebilmesi için normal dağılım göstermeyen değişkenlerde Kruskal Wallis Testi, normal dağılım gösteren değişkenlerde Tek Yönlü Anova Testi kullanılmıştır. Üç veya daha fazla kategorisi olan kategorik değişkenlerde, istatistiki olarak anlamlı farklılaşmanın kaynağının görülebilmesi için en uygun Post Hoç testleri yapılmıştır. Ayrıca son olarak ölçeğin boyutları arasındaki ilişkinin görülebilmesi için Spearman Korelasyon Analizi yapılmıştır.

Tüm analizlerde anlamlılık (p) değeri 0,05 olarak kabul edilmiş ve p değerinin 0,05'den küçük olduğu analiz bulgularında istatistiki bir anlamlılık olduğu, aksi durumda istatistiki olarak anlamlılık olmadığı kabul edilmiştir.

3.3.6.2. Nitel Verilerin Analizi

Verilerin toplanmasından sonra elde edilen verilerin çözümlenmesi aşamasına geçilmiştir. Mülakat yapılan her bir katılımcıya K1 ve K18 arasında kod numaraları verilmiştir. Katılımcılardan alınan cevaplarda herhangi bir değişiklik yapılmamıştır. Yarı yapılandırılmış mülakat tekniğinden elde edilen verilerde amaç genellemelere varmaktan ziyade katılımcıların bakış açılarının ve görüşlerinin açığa çıkmasını sağlamaktır. Mülakat tekniğinden elde edilen veriler MAXQDA Analytics Pro (Release 20.4.0) programına aktarılmış ve analiz süreci bu program üzerinden yürütülmüştür. Verilerin analizi için içerik analizi yöntemi kullanılmıştır.

Mülakat tekniğinden elde edilen nitel araştırma verilerinin analiz edilmesinde dört aşama bulunmaktadır (Yıldırım ve Şimşek, 2018: 243):

- Verileri kodlamak
- Temaları belirlemek

- Kodları ve temaları düzenlenmek
- Bulguları tanımlanmak ve yorumlanmaktır.

3.3.7. Araştırmanın Bulguları ve Değerlendirilmesi

Bulgular bölümünde, bu tez kapsamında gerçekleştirilen nicel ve nitel araştırmalar sonucunda elde edilen veriler sunulmaktadır.

3.3.7.1. Nicel Araştırma Bulguları

Araştırma kapsamında ilk olarak araştırmanın nicel bulgularına yer verilmiştir. Bu kapsamda gerçekleştirilen tüm aşamalar sırasıyla verilmiştir.

3.3.7.1.1. Tanımlayıcı Bulguları

Tanımlayıcı bulgular kapsamında, demografik bilgilerin ve ölçeğe verilen cevaplar incelenmiştir.

Bu bağlamda demografik bilgilerin tanımlayıcı bulguları Tablo 3.2'de olduğu gibidir.

Tablo 3.2. Demografik Bilgilerim Tanımlayıcı Bulguları

Demografik Bilgiler	Kategoriler	Sayı (n)	Oran (%)
Cinsiyet	Kadın	36	15,8
	Erkek	192	84,2
	Toplam	228	100,0
Yaş	18-25 Yaş Arası	86	37,7
	26-33 Yaş Arası	99	43,4
	34-41 Yaş Arası	24	10,5
	42-49 Yaş Arası	14	6,1
	50 Yaş ve Üzeri	5	2,2
	Toplam	228	100,0
Eğitim Durumu	İlköğretim	2	0,9
	Ortaöğretim (lise)	26	11,4
	Ön Lisans	60	26,3
	Lisans	117	51,3
	Lisansüstü	23	10,1
	Toplam	228	100,0
Çalışma Süresi	1 Yıldan Az	61	26,8
	1-3 Yıl Arası	78	34,2
	3-5 Yıl Arası	44	19,3
	5-15 Yıl Arası	34	14,9

	15-25 Yıl Arası	7	3,1
	25 Yıldan Fazla	4	1,8
	Toplam	228	100,0
İşletmedeki Pozisyon	Üst Düzey Yönetici	27	11,8
	Orta Düzey Yönetici	31	13,6
	Alt Düzey Yönetici	24	10,5
	Teknik Çalışan	135	59,2
	İdari Çalışan	11	4,8
	Toplam	228	100,0

Tablo 3.2'e göre; katılımcıların 36 (%15,8) tanesinin kadın, 192 (%84,2) tanesinin erkek olduğu, 86 (%37,7) tanesinin 18-25 yaş arasında, 99 (%43,4) tanesinin 26-33 yaş arasında, 24 (%10,5) tanesinin 33-41 yaş arasında, 14 (%6,1) tanesinin 42-49 yaş arasında ve 5 (%2,2) tanesinin 50 yaş ve üzerinde olduğu,

Katılımcıların eğitim durumlarına bakıldığında; 2 (%0,9) tanesinin ilköğretim mezunu, 26 (%11,4) tanesinin ortaöğretim (lise) mezunu, 60 (%26,3) tanesinin ön lisans mezunu, 117 (%51,3) tanesinin lisans mezunu, 23 (%10,1) tanesinin lisansüstü eğitim mezunu olduğu,

Çalışma süresinde göre katılımcıların 61 (%26,8) tanesinin 1 yıldan az, 78 (%34,2) tanesinin 1-3 yıl arasında, 44 (%19,3) tanesinin 3-5 yıl arasında, 34 (%14,9) tanesinin 5-15 yıl arasında, 7 (%3,1) tanesinin 15-25 yıl arasında, 4 (%1,8) tanesinin 25 yıldan fazla çalışma süresi olduğu ve son olarak katılımcıların 27 (%11,8) tanesinin üst düzey yönetici, 31 (%13,6) tanesinin orta düzey yönetici, 24 (%10,5) tanesinin alt düzey yönetici, 135 (%59,2) tanesinin teknik çalışan ve 11 (%4,8) tanesinin idari çalışan olduğu görülmüştür.

Siber Güvenlik Farkındalığı Ölçeği (SGFÖ)'nde yer alan ifadelere verilen cevaplara ve ölçeğin geneline ilişkin tanımlayıcı bulgular Tablo 3.3'de olduğu gibidir.

Tablo 3.3. SGFÖ'nün Tanımlayıcı Bulguları

Ölçeğin Geneli ve Cevaplar	**n**	**min**	**max**	**$\bar{x}$**	**ss**
1. İşletmemizde, bilgi güvenliğini artırmak amacıyla antivirüs ve kötü amaçlı yazılım yazılımları aktif olarak kullanılıyor.	228	1	5	4,36	1,059

2. Yetki sahibi olmadığımız dosyalara erişimimiz işletmemiz tarafından engellenmektedir.	228	1	5	4,35	1,028
3. İşletmemizde, yeni çalışanlara yönelik oryantasyon kapsamında siber güvenlik eğitimlerine yer verilmektedir.	228	1	5	3,63	1,251
4. Bilgisayar ve bilgi güvenliği konusunda eğitim aldım.	228	1	6	4,34	0,946
5. Bilgisayar becerilerimi güncellemek için eğitimlere katılmak benim için önemlidir.	228	1	5	4,49	0,837
6. Bilgisayar güvenliğine dikkat edilmesinin önemli olduğunu düşünüyorum.	228	1	6	4,68	0,779
7. İşletme yönetimimiz siber güvenlik konusunu çok ciddiye alır.	228	1	5	4,32	0,951
8. İşletmemiz sık sık kurumun siber güvenlik durumuna ilişkin bilgiler gönderiyor.	228	1	5	3,63	1,212
9. Bilgisayarlar konusunda bilgili olduğumu düşünüyorum.	228	1	5	4,35	0,855
10. Önemli bilgileri yedekleyip güvenliğini sağlarım.	228	1	5	4,50	0,873
11. Şifrelerimi özenle korurum.	228	1	5	4,57	0,844
12. Çalışanları çeşitli siber güvenlik tehditlerine karşı sürekli olarak uyarmanın motive edeceğine inanıyorum.	228	1	5	3,86	1,181
13. Siber tehditlerin işletmemiz üzerinde olumsuz bir etkisi olabileceğine inanıyorum.	228	1	5	4,28	1,065
14. İşletmemizde, korumamız gereken müşteri veya tedarikçi verilerine sahibiz.	228	1	5	4,37	0,974
15. İşletmemizde kendi BT sistemlerine bağlantı sağlayan ya da bizim sistemlerimize bağlanmasına izin verdiğimiz tedarikçilerimiz veya müşterilerimiz var.	228	1	5	3,64	1,464

16. İş yerindeki herkes şirketin paylaşılan dosya sunucularındaki herhangi bir dosyaya erişebilir.	228	1	5	2,24	1,453
17. İşletmemizde, bilgisayarlarımızın kurulumu için özel Bilgi Teknolojileri destek personeli bulunmaktadır.	228	1	5	3,82	1,444
18. İşletmemiz, siber güvenliği de içeren derinlemesine bir risk analizi yapmaktadır.	228	1	5	3,72	1,227
19. Şifrelerimi oluştururken semboller, sayılar ve büyük harfler içeren tahmin edilmesi zor bir şifre seçiyorum.	228	1	5	4,57	0,756
20. Hesaplarımın şifrelerini kimseyle paylaşmıyorum.	228	1	5	4,59	0,821
21. Cihazlarımda yüklü olan güvenlik duvarını açık tutuyorum.	228	1	5	4,05	1,310
22. İnternetten indirdiğim dosyaları antivirüs programı ile tarama yapmadan açmıyorum.	228	1	5	3,81	1,309
23. Cihazlarımı düzenli olarak bir anti-virüs programı ile tararım.	228	1	5	3,72	1,252
24. Tanımadığım kişilerden gelen e-postalara güvenmiyorum.	228	1	5	4,50	0,873
25. Bilinmeyen kaynaklardan gelen bağlantıları ve ekleri açmıyorum.	228	1	5	4,43	0,980
26. Bilgisayarımda bir casus yazılım önleme aracı kullanıyorum.	228	1	5	3,77	1,322
27. E-posta gönderirken şifreleme kullanıyorum.	228	1	5	3,05	1,470
28. Olağandışı bilgisayar davranışlarını/yanıtlarını izlerim (örneğin bilgisayarın yavaşlaması veya donması, açılır pencereler vb.)	228	1	5	4,46	0,931
29. Casus yazılım ve kötü amaçlı yazılımlardan kurtulma konusunda kendime güveniyorum.	228	1	5	3,74	1,210
30. Şifrelerin düzenli olarak değiştirilmesi gerektiğini düşünüyorum.	228	1	5	4,25	1,017

31. Kişisel akılı telefonumu iş ile ilgili konularda da kullanıyorum.	228	1	5	3,61	1,487
32. Dosyaları düzenli olarak yedekliyorum.	228	1	5	4,41	0,858
Ölçeğin Geneli	228	1,44	5,00	4,07	0,532

n: Sayı, min: Minimum, max: Maksimum, $\bar{x}$: Ortalama, ss: Standart Sapma

Tablo 3.3'de; SGFÖ'nün genelinin ortalamasının 4,07 olduğu ve bunun katılımcıların genelinin sorularak katılıyorum meyilli cevap verdiği anlamına geldiği, ölçeğin en yüksek skor alan ifadesinin 4,68 puan ile 6.ifade olduğu, en düşük skor alan ifadesinin ise 2,24 puan ile 16.ifade olduğu görülmüştür.

3.3.7.1.2. Geçerlik Bulguları

Siber Güvenlik Farkındalığı Ölçeği (SGFÖ)'ne yapılan Geçerlilik Analizi bulguları Tablo 3.4'de olduğu gibidir.

Tablo 3.4. Geçerlilik Analizi Bulguları

Kaiser-Meyer-Olkin (KMO) Örneklem Yeterliliği	0,853
Bartlett Küresellik Testi (p)	0,000

Tablo 3.4'e göre; Kaiser-Meyer-Olkin (KMO) değerinin (0.853) yüksek ve 1'e yakın bir değer olması, Barlett Küresellik Testi p değerinin (0,000) olması sonucunda toplanan verilerin istatistiki olarak anlamlı ($p<0,05$) ve normal dağılım göstermesi, örneklemin temsiliyet gücünün yeterli olduğunu ve bu veri setinin faktör analizine uygun olduğunu göstermektedir (Çokluk, Şekercioğlu ve Büyüköztürk, 2010).

3.3.7.1.3. Açımlayıcı Faktör Analizi (AFA) Bulguları

Alt boyut sayısı belirtilmeden yapılan AFA sonucunda SGFÖ'nün 8 alt boyutu olduğu görülmüştür. Ancak alt boyut sayısının fazla, alt boyutlardaki ifade sayısının ise düşük kalması sebebiyle alt boyut sayısı 5 olarak belirlenerek tekrar AFA yapılmış ve elde edilen alt boyutların açıkladığı varyans oranları Tablo 3.5'de olduğu gibidir.

Tablo 3.5. SGFÖ ve Alt Boyutlarının Açıkladığı Varyans Bulguları

Boyutlar	Özdeğer	Varyans Yüzdesi	Kümülatif Yüzde
1	9,035	28,235	28,235
2	2,926	9,143	37,378

3	1,786	5,580	42,958
4	1,532	4,788	47,746
5	1,438	4,492	52,238

Tablo 3.5'e göre; 5 alt boyutla sınırlandırılmış olan SGFÖ'nün, birinci alt boyuta ait özdeğer 9,035 ve açıkladığı varyans %28,235 oranında, ikinci alt boyuta ait özdeğer 2,926 ve açıkladığı varyans %9,143 oranında, üçüncü alt boyuta ait özdeğer 1,786 ve açıkladığı varyans %5,580 oranında, dördüncü alt boyuta ait özdeğer 1,532 ve açıkladığı varyans %4,788 oranında ve beşinci alt boyuta ait özdeğer 1,438 ve açıkladığı varyans ise %4,492 oranında olduğu, 5 alt boyutun da toplamda ölçeğin %52,238'lik kısmını açıkladığı görülmüştür.

Belirlenen 5 alt boyuta ait ifadeler ile bunlara ait yüklere ilişkin bulgular Tablo 3.6'da belirtilmiştir.

Tablo 3.6. SGFÖ'nün Alt Boyutlarına Ait İfadeler ve Yüklerine İlişkin Bulgular

İfadeler	**Alt Boyutlar**				
	1.Alt Boyut Bilgisayar ve Veri Güvenliği	**2.Alt Boyut Siber Güvenlik Yönetimi**	**3.Alt Boyut Cihaz Güvenliği**	**4.Alt Boyut Siber Tehditlere Karşı Güven**	**5.Alt Boyut Şifre Yönetimi ve Güvenliği**
SGF10	0,751				
SGF9	0,707				
SGF11	0,638				
SGF4	0,621				
SGF28	0,602				
SGF6	0,571				
SGF5	0,534				
SGF14	0,531				
SGF32	0,452				
SGF30	0,395				
SGF1	0,367				
SGF18		0,794			
SGF3		0,729			
SGF8		0,670			
SGF7		0,600			
SGF2		0,511			
SGF17		0,487			
SGF15		0,410			
SGF12					

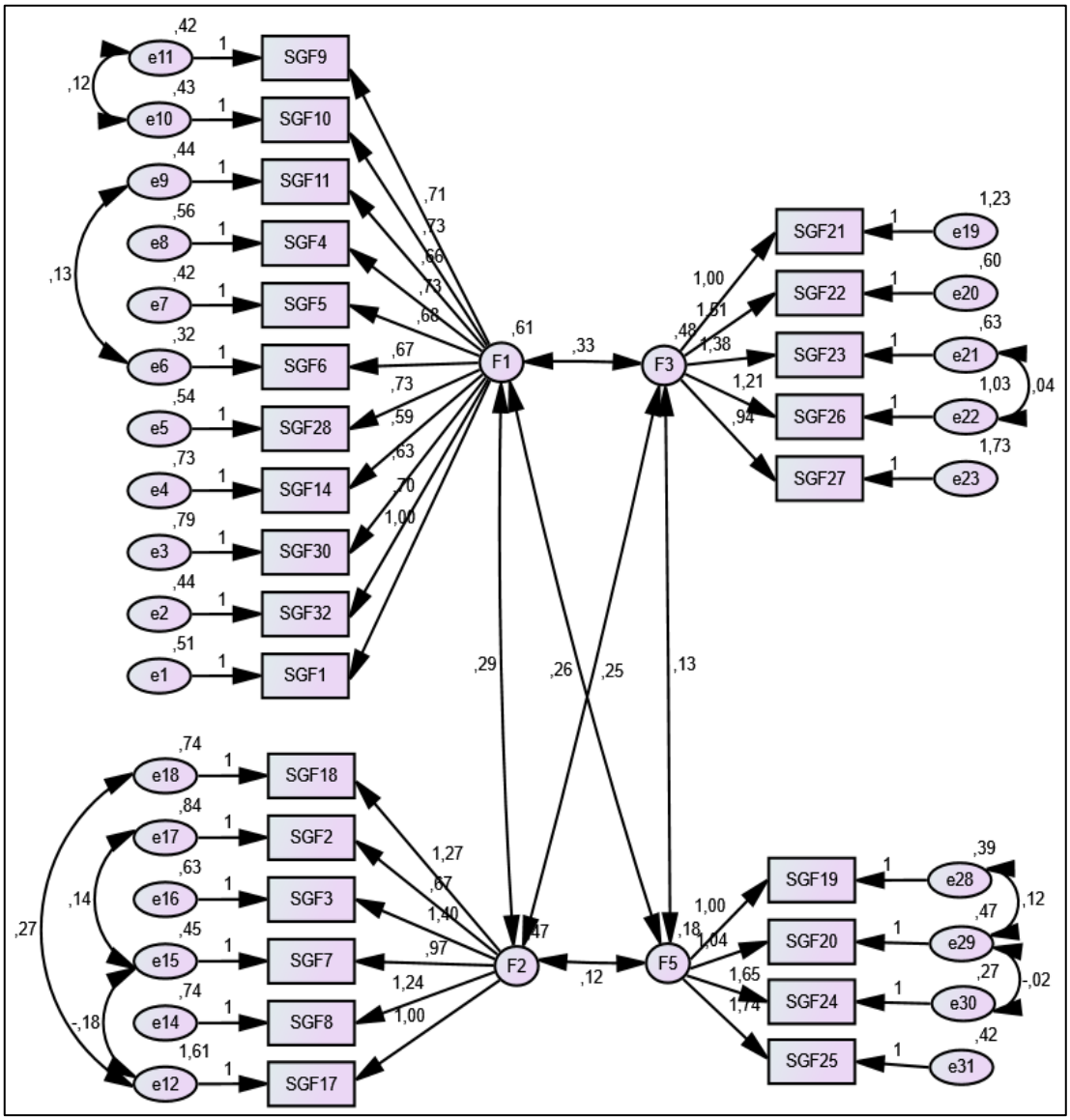
SGF23	0,792		
SGF26	0,735		
SGF22	0,728		
SGF21	0,570		
SGF27	0,515		
SGF29		-0,607	
SGF31		0,546	
SGF13		0,383	
SGF19			-0,648
SGF16			0,603
SGF24			-0,573
SGF25			-0,570
SGF20			-0,516

AFA kapsamında belirlenen alt boyutların yük değerleri, 12.ifade çıkarıldığında daha belirgin hale geldiği görülmüştür. Bu bağlamda Tablo 3.6'e göre indeksin; 1.alt boyutunun 11 ifadeden, 2.alt boyutunun 7 ifadeden, 3.alt boyutunun 5 ifadeden, 4.alt boyunun 3 ifadeden ve 5.alt boyutunun ise 5 ifadeden oluştuğu görülmüştür.

3.3.7.1.4. Doğrulayıcı Faktör Analizi (DFA) Bulguları

AFA sonrasında elde edilen alt boyutlar esas alınarak yapılan Doğrulayıcı faktör analizi sonucunda elde edilen model Şekil 3.1'de olduğu gibidir.

Şekil 3.1. DFA Modeli



SGFÖ'nün alt boyutlarını test etmek amacıyla yapılan doğrulayıcı faktör analizi kapsamında modelde iyileştirme yapılırken uyumu azaltan değişkenler belirlenmiş, artık değerler arasında kovaryansı yüksek olanlar için yeni kovaryanslar oluşturulmuştur. Bu bağlamda; 2.alt boyutta bulunan 15.ifade ile 4.alt boyutta bulunan 13, 29 ve 31.ifadeler çıkarılmıştır. Yapılan düzenlemelerin sonucunda elde edilen uyum iyiliği bulguları Tablo 3.7'de belirtilmiştir.

Tablo 3.7. Uyum İyiliği Bulguları

Uyum Ölçütleri	**Kriterler**	**Değerler**	**Sonuç**

Anlamlılık Değeri (p)	<0,05	0,000	Anlamlı
Ki-Kare Serbestlik Derecesi Oranı (CMIN/DF, X^2/df)	≤5	2,459	İyi
İyilik Uyum İndeksi (Goodness of Fit Index-GFI)	<0,85	0,815	Düşük
Düzeltilmiş İyilik Uyum İndeksi (Adjusted Goodness of Fit Index-AGFI)	<0,80	0,772	Düşük
Karşılaştırmalı Uyum İndeksi (Comparative Fit Index-CFI)	<0,90	0,830	Düşük
Artan Uyum İndeksi (Increasing Fit Index-IFI)	<0,90	0,833	Düşük
Yaklaşık Hataların Ortalama Karekökü (Root Mean Square Error of Approximation-RMSEA)	0,06-0,08	0,080	Kabul edilebilir

Mevcut örneklem için hesaplanan uyum değerleri incelendiğinde Tablo 3.7'e göre; doğrulayıcı faktör analizinin istatistiki olarak anlamlı sonuçlar (p=0,000) verdiği (p<0,05), Ki-Kare Serbestlik Derecesi Oranı (X^2/df=2,459) değeri 3'ün altında olduğu (Hooper, Coughlan ve Mullen, 2008) için iyi düzeyde olduğu, Yaklaşık Hataların Ortalama Karekökü (RMSEA=0,080) değerinin de kabul edilebilir düzeyde olduğu (Hoe, 2008) görülmüştür. İyilik Uyum İndeksi (GFI=0,825) değerinin, Düzeltilmiş İyilik Uyum İndeksi (AGFI=0,793) değerlerinin (Bentler ve Bonett, 1980), Karşılaştırmalı Uyum İndeksi (CFI=0,905) değerinin (Şimşek, 2007) ve Artan Uyum İndeksi (IFI=0,905) değerinin (Bentler ve Bonett, 1980) düşük karşın kabul edilebilir olması, diğer uyum değerlerinin iyi veya kabul edilebilir düzeyde olması ve örneklem sayısının iyi düzeyde olması sebebiyle modelin genelinin yeterli temsiliyeti sağladığı değerlendirilmiştir.

3.3.7.1.5. Güvenirlik Bulguları

SGFÖ'nün geneline ve AFA ve DFA sonucu elde edilen alt boyutlarına yapılan güvenirlik analizi bulguları Tablo 3.8'de olduğu gibidir.

Tablo 3.8. Güvenirlik Analizi Bulguları

Alt Boyutlar	Cronbach's Alpha (α)	Genel Cronbach's Alpha (α)
1	0,871	0,891
2	0,796	
3	0,765	
4	0,329	

Tablo 3.8'e göre güvenirlik düzeyi olan Cronbach's Alpha (α) değerlerine bakıldığında; SGFÖ'nün Genelinin, 1.alt boyutunun, 2.alt boyutunun ve 3.alt boyutunun güvenirliğinin iyi düzeyde ($0.7 \leq \alpha < 0.9$) olduğu, 4.alt boyutunun güvenirlik düzeyinin ise kabul edilemez ($\alpha < 0.5$) olduğu görülmüştür. (George ve Mallery, 2001; Tabachnick ve Fidell, 2007). Bu sebeple, ölçeğin 4.alt boyutu ilişkisel analizlerde kullanılamamıştır.

3.3.7.1.6. Normallik Bulguları

Siber Güvenlik Farkındalığı Ölçeği (SGFÖ)'ne verilen cevapların normal dağılıp dağılmadığının belirlenmesi için Normallik Testi yapılmış ve elde edilen bulgular Tablo 3.9'da belirtilmiştir.

Tablo 3.9. SGFÖ'nün Normallik Testi Bulguları

Ölçek ve Alt Boyutları	Kolmogorov-Smirnov	Shapiro Wilk	Çarpıklık (Skewness)	Basıklık (Kurtosis)
	p	p		
Genel	0,001	0,000	-1,197	2,675
F1	0,000	0,000	-2,273	7,667
F2	0,000	0,000	-,0595	-0,254
F3	0,000	0,000	-0,703	0,150

p:%95 güven aralığında anlamlılık değeri

Yapılan normallik analizleri kapsamında; Kolmogorov-Smirnov ve Shapiro Wilk Testlerine göre ölçeğin normal dağılmadığı görülmüştür ($p<0,05$). Ancak ölçeklere verilen cevapların normal dağılıp dağılmadıklarına karar verilirken, çarpıklık (skewness) ve basıklık (kurtosis) değerlerine de bakılmalıdır. Bu bağlamda literatürde kabul görmüş bir yaklaşım olan Tabachnik ve Fidell (2013)'e göre; çarpıklık ve basıklık değerlerinin -1,50 ile +1,50 arasında olması durumunda cevapların dağılımın normal kabul edilebileceği belirtilmektedir. Buna göre, ölçeğin geneli ile 1.alt boyutuna verilen cevapların normal dağılmamasına karşın 2.ve 3.alt boyutlarına verilen cevapların normal dağıldığı görülmüştür.

3.3.7.1.7. İlişkisel Bulgular

İlişkisel analizlerde; SGFÖ'nün geneli ile 1.alt boyutuna verilen cevapların normal dağılım göstermemesi sebebiyle parametrik olmayan yöntemler, 2. ve 3.alt

boyutlarına verilen cevaplar ise normal dağılım gösterdiği için parametrik yöntemler kullanılmıştır.

3.3.7.1.7.1. Cinsiyet ile SGFÖ Arasındaki Fark Testi Bulguları

Cinsiyet değişkeni ile SGFÖ'nin geneli ve 1.boyutuna verilen cevaplar arasında yapılan Mann Whitney U Testi bulguları Tablo 3.10'da olduğu gibidir.

Tablo 3.10. Cinsiyet ile SGFÖ Arasındaki Mann Whitney U Testi Bulguları

Ölçek ve Alt Boyutları	Cinsiyet	n	sıra $\bar{x}$	$\bar{x}$	ss	p
Genel	Kadın	36	83,65	3,8488	0,62475	0,002
	Erkek	192	120,28	4,1599	0,52574	
1.Alt Boyut	Kadın	36	94,46	4,2172	0,75882	0,046
	Erkek	192	118,26	4,4754	0,56017	

n: Sayı, sıra $\bar{x}$: Sıra Ortalaması, $\bar{x}$: Ortalama, ss: Standart Sapma, p:%95 güven aralığında anlamlılık değeri

Tablo 3.10'a göre; Cinsiyet değişkeni ile SGFÖ'nün geneline ve 1.alt boyutuna verilen cevaplar arasında istatistiki olarak anlamlı bir farklılaşma olduğu görülmüştür ($p<0,05$). Farklılaşmaların sebebine bakıldığında; 1.alt boyut olan bilgisayar ve veri güvenliği için erkeklerin verdiği cevapların ortalamalarının kadınların verdikleri cevapların ortalamalarından yüksek olduğu görülmüştür. Yani kadınların bilgisayar ve veri güvenliği konusunda erkeklere göre daha az farkındalık sahibi oldukları görülmektedir.

Cinsiyet değişkeni ile SGFÖ'nin 2. ve 3.boyutuna verilen cevaplar arasında yapılan Bağımsız Örneklem T Testi bulguları Tablo 3.11'de olduğu gibidir.

Tablo 3.11. Cinsiyet ile SGFÖ Arasındaki Bağımsız Örneklem T Testi Bulguları

Ölçek ve Alt Boyutları	Cinsiyet	n	$\bar{x}$	ss	p
2.Alt Boyut	Kadın	36	3,4861	0,88764	0,001
	Erkek	192	3,9913	0,81055	
3.Alt Boyut	Kadın	36	3,2778	1,05102	0,006
	Erkek	192	3,7562	0,92355	

n: Sayı, $\bar{x}$: Ortalama, ss: Standart Sapma, p:%95 güven aralığında anlamlılık değeri

Tablo 3.11'e göre; Cinsiyet değişkeni ile SGFÖ'nün 2. ve 3.alt boyutuna verilen cevaplar arasında istatistiki olarak anlamlı bir farklılaşma olduğu görülmüştür

(p<0,05). Farklılaşmaların sebebine bakıldığında; siber güvenlik yönetimi ve cihaz güvenliği konusunda erkeklerin verdiği cevapların ortalamalarının kadınların verdikleri cevapların ortalamalarından yüksek olduğu görülmüştür. Yani kadınların ölçeğe verdiği cevapların, katılıyorum seçeneğine erkeklere göre daha yakın olduğu görülmüştür.

3.3.7.1.7.2. Yaş ile SGFÖ Arasındaki Fark Testi Bulguları

Yaş değişkeni ile ile SGFÖ'nin geneli ve 1.boyutuna verilen cevaplar arasında yapılan Kruskal Wallis Testi bulguları Tablo 3.12'de olduğu gibidir.

Tablo 3.12. Yaş ile SGFÖ Arasındaki Kruskal Wallis Testi Bulguları

Ölçek ve Alt Boyutları	Yaş	n	sıra $\bar{x}$	$\bar{x}$	ss	p	Post Hoc (LSD)
Genel	18-25 Yaş Arası	86	103,10	4,0254	0,56116	0,040	42-49 Yaş Arası> 18-25 Yaş Arası
	26-33 Yaş Arası	99	113,64	4,1268	0,47877		
	34-41 Yaş Arası	24	130,10	4,2377	0,49110		
	42-49 Yaş Arası	14	156,04	4,3862	0,56220		
	50 Yaş ve Üzeri	5	136,40	3,8815	1,42638		
1.Alt Boyut	18-25 Yaş Arası	86	96,41	4,3140	0,59762	0,001	42-49 Yaş Arası> 18-25 Yaş Arası, 50 Yaş ve Üzeri
	26-33 Yaş Arası	99	116,47	4,4876	0,48287		
	34-41 Yaş Arası	24	135,54	4,5530	0,62808		
	42-49 Yaş Arası	14	166,86	4,7208	0,57215		
	50 Yaş ve Üzeri	5	138,90	4,0909	1,72966		

n: Sayı, sıra $\bar{x}$: Sıra Ortalaması, $\bar{x}$: Ortalama, ss: Standart Sapma, p:%95 güven aralığında anlamlılık değeri

Tablo 3.12'e göre; Yaş değişkeni ile SGFÖ'nün geneli ile 1.alt boyutuna verilen cevaplar arasında istatistiki olarak anlamlı bir farklılaşma olduğu görülmüştür (p<0,05). Farklılaşmaların sebebine bakıldığında; ölçeğinde genlinde, 42-49 yaş arasında olan katılımcıların cevaplarının ortalamalarının 18-25 yaş arası katılımcıların cevapların ortalamalarından yüksek olduğu, 1.alt boyutta ise, 42-49 yaş arasında olan katılımcıların cevaplarının ortalamalarının 18-25 yaş arasında ve 50 yaş üzerinde olan katılımcıların cevapların ortalamalarından yüksek olduğu görülmüştür.

Yaş değişkeni ile ile SGFÖ'nin 2. ve 3.boyutuna verilen cevaplar arasında yapılan Tek Yönlü Anova Testi bulguları Tablo 3.13'de olduğu gibidir.

Tablo 3.13. Yaş ile SGFÖ Arasındaki Tek Yönlü Anova Testi Bulguları

Ölçek ve Alt Boyutları	Yaş	n	x̄	ss	p	Post Hoc (LSD)
2.Alt Boyut	18-25 Yaş Arası	86	3,9225	0,72657	0,534	-
	26-33 Yaş Arası	99	3,8552	0,93334		
	34-41 Yaş Arası	24	4,0486	0,77938		
	42-49 Yaş Arası	14	4,1429	0,74207		
	50 Yaş ve Üzeri	5	3,5333	1,34061		
3.Alt Boyut	18-25 Yaş Arası	86	3,5116	1,02835	0,090	-
	26-33 Yaş Arası	99	3,6828	0,80408		
	34-41 Yaş Arası	24	3,9750	0,92935		
	42-49 Yaş Arası	14	4,0857	1,21203		
	50 Yaş ve Üzeri	5	4,0000	1,49666		

n: Sayı, x̄: Ortalama, ss: Standart Sapma, p:%95 güven aralığında anlamlılık değeri

Tablo 3.13'e göre; Yaş değişkeni ile SGFÖ'nün 2. ve 3.alt boyutuna verilen cevaplar arasında istatistiki olarak anlamlı bir farklılaşma olmadığı görülmüştür (p>0,05). Yani ölçeğin siber güvenlik yönetimi ve cihaz güvenliği boyutlarına verilen cevapların katılımcıların yaşlarına göre farklılık göstermediği görülmüştür.

3.3.7.1.7.3. Eğitim Durumu ile SGFÖ Arasındaki Fark Testi Bulguları

Eğitim Durumu değişkeni ile SGFÖ'nin geneli ve 1.boyutuna verilen cevaplar arasında yapılan Kruskal Wallis Testi bulguları Tablo 3.14'de olduğu gibidir.

Tablo 3.14. Eğitim Durumu ile SGFÖ Arasındaki Kruskal Wallis Testi Bulguları

Ölçek ve Alt Boyutları	Eğitim Durumu	n	sıra x̄	x̄	ss	p	Post Hoc (LSD)
Genel	İlköğretim	2	35,25	3,3704	0,68092	0,043	Lisans> İlköğretim
	Ortaöğretim (lise)	26	118,58	4,1595	0,50302		
	Ön Lisans	60	100,96	4,0259	0,49743		
	Lisans	117	125,01	4,1744	0,59033		
	Lisansüstü	23	98,63	4,0177	0,49134		
1.Alt Boyut	İlköğretim	2	48,00	3,6364	1,15708	0,184	-
	Ortaöğretim (lise)	26	118,96	4,4755	0,60264		
	Ön Lisans	60	102,45	4,3621	0,58354		
	Lisans	117	122,39	4,4856	0,60174		
	Lisansüstü	23	106,52	4,3874	0,58802		

n: Sayı, sıra x̄: Sıra Ortalaması, x̄: Ortalama, ss: Standart Sapma, p:%95 güven aralığında anlamlılık değeri

Tablo 3.14'e göre; Eğitim Durumu değişkeni ile SGFÖ'nün sadece geneline verilen cevaplar arasında istatistiki olarak anlamlı bir farklılaşma olduğu görülmüştür (p<0,05). Bu bağlamda; lisans eğitimi görmüş katılımcıların verdikleri cevapların ortalamalarının ilköğretim mezunu katılımcıların verdikleri cevapların ortalamalarından yüksek olduğu, ölçeğin 1.alt boyut olan bilgisayar ve veri güvenliğine verilen cevapların ise eğitim durumuna göre farklılaşmadığı görülmüştür.

Eğitim Durumu değişkeni ile SGFÖ'nin 2. ve 3.alt boyutuna verilen cevaplar arasında yapılan Tek Yönlü Anova Testi bulguları Tablo 3.15'de olduğu gibidir.

Tablo 3.15. Eğitim Durumu ile SGFÖ Arasındaki Tek Yönlü Anova Testi Bulguları

Ölçek ve Alt Boyutları	Eğitim Durumu	n	$\bar{x}$	ss	p	Post Hoc
2.Alt Boyut	İlköğretim	2	3,1667	0,47140	0,401	-
	Ortaöğretim (lise)	26	3,9231	0,93480		
	Ön Lisans	60	3,8444	0,71365		
	Lisans	117	3,9915	0,87287		
	Lisansüstü	23	3,7319	0,89010		
3.Alt Boyut	İlköğretim	2	3,0000	0,28284	0,172	-
	Ortaöğretim (lise)	26	3,7077	0,91953		
	Ön Lisans	60	3,5300	1,02764		
	Lisans	117	3,8137	0,92577		
	Lisansüstü	23	3,4261	0,94639		

n: Sayı, $\bar{x}$: Ortalama, ss: Standart Sapma, p:%95 güven aralığında anlamlılık değeri

Tablo 3.15'e göre; Eğitim Durumu değişkeni ile SGFÖ'nün 2. ve 3.alt boyutlarına verilen cevaplar arasında istatistiki olarak anlamlı bir farklılaşma olmadığı görülmüştür (p>0,05). Yani katılımcıların ölçeğin siber güvenlik yönetimi ve cihaz güvenliği boyutlarına verdikleri cevapların eğitim durumuna göre farklılaşmadığı görülmüştür.

3.3.7.1.7.4. Çalışma Süresi ile SGFÖ Arasındaki Fark Testi Bulguları

Çalışma Süresi değişkeni ile SGFÖ'nin geneli ve 1.boyutuna verilen cevaplar arasında yapılan Kruskal Wallis Testi bulguları Tablo 3.16'da olduğu gibidir.

Tablo 3.16. Çalışma Süresi ile SGFÖ Arasındaki Kruskal Wallis Testi Bulguları

Ölçek ve Alt Boyutları	Çalışma Süresi	n	sıra $\bar{x}$	$\bar{x}$	ss	p	Post Hoc (LSD)

Genel	1 Yıldan Az	61	101,77	4,0134	0,57421	0,160	-
	1-3 Yıl Arası	78	114,17	4,1192	0,51322		
	3-5 Yıl Arası	44	119,22	4,1423	0,54286		
	5-15 Yıl Arası	34	121,38	4,1373	0,64766		
	15-25 Yıl Arası	7	124,36	4,2646	0,42089		
	25 Yıldan Fazla	4	187,50	4,5926	0,00000		
1.Alt Boyut	1 Yıldan Az	61	99,01	4,3174	0,62272	0,000	5-15 Yıl Arası, 15-25 Yıl Arası> 1 Yıldan Az
	1-3 Yıl Arası	78	105,63	4,4021	0,51478		
	3-5 Yıl Arası	44	106,31	4,3967	0,61785		
	5-15 Yıl Arası	34	152,44	4,6283	0,72533		
	15-25 Yıl Arası	7	173,71	4,8442	0,21458		
	25 Yıldan Fazla	4	187,63	4,9091	0,12856		

n: Sayı, sıra $\bar{x}$: Sıra Ortalaması, $\bar{x}$: Ortalama, ss: Standart Sapma, p:%95 güven aralığında anlamlılık değeri

Tablo 3.16'ya göre; Çalışma Durumu değişkeni ile SGFÖ'nün sadece 1.alt boyutuna verilen cevaplar arasında istatistiki olarak anlamlı bir farklılaşma olduğu görülmüştür ($p<0,05$). Bu bağlamda; çalışma süresi 1 yıldan az olan katılımcıların verdikleri cevapların ortalamalarının çalışma süresi 5-15 yıl arası ve 15-25 yıl arası olan katılımcıların verdikleri cevapların ortalamalarından düşük olduğu, ölçeğin geneline verilen cevaplara göre ise çalışma süresine göre farklılaşmadığı görülmüştür.

Çalışma Süresi değişkeni ile SGFÖ'nin 2. ve 3.boyutuna verilen cevaplar arasında yapılan Tek Yönlü Anova Testi bulguları Tablo 3.17'de olduğu gibidir.

Tablo 3.17. Çalışma Süresi ile SGFÖ Arasındaki Tek Yönlü Anova Testi Bulguları

Ölçek ve Alt Boyutları	Çalışma Süresi	n	$\bar{x}$	ss	p	Post Hoc (LSD)
2.Alt Boyut	1 Yıldan Az	61	4,0055	0,85741	0,522	-
	1-3 Yıl Arası	78	3,8953	0,86127		
	3-5 Yıl Arası	44	3,9659	0,78139		
	5-15 Yıl Arası	34	3,7157	0,90781		
	15-25 Yıl Arası	7	3,6667	0,61614		
	25 Yıldan Fazla	4	4,2917	0,53359		
3.Alt Boyut	1 Yıldan Az	61	3,4131	0,99255	0,045	1-3 Yıl Arası, 3-5 Yıl Arası, 25 Yıldan Fazla> 1 Yıldan Az
	1-3 Yıl Arası	78	3,7949	0,81031		
	3-5 Yıl Arası	44	3,8273	0,84588		
	5-15 Yıl Arası	34	3,6000	1,15365		
	15-25 Yıl Arası	7	3,6571	1,49092		
	25 Yıldan Fazla	4	4,6500	0,41231		

n: Sayı, $\bar{x}$: Ortalama, ss: Standart Sapma, p:%95 güven aralığında anlamlılık değeri

Tablo 3.17'e göre; Çalışma Durumu değişkeni ile SGFÖ'nün sadece 3.alt boyut olan cihaz güvenliğine verilen cevaplar arasında istatistiki olarak anlamlı bir farklılaşma olduğu görülmüştür (p<0,05). Bu bağlamda; çalışma süresi 1 yıldan az olan katılımcıların verdikleri cevapların ortalamalarının çalışma süresi 1-3 yıl arası, 3-5 yıl arası ve 25 yıldan fazla olan katılımcıların verdikleri cevapların ortalamalarından düşük olduğu, ölçeğin 2.alt boyut olan siber güvenlik yönetimine verilen cevapların ise çalışma süresine göre farklılaşmadığı görülmüştür.

3.3.7.1.7.5. İşletmedeki Pozisyon ile SGFÖ Arasındaki Fark Testi Bulguları

İşletmedeki Pozisyon değişkeni ile SGFÖ'nin geneli ve 1.boyutuna verilen cevaplar arasında yapılan Kruskal Wallis Testi bulguları Tablo 3.18'de olduğu gibidir.

Tablo 3.18. İşletmedeki Pozisyon ile SGFÖ Arasındaki Kruskal Wallis Testi Bulguları

Ölçek ve Alt Boyutları	İşletmedeki Pozisyon	n	sıra $\bar{x}$	$\bar{x}$	ss	p	Post Hoc
Genel	Üst Düzey Yönetici	27	121,26	4,2030	0,45365	0,525	-
	Orta Düzey Yönetici	31	126,19	4,1912	0,52475		
	Alt Düzey Yönetici	24	116,96	4,0586	0,76177		
	Teknik Çalışan	135	108,57	4,0733	0,52873		
	İdari Çalışan	11	132,41	4,2323	0,64195		
1.Alt Boyut	Üst Düzey Yönetici	27	147,54	4,6599	0,43496	0,010	Üst Düzey Yönetici> Teknik Çalışan
	Orta Düzey Yönetici	31	131,15	4,5220	0,63980		
	Alt Düzey Yönetici	24	120,00	4,3523	0,95207		
	Teknik Çalışan	135	105,14	4,3980	0,53724		
	İdari Çalışan	11	89,32	4,2645	0,55812		

n: Sayı, sıra $\bar{x}$: Sıra Ortalaması, $\bar{x}$: Ortalama, ss: Standart Sapma, p:%95 güven aralığında anlamlılık değeri

Tablo 3.18'e göre; İşletmedeki Pozisyon değişkeni ile SGFÖ'nün sadece 1.alt boyut olan bilgisayar ve veri güvenliğine verilen cevaplar arasında istatistiki olarak anlamlı bir farklılaşma olduğu görülmüştür (p<0,05). Bu bağlamda; üst düzey yöneticilerin verdikleri cevapların ortalamalarının teknik çalışanların verdikleri cevapların ortalamalarından yüksek olduğu, ölçeğin geneline verilen cevapların ise işletmedeki pozisyona göre farklılaşmadığı görülmüştür.

İşletmedeki Pozisyon değişkeni ile SGFÖ'nin 2. ve 3.boyutuna verilen cevaplar arasında yapılan Tek Yönlü Anova Testi bulguları Tablo 3.19'de olduğu gibidir.

Tablo 3.19. İşletmedeki Pozisyon ile SGFÖ Arasındaki Tek Yönlü Anova Testi Bulguları

Ölçek ve Alt Boyutları	İşletmedeki Pozisyon	n	$\bar{x}$	ss	p	Post Hoc
2.Alt Boyut	Üst Düzey Yönetici	27	3,8333	0,78854	0,687	-
	Orta Düzey Yönetici	31	4,0376	0,72739		
	Alt Düzey Yönetici	24	3,9861	0,89943		
	Teknik Çalışan	135	3,8667	0,84686		
	İdari Çalışan	11	4,1364	1,11509		
3.Alt Boyut	Üst Düzey Yönetici	27	3,5852	1,35978	0,598	-
	Orta Düzey Yönetici	31	3,7161	0,97676		
	Alt Düzey Yönetici	24	3,6500	0,83666		
	Teknik Çalışan	135	3,6607	0,88445		
	İdari Çalışan	11	4,1273	0,91334		

n: Sayı, $\bar{x}$: Ortalama, ss: Standart Sapma, p:%95 güven aralığında anlamlılık değeri

Tablo 3.19'a göre; İşletmedeki Pozisyon ile SGFÖ'nün 2. ve 3.alt boyutuna verilen cevaplar arasında istatistiki olarak anlamlı bir farklılaşma olmadığı görülmüştür ($p>0,05$). Yani ölçeğin siber güvenlik yönetimi ve cihaz güvenliği boyutlarına verilen cevapların katılımcıların işletmedeki pozisyonlarına göre farklılaşmadığı görülmüştür.

3.3.7.1.7.6. SGFÖ'nün Geneli ve Alt Boyutları Arasındaki Korelasyon Bulguları

Ölçeğin geneli ve alt boyutları arasında yapılan Spearman Korelasyon Analizi bulguları Tablo 3.20'de olduğu gibidir.

Tablo 3.20. Spearman Korelasyon Analizi Bulguları

		Genel	1.Alt Boyut	2.Alt Boyut	3.Alt Boyut
Genel	r	1,000	-	-	-
	p	-	-	-	-
	n	228	-	-	-
1.Alt Boyut	r	0,794	1,000	-	-
	p	0,000	-	-	-
	n	228	228	-	-
2.Alt Boyut	r	0,779	0,450	1,000	-

	p	0,000	0,000	-	-
	n	228	228	228	-
3.Alt Boyut	r	0,827	0,546	0,511	1,000
	p	0,000	0,000	0,000	-
	n	228	228	228	228

r:Korelasyon katsayısı, n:Sayı, p:%95 güven aralığında anlamlılık değeri

Tablo 3.20'e göre; SGFÖ'nün Geneli ve tüm alt boyutları arasında istatistiki olarak anlamlı ve pozitif korelasyonlar olduğu görülmüştür ($p<0,05$).

Bu bağlamda en yüksek pozitif korelasyonun SGFÖ'nün Geneli ile 3.alt boyutu arasında 0,827 boyutunda olduğu görülmüştür. Bunun anlamı SGFÖ'nün geneline verilen cevapların ortalamasında 1 birim artış olduğunda 3.alt boyutuna verilen cevapların ortalamasının %82,7 oranında bir artış olmasıdır. Bu durum tam tersi için de geçerlidir.

Ayrıca; ölçeğin geneli ile 1.alt boyutu arasında 0,794 boyutunda, ölçeğin geneli ile 2.alt boyutu arasında 0,779 boyutunda, ölçeğin 1.alt boyutu ile 2.alt boyutu arasında 0,450 boyutunda, ölçeğin 1.alt boyutu ile 3.alt boyutu arasında 0,546 boyutunda ve ölçeğin 2.alt boyutu ile 3.alt boyutu arasında ise 0,511 boyutunda pozitif korelasyonlar olduğu görülmüştür.

3.3.7.2. Nitel Araştırma Bulguları

3.3.7.2.1. Katılımcıların Özellikleri

Konya'da bilişim sektöründe faaliyet gösteren KOBİ'lerden seçilerek görüşme sağlanan 18 yönetici ve/veya müdür katılımcılarına ve işletmelerine ilişkin genel özellikler Tablo 3.21'de sunulmuştur.

Tablo 3.21. Katılımcıların Özellikleri

	İşletmenin faaliyet yılı	**Pozisyon**	**Çalışan sayısı**	**Dijital cihazları ve internet kullanım becerisi**
K1	20	Şube Müdürü	15	10/8
K2	18	Yönetici	5	10/8
K3	3	Yönetici	35	Çok iyi
K4	30	Müdür	11	Çok iyi
K5	2	İşveren	3	Orta-üst düzey
K6	5	CTO	4	Üst düzey

K7	10	Siber Güvenlik Uzmanı	25	İleri düzey
K8	15	Proje Koordinatörü/ Yöneticisi	39	İleri düzey
K9	20	Yazılım Müdürü	70	İyi
K10	4	Otomasyon Süreç Yöneticisi	12	İyi
K11	30	Orta Düzey Yönetici	20	İyi
K12	4	Satış Müdürü	10	İyi
K13	8	Yazılım Ekip Lideri-CTO	15	Çok iyi
K14	8	Kurucu	12	Gülücük konulmuş
K15	4	Genel Müdür	11	10/10
K16	8	Satıştan Sorumlu Kurucu	13	10/9
K17	6	Genel Müdür	8	Çok iyi
K18	10	Kurucu/ Yönetici	10	Yeterli

Araştırmaya katılan 18 katılımcı, işletmelerinin özellikleri ve dijital becerileri ile ilgili farklı profil ve deneyimlere sahiptir. Katılımcıların işletmeleri, faaliyet yılları açısından 2 yıldan 30 yıla kadar değişiklik göstermektedir. Bu durum hem köklü işletmelerin hem de daha yeni kurulan işletmelerin siber güvenlik farkındalığına dair değerlendirmelerini içermektedir. İşletme faaliyet yılı bakımından en eski işletme 30 yıldır faaliyet gösterirken, en yeni işletme ise 2 yıllık geçmişe sahiptir. Bu çeşitlilik, deneyim ve ihtiyaçların karşılaştırılabilir bir şekilde ele alınmasını sağlamaktadır.

Katılımcılar, işletmelerinde çeşitli pozisyonlarda görev yapmaktadır. Bunlar arasında şube müdürü, yönetici, müdür, CTO (Chief Technology Officer), siber güvenlik uzmanı, proje koordinatörü/yöneticisi, yazılım müdürü, otomasyon süreç yöneticisi, satış müdürü, yazılım ekip lideri, kurucu ve genel müdür gibi unvanlar yer almaktadır. Bu çeşitlilik, siber güvenlik farkındalığının farklı seviyelerdeki pozisyonlara nasıl yansıdığını anlamayı kolaylaştırmaktadır.

İşletmelerin çalışan sayısı 3 ile 70 arasında değişiklik göstermektedir. Bu farklılık, küçük ölçekli işletmelerden daha büyük ve çok çalışanlı işletmelere kadar geniş bir yelpazeyi kapsamaktadır. En az çalışan sayısına sahip işletme 3 kişilik bir ekipten oluşurken, en büyük işletmede 70 çalışan bulunmaktadır.

Katılımcıların dijital cihazları ve internet kullanım becerileri oldukça çeşitlilik göstermektedir. Çoğu katılımcı, "çok iyi", "ileri düzey" ve "iyi" becerilere sahip olduğunu belirtirken, bazı katılımcılar yeterli ya da orta-üst düzey beceri seviyelerine sahiptir. Özellikle teknik pozisyonlarda çalışanlar (örneğin CTO, yazılım müdürü, siber güvenlik uzmanı), dijital beceriler açısından daha yüksek bir yetkinlik

sergilemektedir. Bazı katılımcılar ise beceri seviyelerini net bir şekilde tanımlamak yerine semboller veya puanlama sistemi (örneğin 10/10) kullanmıştır, bu da bireysel değerlendirme farklılıklarını yansıtmaktadır.

3.3.7.2.2. Güvenirlik Analizi

Araştırma bulgularının bilimsel değerini belirleyen temel unsurlar arasında geçerlik ve güvenirlik yer almaktadır. Güvenirlik, bir ölçme aracının standart ve tekrarlanabilir sonuçlar üretme kapasitesini ifade ederken, geçerlik, ölçme aracının hedeflediği özelliği ne derece doğru ölçtüğünü açıklar (Ercan ve Kan, 2004: 211). Nicel araştırmalarda bu kavramlar belirli parametrelerle değerlendirilebilirken, nitel araştırmalarda ölçüm daha zordur. Bu nedenle nitel araştırmalarda inandırıcılık, sonuçların doğruluğu ve araştırmacının yetkinliği gibi kavramlar öne çıkmaktadır (Krefting, 1991'den akt. Başkale, 2016). Guba ve Lincoln (1982), geçerlik ve güvenirlik yerine inandırıcılık, güvenilirlik, onaylanabilirlik ve aktarılabilirlik olmak üzere dört ana kriterin sağlanmasını önermiştir (Creswell, 2003'ten akt. Başkale, 2016). Bu kriterlerden herhangi birinin veya birkaçının uygulanması, bulguların doğruluğunu kontrol etmek için yeterlidir.

Bu araştırmada inandırıcılığı sağlamak amacıyla görüşme soruları alan yazın incelenerek oluşturulmuş ve uzman görüşüne sunulmuştur. Uzmanların değerlendirdiği taslak form, anlaşılabilirlik ve kapsam açısından gözden geçirilmiş ve gerekli düzenlemeler yapılarak son haline getirilmiştir. Araştırma verileri, birbirinden bağımsız iki kodlayıcı tarafından MAXQDA programı kullanılarak kodlanmış ve kodlayıcılar arasında %85 benzerlik oranı sağlanmıştır; bu da kodlamanın güvenirliğini desteklemiştir (Miles ve Huberman, 1994). Araştırmada geçerlik, bulguların doğruluğunu, güvenirlik ise bulguların tekrarlanabilirliğini ifade etmektedir (Yıldırım ve Şimşek, 2013). Stenbacka (2001: 551), nicel araştırmalarda güvenirliğin açıklama amacıyla ilişkilendirildiğini, nitel çalışmalarda ise anlamlandırmaya odaklandığını belirtmiştir.

İnandırıcılık, araştırmanın her aşamasında nesnelliğin sağlanmasını içerir ve uzun süreli etkileşim, uzman incelemesi ve çeşitli kaynaklardan veri toplama gibi stratejilerle artırılabilir. Bu bağlamda, araştırma sırasında katılımcılarla derinlemesine görüşmeler yapılmış ve farklı araştırmacılardan kodlama ve tema oluşturma

süreçlerinde destek alınmıştır. Aktarılabilirlik, nitel araştırmaların genellenebilirlik yerine bulguların benzer ortamlara aktarılabilirliğini ifade eder. Bu amaçla detaylı veri toplama, amaçlı örnekleme ve ayrıntılı betimleme stratejileri kullanılmıştır. Tutarlılık, olguların değişkenliğini tutarlı bir şekilde yansıtmayı ifade eder ve bu araştırmada veri toplama ve analiz süreçlerinde danışman kontrolü ile sağlanmıştır. Doğrulanabilirlik, verilerin teyit edilebilirliğini içerir ve bu çalışmada kullanılan görüşme kayıtları, dökümler ve alınan izinler gibi materyaller saklanarak gerektiğinde incelenebilir hale getirilmiştir.

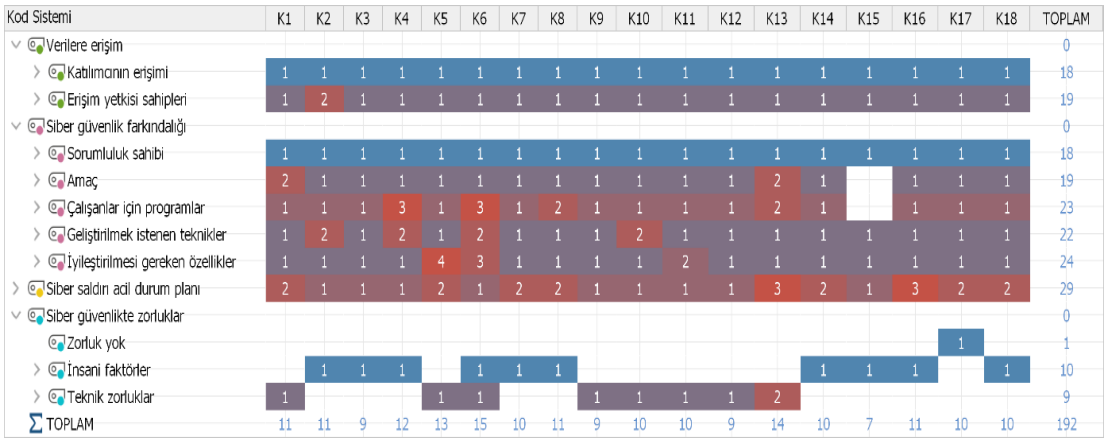
Creswell ve Plano Clark (2011), nitel araştırmalarda geçerliliği artırmak için uzman görüşü alma, detaylı betimleme ve yeterli kanıt sunma stratejilerini önermektedir. Bu araştırmada, veri toplama araçlarının geliştirilmesinden analiz süreçlerine kadar uzman görüşlerine başvurulmuş, dış denetleyicilerle çalışılmış ve elde edilen veriler farklı kaynaklarla karşılaştırılarak zenginleştirilmiştir. Ayrıca, verilerin toplanma süreci detaylı bir şekilde raporlanmış ve araştırmacının nasıl sonuçlara ulaştığı açıkça belirtilmiştir (Creswell, 2009). Çalışmada elde edilen bulgular, frekans bilgileri, katılımcıların demografik verileri, doğrudan alıntılar ve kavramsal kategoriler ile desteklenmiş, böylece çalışmanın geçerlik ve güvenirliği pekiştirilmiştir.

3.3.7.2.3. Kod, Alt Tema, Temalar

18 katılımcıdan elde edilen nitel veriler, MAXQDA Analytics Pro (Release 20.4.0) yazılımına aktarılmış ve analiz süreci bu yazılım üzerinden yürütülmüştür. Verilerin analizi için içerik analizi yöntemi kullanılmıştır. Her bir belgedeki katılımcı yanıtları satır satır incelenerek araştırmanın amaçlarına uygun bir şekilde kodlama yapılmıştır (Creswell, 2015; Creswell ve Poth, 2018). Elde edilen kodlar arasında benzerlikler belirlenmiş ve bu kodlar gruplandırılarak alt temalar oluşturulmuştur. Ardından, benzer alt temalar birleştirilerek daha kapsamlı temalar elde edilmiştir. Süreç boyunca dil ve içerik açısından iyileştirmeler yapılmıştır. Analiz sonucunda, verilerden 4 ana tema ve 9 alt tema ortaya çıkarılmış ve bu temalar araştırmanın bulgularını derinleştirmek amacıyla ayrıntılı bir şekilde incelenmiştir.

Bu bağlamda ortaya çıkan tema ve alt temalar MAXQDA programındaki kod-matris tarayıcı görünümü Şekil 3.2'de verilmiştir.

Şekil 3.2. Tema ve Alt Temalar

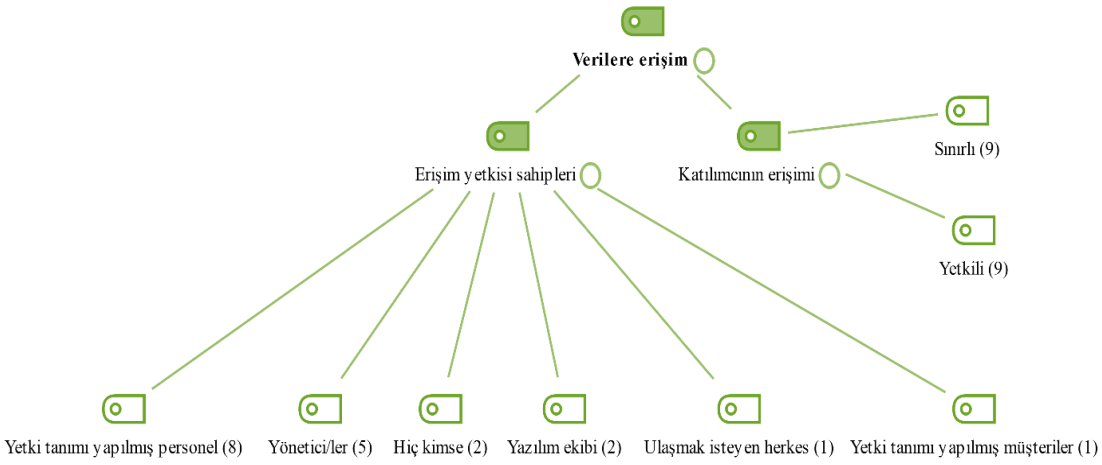


3.3.7.2.3.1. Verilere Erişim Teması

Bu bölümde nitel analiz sonucunda ortaya çıkan 4 tema ve 9 alt tema çerçevesinde bulgular sunulmuştur.

Verilere erişim temasına ilişkin alt temalar, bunların kodları ve frekansların Şekil 3. 3'deki hiyerarşik kod-alt kod modeli ile gösterilmiştir.

Şekil 3.3. Verilere Erişim Temasına İlişkin Alt Temaları Kodları ve Frekansları



Katılımcılara hassas verilere erişimlerinin olup olmadığı sorulmuştur. 9'u hassas verilere erişimde yetkili olduğunu, 9'u ise sınırlı erişime sahip olduğunu belirtmiştir.

"Birçok kişisel özel verilere sınırsız erişimim var." (K16)

"Yönetici olduğum için değil." (K9)

"Şirket içerisinde sınırlı" (K1)

"Evet" (K12)

Katılımcılara "Verilerinize kimler erişim sağlayabilir?" sorusu yöneltilmiştir. Katılımcıların 8'i verilerine yalnızca yetki tanımı yapılmış personelin erişim sağlayabileceğini belirtmiştir. 5 katılımcı, yöneticilerin erişim sağlayabileceğini ifade ederken, 2 katılımcı verilerine hiç kimsenin erişemediğini belirtmiştir. Bunun yanı sıra, 2 katılımcı yazılım ekibinin erişim sağlayabileceğini söylerken, 1 katılımcı verilerine ulaşmak isteyen herkesin erişebileceğini dile getirmiştir. Son olarak, 1 katılımcı ise yetki tanımı yapılmış müşterilerin verilerine erişim sağlayabileceğini belirtmiştir. Bu veriler, erişim yetkilerinin farklı gruplar arasında dağılımını ve katılımcıların algılarını yansıtmaktadır.

"*Admin seviyesinde yetki verilmiş kişiler*." (K11)

"Sadece yönetici" (K1)

"Hiç kimse" (K8)

"Yazılım ekibinden belirli kişiler pozisyonları çerçevesinde kısıtlı verilere erişimleri mevcuttur." (K13)

"Ulaşmak isteyen herkes" (K15)

"Yetki tanımı yapılmış olan personel ya da müşterilerimiz" (K2)

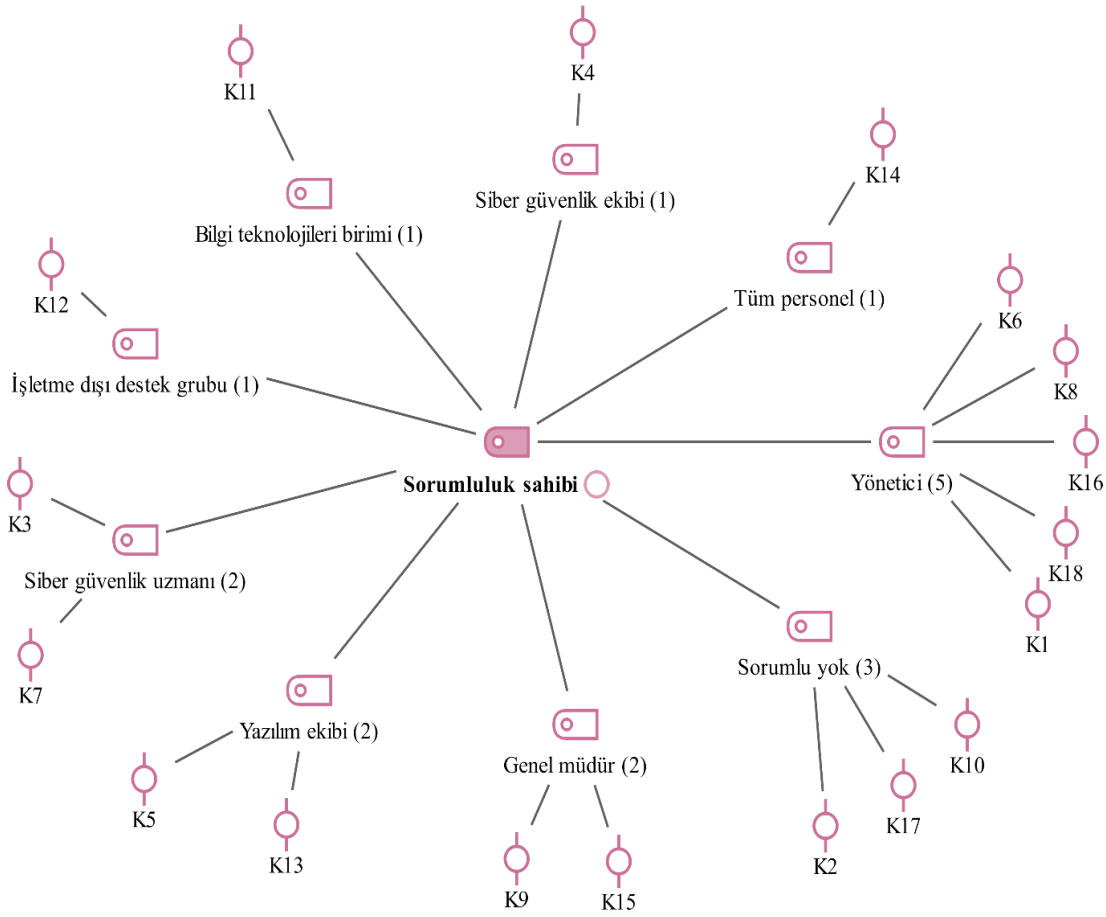
3.3.7.2.3.2. Siber Güvenlik Farkındalığı Teması

Siber güvenlik farkındalığı teması çerçevesinde ortaya çıkan 5 alt tema ayı ayrı başlıklarda sunulmuştur.

3.3.7.2.3.2.1. Sorumluluk Sahibi Teması

Siber güvenlik temasının alt teması olan sorumluluk sahibi alt temasının kodları ve frekansları kod-alt kod-bölümler modeli ile Şekil 3.4'te sunulmuştur.

Şekil 3.4. Sorumluluk Sahibi Alt Temasına İlişkin Kodlar ve Frekansları



Katılımcılara işletmelerinde siber güvenlik farkındalığından kimin sorumlu olduğu sorulmuştur. Katılımcıların 5'i bu sorumluluğun yöneticilere ait olduğunu belirtmiştir. 3 katılımcı işletmelerinde bu konuda herhangi bir sorumlu olmadığını ifade ederken, 2 katılımcı genel müdürün sorumlu olduğunu, 2 katılımcı ise yazılım ekibinin bu sorumluluğu üstlendiğini dile getirmiştir. Ayrıca, 2 katılımcı siber güvenlik uzmanını sorumlu olarak görürken, 1 katılımcı tüm personelin sorumlu olduğunu, 1 katılımcı işletme dışı bir destek grubunun bu sorumluluğu üstlendiğini, 1 katılımcı bilgi teknolojileri biriminin sorumlu olduğunu ve 1 katılımcı ise siber güvenlik ekibinin bu sorumluluğu taşıdığını ifade etmiştir. Bu bulgular, siber güvenlik farkındalığı sorumluluğunun organizasyonel rollere ve yapılandırmalara göre farklılaştığını göstermektedir.

"Kapalı bir çalışma şeklimiz var. gerekli bilgilendirmeleri yönetici yapıyor." (K18)

"Tam anlamıyla siber güvenlik departmanımız yok." (K17)

"Genel Müdür" (K9)

"Yazılım ekibi" (K5)

"Siber güvenlik uzmanı sorumlu" (K7)

"Tüm çalışanlar" (K14)

"Dışarıdan destek alıyoruz." (K12)

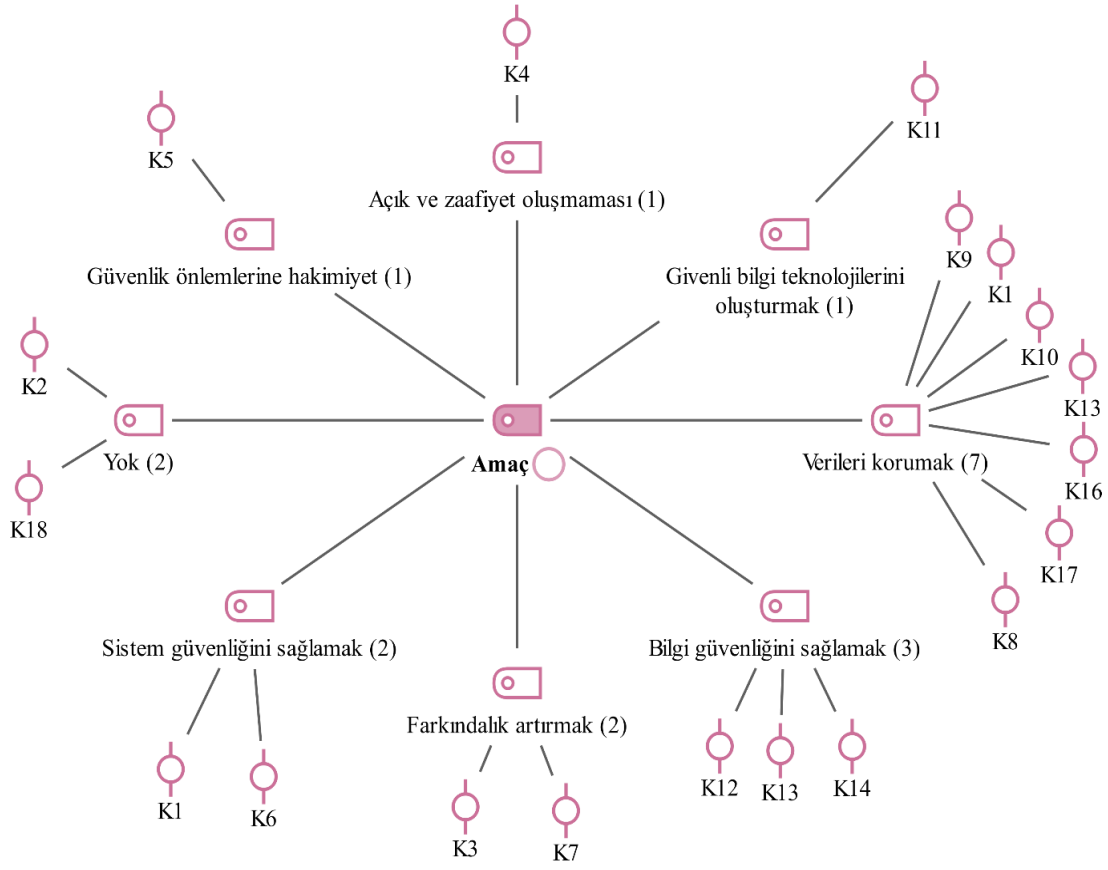
"BT Teknolojileri Birimi" (K11)

"Siber güvenlik ekibimiz var ayrıca farkındalık oluşması için tüm personelimize siber güvenlik alanında eğitim aldırıldı." (K4)

3.3.7.2.3.2.2. Amaç Teması

Siber güvenlik temasının alt teması olan amaç alt temasının kodları ve frekansları kod-alt kod-bölümler modeli ile Şekil 3.5'te sunulmuştur.

Şekil 3.5. Amaç Alt Temasına İlişkin Kodlar ve Frekansları



Katılımcılara işletmelerinde siber güvenlik farkındalığı girişimlerinin amacı sorulmuştur. Katılımcıların 7'si bu girişimlerin amacını verileri korumak olarak ifade etmiştir. 3 katılımcı bilgi güvenliğini sağlamak, 2 katılımcı farkındalık artırmak ve 2 katılımcı sistem güvenliğini sağlamak amacıyla bu tür girişimlerde bulunduklarını belirtmiştir. Bunun yanı sıra, 1 katılımcı güvenli bilgi teknolojilerini oluşturmak, 1 katılımcı güvenlik önlemlerine hakimiyet sağlamak ve 1 katılımcı açık ve zaafiyet oluşmamasını sağlamak olarak bu girişimlerin amacını açıklamıştır. Ancak, 2 katılımcı işletmelerinde böyle bir amacın bulunmadığını ifade etmiştir. Bu veriler, işletmelerin siber güvenlik girişimlerine yönelik farklı bakış açılarını ve önceliklerini ortaya koymaktadır.

"Kendi sistem güvenliğimiz, verilerimizin kaybolmaması ön muhasebe firması olduğumuz için kullanıcı adı verileri bizim için çok önemli bir veri kaybı bile çok büyük maddi zarara yol açabiliyor bu yüzden siber güvenlik farkındalığı bizim için çok önemi." (K1)

"Bilgi güvenliği" (K12)

"Siber güvenlik farkındalığı" (K3)

"Başta işletmemiz olmak üzere bizimle çalışan müşterilerimizin ve aynı zamanda kendi güvenliğimizi sağlamak." (K6)

"Daha Güvenli bir BT oluşturma" (K11)

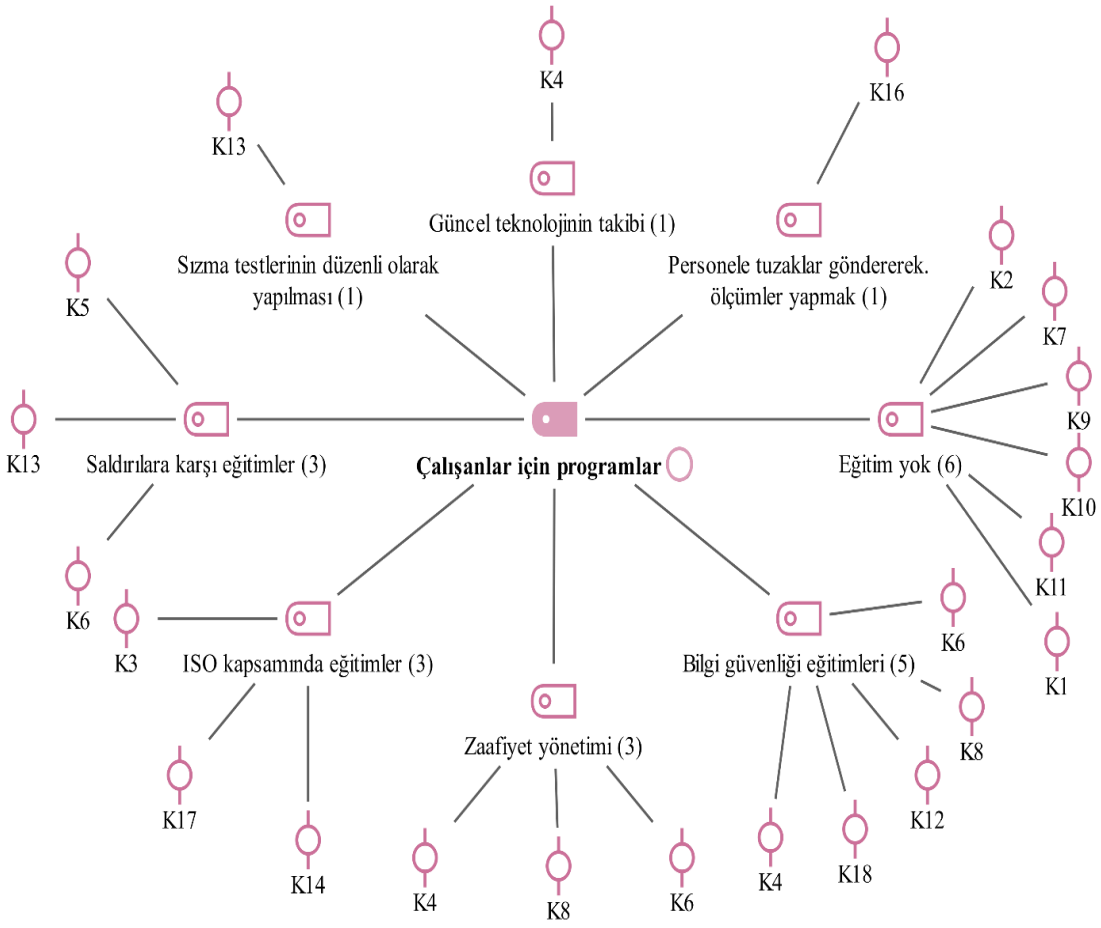
"Siber saldırılara karşı güvenlik önlemlerine hâkimiyet." (K5)

"Geliştirmelerimizde ve sistemde açık ve zafiyetin oluşmaması." (K4)

3.3.7.2.3.2.3. Çalışanlar için programlar Teması

Siber güvenlik temasının alt teması olan çalışanlar için programlar alt temasının kodları ve frekansları kod-alt kod-bölümler modeli ile Şekil 3.6'te sunulmuştur.

Şekil 3.6. Çalışanlar İçin Programlar Alt Temasına İlişkin Kodlar ve Frekansları



Katılımcılara çalışanlarına rutin olarak ne tür siber önleme eğitimi ve öğretimi sağladıkları sorulmuştur. Katılımcıların 6'sı herhangi bir eğitim verilmediğini belirtmiştir. 5 katılımcı bilgi güvenliği eğitimleri verdiklerini ifade ederken, 3 katılımcı saldırılara karşı (örneğin, DDoS, kimlik avı, XSS, SQL injection gibi) eğitimler sağladıklarını dile getirmiştir. Ayrıca, 3 katılımcı zaafiyet yönetimi eğitimleri, 3 katılımcı ise ISO standartları kapsamında eğitimler verdiklerini belirtmiştir. Bunların yanı sıra, 1 katılımcı personele tuzaklar göndererek ölçümler yaptıklarını, 1 katılımcı düzenli olarak sızma testleri gerçekleştirdiklerini ve 1 katılımcı güncel teknolojilerin takibini sağladıklarını ifade etmiştir. Bu bulgular, işletmelerin çalışanlarını siber güvenlik konusunda eğitme konusundaki yaklaşımlarının çeşitlilik gösterdiğini ortaya koymaktadır.

"Şu an öyle bir eğitimimiz yok fakat ilerleyen süreçte haftada bir gün böyle bir eğitim vermeyi düşünüyoruz." (K7)

"Periyodik olarak çalışanlarımız temel siber güvenlik eğitimlerine katılmaktadır." (K12)

"ddos , kimlik avı , xss sql injection gibi saldırılara karşı güvenlik önlemleri" (K5)

"Temel Teknolojileri & Network Bileşenleri, Host/Ağ/Port Keşif ve Tarama, DOS/DDOS Saldırıları ve Korunma Yöntemleri, Açıklık Tarama ve Zafiyet Tespiti vb. gerekli olan temel siber eğitimleri sağlıyoruz." (K6)

"Farkındalık eğitimleri ISO 27001 kapsamında yılda bir kez." (K3)

"Kendi personellerime tuzaklar gönderip yakalanıp yakalanmadıklarını ölçüyorum. Güncellemelerden sonra güncelleme eğitimleri veriyoruz." (K16)

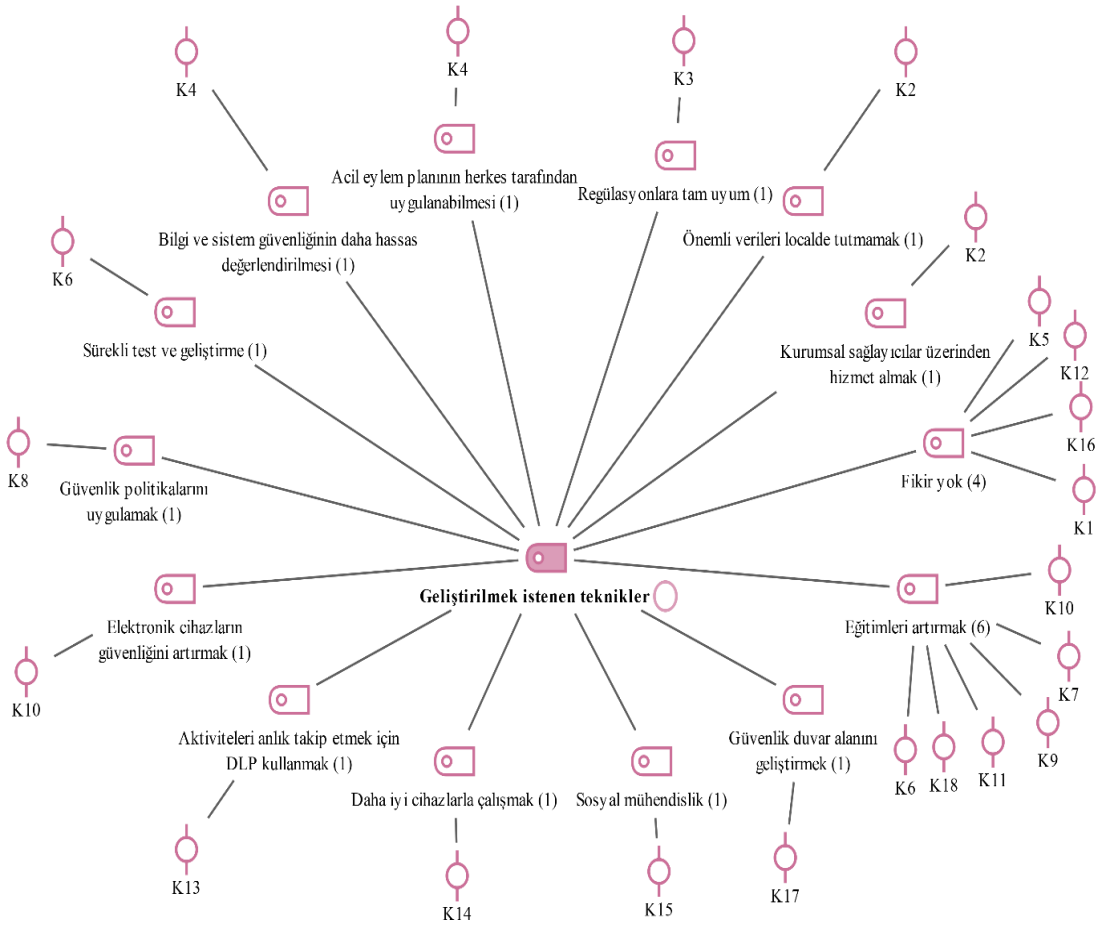
"6 ayda bir 3. Parti firmalardan sızma testi hizmeti alınmaktadır, ilgili firmalardan sızma testi öncesi veya sonrası en güncel bilgileri de içeren eğitimler alınmaktadır." (K13)

"Güncel teknolojilerin takibi, bilgi güvenliği eğitimleri, zaafiyet yönetimi" (K4)

3.3.7.2.3.2.4. Geliştirilmek İstenen Teknikler Teması

Siber güvenlik temasının alt teması olan geliştirilmek istenen teknikler alt temasının kodları ve frekansları kod-alt kod-bölümler modeli ile Şekil 3.7'da sunulmuştur.

Şekil 3.7. Geliştirilmek İstenen Teknikler Alt Temasına İlişkin Kodlar ve Frekansları



Katılımcılara işletmelerinde güvenlik farkındalığını artırmak için geliştirmek istedikleri teknikler sorulmuştur. Katılımcıların 4'ü bu konuda herhangi bir fikir belirtmemiştir. 6 katılımcı, güvenlik politikaları, e-posta ve mesaj güvenliği gibi konularda eğitimlerin artırılması gerektiğini, uygulamalı ve örnekli eğitimlerin daha etkili olabileceğini ifade etmiştir. Bunun dışında, 1 katılımcı güvenlik duvar alanını geliştirmek gerektiğini, 1 katılımcı sosyal mühendislik yöntemlerini kullanmayı düşündüğünü, 1 katılımcı daha iyi cihazlarla çalışmayı planladığını ve 1 katılımcı anlık aktiviteleri takip etmek için DLP kullanmak istediğini belirtmiştir. Ayrıca, 1 katılımcı elektronik cihazların güvenliğini artırmayı, 1 katılımcı güvenlik politikalarını uygulamayı, 1 katılımcı sürekli test ve geliştirme süreçlerini önemsemeyi ifade etmiştir. Diğer öneriler arasında bilgi ve sistem güvenliğinin daha hassas değerlendirilmesi, acil eylem planlarının herkes tarafından uygulanabilir olması, regülasyonlara tam uyum, önemli verilerin localde tutulmaması ve kurumsal

sağlayıcılar üzerinden hizmet alınması yer almaktadır. Bu bulgular, işletmelerin güvenlik farkındalığını artırma konusunda farklı yöntemler ve stratejiler geliştirme çabası içerisinde olduğunu göstermektedir.

"Siber güvenlik uzmanı olmadığım için bu konuda pek bir fikrim yok." (K1)

"Sürekli test ve geliştirme, güvenlik politikaları, eposta ve mesaj güvenliği eğitimleri" (K6)

"Güvenlik duvar alanlarını geliştirmek istiyoruz." (K17)

"Sosyal mühendislik" (K15)

"Personellerimiz laboratuvar ve canlı ortamlarda bizzat işlemler yaparak uygulamalarla öğreniyor. Daha yüksek bütçeler ve daha iyi cihazlarla çalışmak isterdik." (K14)

"Çalışan kişilerden kaynaklı bir güvenlik açığı vermek istemeyiz, çalışanların yaptığı aktiviteleri anlık takip edip gerekli uyarıları anlık almak için bir DLP programı kullanımı gerçekleştirmek isteriz." (K13)

"Partner firmalardan eğitim hizmeti ile kullanılan elektronik cihazlarımızın güvenliğini sağlamak." (K10)

"*Güvenlik politikaların anlatımı ve kullanılması"* (K8)

"Developer seviyesine kadar bilgi ve sistem güvenliği konusunun hassas ele alınması. Acil eylem planlarının oluşturulup gerektiğinde herkes tarafından uygulanabilir olması." (K4)

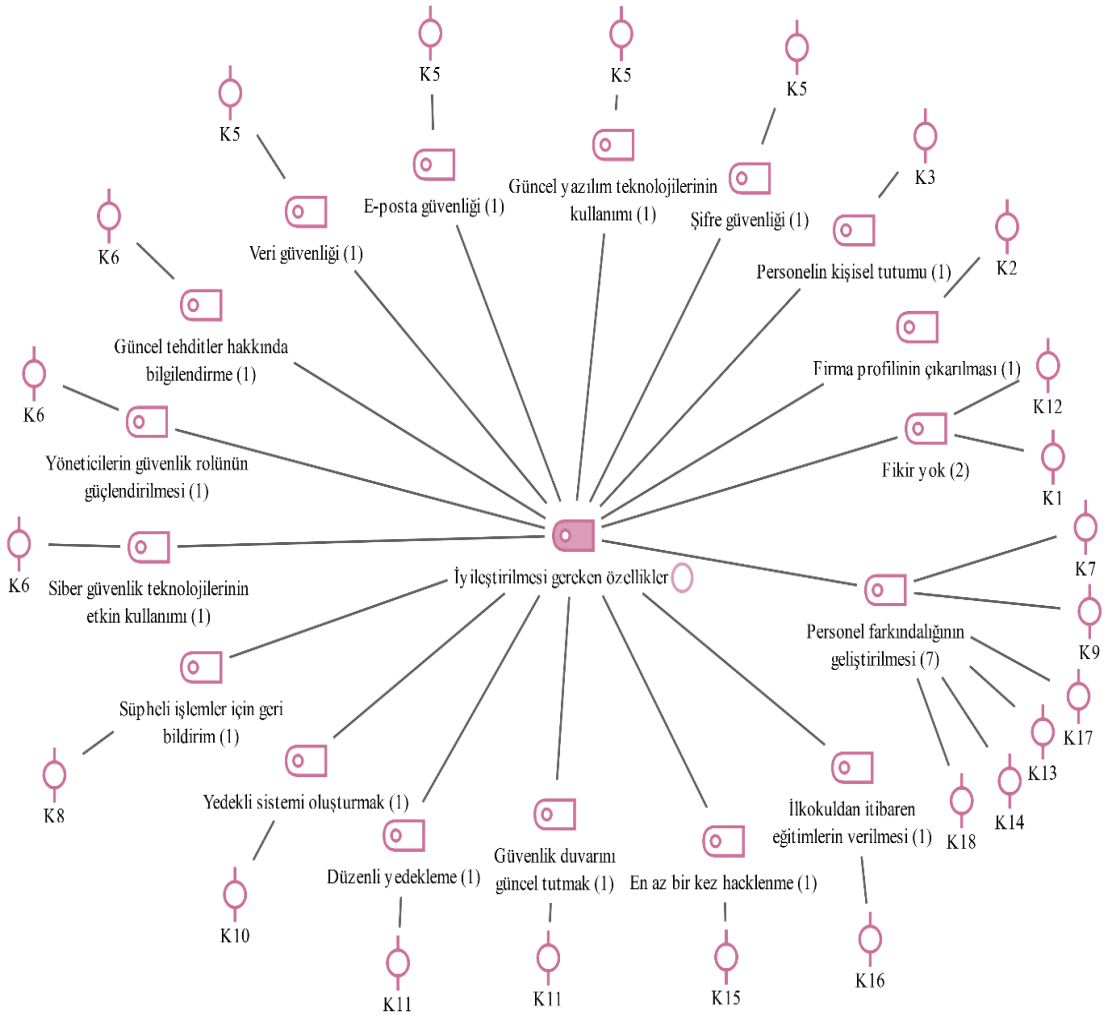
"Regülasyonlara tam uyum." (K3)

"Kurumsal sağlayıcılar üzerinden hizmetler alarak localimizde herhangi bir önemli veri tutmamak." (K2)

3.3.7.2.3.2.5. İyileştirilmesi gereken özellikler Teması

Siber güvenlik temasının alt teması olan iyileştirilmesi gereken özellikler alt temasının kodları ve frekansları kod-alt kod-bölümler modeli ile Şekil 3.8'de sunulmuştur.

Şekil 3.8. İyileştirilmesi Gereken Özellikler Alt Temasına İlişkin Kodlar ve Frekansları



Katılımcılara siber güvenlik farkındalığında hangi özelliklerin iyileştirilmesi gerektiği sorulmuştur. Katılımcıların 7'si personel farkındalığının geliştirilmesi gerektiğini vurgulamıştır. 2 katılımcı herhangi bir fikir belirtmezken, diğer katılımcılar farklı önerilerde bulunmuştur. Bu öneriler arasında ilkokuldan itibaren eğitimlerin verilmesi, en az bir kez hacklenme deneyiminin farkındalık yaratabileceği, güvenlik duvarının güncel tutulması, düzenli yedekleme yapılması, yedekli bir sistemin oluşturulması ve şüpheli işlemler için geri bildirim mekanizmalarının geliştirilmesi yer almıştır. Ayrıca, siber güvenlik teknolojilerinin etkin kullanımı, yöneticilerin güvenlik rolünün güçlendirilmesi, güncel tehditler hakkında bilgilendirme yapılması, veri güvenliği, e-posta güvenliği, güncel yazılım teknolojilerinin kullanımı ve şifre güvenliğinin sağlanması gerektiği belirtilmiştir. Diğer öneriler arasında personelin kişisel tutumunun iyileştirilmesi ve firma profilinin çıkarılması gibi daha spesifik

öneriler de bulunmaktadır. Bu bulgular, siber güvenlik farkındalığının artırılması için geniş bir yelpazede iyileştirme alanları olduğunu göstermektedir.

"Siber güvenlik uzmanı olmadığım için bu konuda pek bir fikrim yok." (K1)

"Çalışanların daha fazla eğitilmesi ve güvenlik konusunda daha hassas olmaları, yaptıkları bir işlemin tehdit oluşturup oluşturmayacağını anlamaları konularının iyileştirilmesi gerekir." (K13)

"Bu eğitimin ilkokuldan itibaren verilmesi gerekiyor." (K16)

"Herkesin maddi yada manevi olarak ciddi zarar görebilecek şekilde en az 1 kez hacklenmesi gerekiyor." (K15)

"Düzenli Yedekleme, Güvenlik duvarını Virus yazılımlarını güncel tutma." (K11)

"Siber saldırı ihtimalinin her an yaşanabileceği ve yedekli bir sistemin oluşturulması." (K10)

"Şüpheli faaliyetler yada işlemlerde geri bildirim." (K8)

"Güncel tehditler hakkında bilgilendirme, yöneticilerin güvenlik rolünün güçlendirilmesi, siber güvenlik teknolojilerinin etkin kullanımı" (K6)

"Şifre güvenliği, güncel yazılım teknolojilerinin kullanımı, e-posta ve veri güvenliği." (K5)

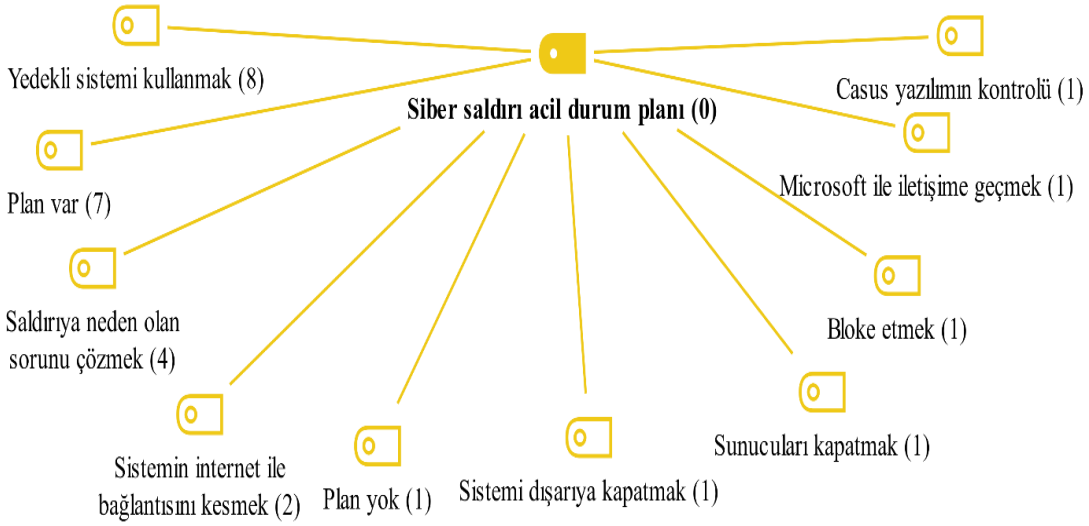
"Personel kişisel tutumları" (K3)

"Firma profili çıkarılarak eksiklerimizin tespit edilebilmesi için gerekli testlerin firmamıza yapılması." (K2)

3.3.7.2.3.3. Siber Saldırı Acil Durum Planı Teması

Siber saldırı acil durum planı temasına ilişkin kodlar ve frekansları Şekil 3.9'deki hiyerarşik kod-alt kod modeli ile gösterilmiştir.

Şekil 3.9. Siber Saldırı Acil Durum Planı Temasına İlişkin Kodlar ve Frekansları



Katılımcılara bir siber saldırı meydana gelmesi durumunda acil durum planlarının ne olduğu sorulmuştur. Katılımcıların 8'i yedekli sistemi kullanacaklarını ifade etmiştir. 7 katılımcı bir acil durum planlarının olduğunu belirtirken, 1 katılımcı herhangi bir planlarının olmadığını dile getirmiştir. Diğer yanıtlar arasında, saldırıya neden olan sorunun çözülmesi gerektiği (4 katılımcı), sistemin internet ile bağlantısının kesilmesi (2 katılımcı), sistemin dışarıya kapatılması (1 katılımcı), Microsoft ile iletişime geçilmesi (1 katılımcı), sunucuların kapatılması (1 katılımcı), casus yazılımın kontrol edilmesi (1 katılımcı), saldırının bloke edilmesi (1 katılımcı), USOM yönergelerine göre hazırlanan planların uygulanması (1 katılımcı) ve yetkililerin planı uygulaması (1 katılımcı) bulunmaktadır. Bu bulgular, işletmelerin siber saldırı durumlarına yönelik farklı yaklaşımlar ve önlemler geliştirdiğini göstermektedir. Ayrıca, yedekli sistemlerin öneminin ön plana çıktığı anlaşılmaktadır.

"Acil durum planı olarak sürekli sunucular arası yedekleme yaptığımız için tam anlamıyla planımız yok." (K17)

"Felaket senaryomuz dahilinde, kurduğumuz yedek altyapısıyla kesinti olmadan işlemlerimize devam edebilmekteyiz." (K12)

"Ekibimiz var acil eylem planı bulunmaktadır." (K4)

"Yedek serverın devreye alınması, mevcut sistemin internet ile ilişkisi kesilmesi." (K8)

"Kaynağı bulup engellemek. yedekleme sistemine dönmek. (Yedeğin Yedeğin Yedeği var)" (K18)

"Microsoft Türkiye ile iletişime geçmek." (K10)

"Sunucuları kapatmak, yedekli sistem kullanmak bu sayede saldırıya maruz kalan dışında sistemin çalışmaya devam etmesi sağlanıyor." (K7)

"Sunucu üzerinden bloke etmek ve yazılım içerisinde çalışan casus yazılım kontrolü." (K5)

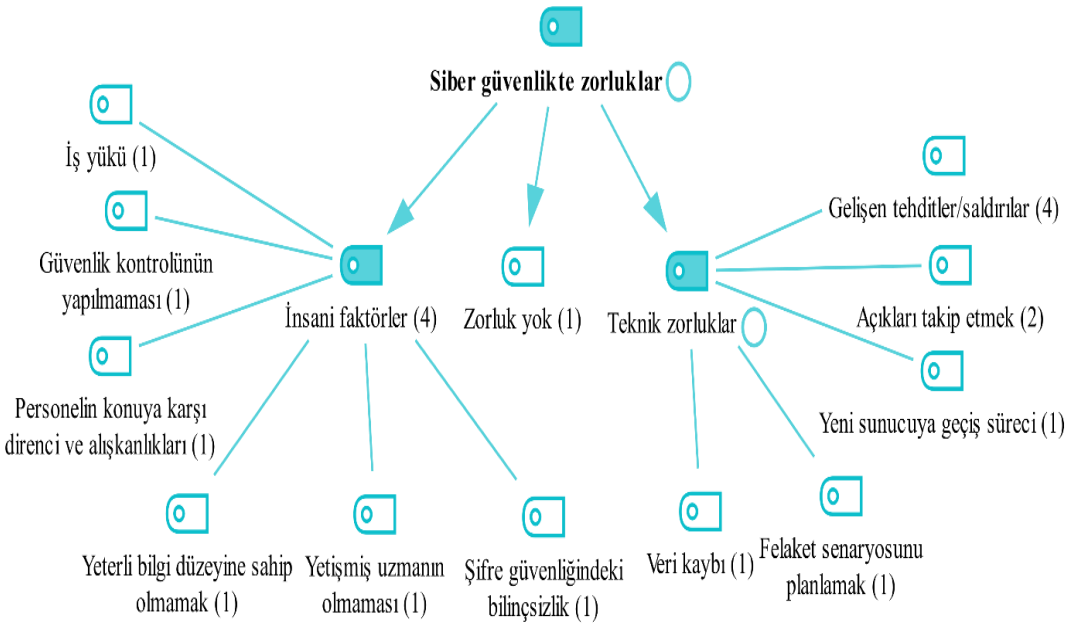
"USOM yönergelerinde hazırladığımız acil eylem planları geçerlidir." (K3)

"Bir önleme planımız var olası bir durumda önce bir haber geliyor sonra yetkili kişi plan doğrultusunda müdahale eder." (K1)

3.3.7.2.3.4. Siber Güvenlikte Zorluklar Teması

Siber güvenlikte zorluklar temasına ilişkin alt temalar, kodlar ve frekansları Şekil 3.10'daki hiyerarşik kod-alt kod modeli ile gösterilmiştir.

Şekil 3.10. Siber Güvenlikte Zorluklar Temasına İlişkin Alt Temalar, Kodlar ve Frekansları



Katılımcılara siber güvenlik konusunda en çok zorlandıkları şey sorulmuştur. 1 katılımcı herhangi bir zorluk yaşamadığını ifade etmiştir. Katılımcıların 4'ü siber güvenlikte insani faktörlerin önemli bir zorluk olduğunu belirtmiştir. Diğer insani

zorluklar arasında iş yükü (1 katılımcı), güvenlik kontrollerinin yapılmaması (1 katılımcı), personelin konuya karşı direnci ve alışkanlıkları (1 katılımcı), yetişmiş uzmanın olmaması (1 katılımcı), yeterli bilgi düzeyine sahip olmamak (1 katılımcı) ve şifre güvenliği konusundaki bilinçsizlik (1 katılımcı) yer almıştır. Bu bulgular, çalışanların bilgi ve davranışları ile ilgili sorunların siber güvenlikte önemli bir etken olduğunu göstermektedir.

"Yedek aldığımız için zorlandığımız bir konu bulunmamaktadır." (K17)

"Lokasyondaki personellerin hataları." (K16)

"Nas Sistemi üzerinden versiyon kontrollü yedekleme ve yetkilendirme yapılıyor. bu kurulumları yönetmek bunun getirdiği iş yükü." (K18)

"Son kullanıcının mail yada bilgilerini güvenlik kontrolü yapmadan kullanması." (K8)

"Personel direnci, alışkanlıklar" (K3)

"Yetişmiş uzman" (K4)

"Konu hakkında yeterli bilgi birikime sahip değiliz. Bu konuda danışmanlık hizmetleri alıyoruz." (K2)

"Kullanıcıların şifre güvenliği konusunda bilinçsiz olması" (K7)

Teknik zorluklar arasında en fazla belirtilen sorun, gelişen tehditler ve saldırılar (4 katılımcı) olmuştur. Bunun yanı sıra, açıkları takip etmek (2 katılımcı), yeni sunucuya geçiş süreci (1 katılımcı), veri kaybı (1 katılımcı) ve felaket senaryolarının planlanması (1 katılımcı) gibi teknik sorunlar dile getirilmiştir. Bu bulgular, hızla değişen teknolojik ortamın ve siber tehditlerin işletmeler için önemli bir zorluk teşkil ettiğini ortaya koymaktadır.

"Her geçen gün yeni bir sistem açığı veya tehdit çıkabilmektedir bunların takibini yapmak zorlayıcı olmaktadır." (K13)

"Sürekli çıkan açıkları takip etmek." (K9)

“Sunucularımıza saldırı olmuştu bu süreçte sunucuların tanınması ve yeni bir sunucuya geçiş süreci baya zorlu olmuştu.” (K1)

*“sql injection sonrası veri kaybı.” (*K5)

“Felaket senaryosunun planlanması” (K12)

TARTIŞMA, SONUÇ VE ÖNERİLER

Dijital dönüşüm, işletmelerin teknolojiyi kullanarak iş süreçlerini daha verimli, esnek ve yenilikçi hale getirme sürecidir. Küresel ekonominin hızla dijitalleştiği günümüzde, bu dönüşüm yalnızca büyük ölçekli firmalar için değil, aynı zamanda KOBİ'ler için de kritik bir gereklilik haline gelmiştir. KOBİ'lerin dijital dönüşümü benimsemeleri, rekabet avantajı sağlamak, verimlilik artırmak ve sürdürülebilir büyüme elde etmek açısından büyük bir öneme sahiptir. Bununla birlikte, dijital dönüşüm sürecinin her aşamasında siber güvenlik, KOBİ'lerin en fazla dikkat etmeleri gereken unsurlardan biri olarak öne çıkmaktadır.

KOBİ'ler, dijital dönüşümü benimseyerek operasyonel süreçlerini modernize edebilir, müşteri deneyimlerini iyileştirebilir ve yeni pazar fırsatlarına ulaşabilirler. Bu dönüşüm, bulut bilişim, veri analitiği, e-ticaret platformları ve otomasyon araçları gibi dijital teknolojilerin entegrasyonunu içermektedir. Dijitalleşme, KOBİ'lerin daha hızlı kararlar almasını, kaynaklarını daha etkin bir şekilde kullanmasını ve operasyonel maliyetlerini azaltmasını sağlar. Ancak, KOBİ'lerin dijitalleşmesiyle birlikte, karşı karşıya kaldıkları siber tehditler de artmaktadır. Geleneksel güvenlik önlemleri, günümüzün gelişmiş siber tehditlerine karşı yetersiz kalabilir. Küçük işletmelerin, büyük ölçekli şirketlere kıyasla daha sınırlı kaynaklara sahip olmaları, onları siber saldırılar karşısında daha savunmasız hale getirebilir. Özellikle fidye yazılımı saldırıları, veri ihlalleri ve kötü amaçlı yazılımlar gibi tehditler, KOBİ'ler için ciddi güvenlik riskleri oluşturur.

KOBİ'lerin siber güvenlik önlemlerini ihmal etmeleri, yalnızca müşteri verilerini tehlikeye atmakla kalmaz, aynı zamanda işletmenin itibarını zedeleyebilir ve yasal yaptırımlara neden olabilir. Bu nedenle, dijital dönüşüm sürecinde siber güvenliğin ön planda tutulması son derece önemlidir. KOBİ'ler için en temel güvenlik önlemleri arasında güçlü şifrelerin kullanımı, iki faktörlü kimlik doğrulama, düzenli yedeklemeler, güvenlik duvarları ve antivirüs yazılımları bulunmaktadır.

Dijital dönüşüm ve siber güvenlik, yalnızca teknolojik bir mesele olmanın ötesindedir. Dijitalleşen işletmeler, bu süreçlerin etkin bir şekilde yönetilmesi için

stratejik bir yaklaşım benimsemek zorundadır. KOBİ'ler için dijital dönüşüm, yalnızca teknoloji yatırımları yapmakla sınırlı kalmayıp, aynı zamanda bu yatırımların güvenliğini sağlamakla da doğrudan ilişkilidir. Bu bağlamda, siber güvenlik dijital dönüşüm sürecinin ayrılmaz bir parçasıdır ve KOBİ'lerin uzun vadeli başarısı için kritik bir öneme sahiptir.

Sonuç olarak, KOBİ'ler dijital dönüşüm süreçlerini hızla benimserken, aynı zamanda güçlü bir siber güvenlik stratejisi oluşturmak zorundadır. Bu iki faktörün dengeli bir biçimde yönetilmesi, KOBİ'lerin gelecekteki başarılarını güvence altına alacaktır. Dijitalleşen dünyada, güvenlik önlemlerinin ihmal edilmemesi, iş sürekliliğini sağlamak ve rekabette öne çıkmak için büyük bir avantaj sağlayacaktır. Çalışmada Konya ilinde bilişim sektöründe faaliyet gösteren KOBİ çalışanlarının siber güvenlik farkındalıklarının demografik özelliklerine göre farlılık gösterip göstermediği belirlenmeye çalışılmıştır. Sonuçlar çalışmaya katılan kullanıcıların yanıtlarına göre yorumlanmıştır.

Siber güvenlik farkındalığını incelemek amacıyla yapılan araştırmanın sonuçları araştırma örneklemini oluşturan çalışanların cevapları bağlamında yürütülen analizlerin sonuçlarına göre değerlendirilmiş ve aşağıda maddeler halinde özetlenmiştir:

Cinsiyet üzerine elde edilen bulgulara bakıldığında, Keser, Çetinkaya ve Güldüren (2016) ve Yılmaz, Şahin ve Akbulut (2016) çalışmalarında erkek öğrenci ve öğretmenlerin siber güvenlik farkındalığının kadınlardan daha yüksek olduğu belirtilmiştir. Bununla birlikte, Arıtürk (2015) ve Nezgitli ve Gökçearslan (2022) gibi çalışmalar cinsiyet açısından anlamlı bir fark bulunmadığını rapor etmiştir. Yiğit ve Seferoğlu (2019) tarafından yapılan çalışmada kadın ve erkek öğrencilerin siber güvenlik sağlama durumları arasında anlamlı bir farklılık bulunmamıştır. Bu çalışmada ise, Cinsiyet değişkeni ile SGFÖ'nün geneline verilen cevaplar arasında istatistiki olarak anlamlı bir farklılaşma olduğu görülmüştür. Bu bulgu, erkek ve kadın katılımcıların siber güvenlik konusundaki bilgi seviyelerinin birbirinden farklı olduğunu göstermektedir.

Yaş üzerine elde edilen bulgulara bakıldığında, Gökmen ve Akgün (2015) ve diğer bazı çalışmalarda da yaşın siber güvenlik bilgisinde belirleyici bir faktör olmadığı gözlenmiştir. Ancak, Yılmaz ve diğerleri (2016) gibi çalışmalar yaş ve kullanım sıklığının farkındalık düzeyinde önemli rol oynadığını bildirmiştir. Bu çalışmada ise, Yaş değişkeni ile SGFÖ'nün geneline verilen cevaplar arasında istatistiki olarak anlamlı bir farklılaşma olduğu görülmüştür. Bu bulgu, bireylerin yaş gruplarına bağlı olarak siber güvenlik konusundaki farkındalık düzeylerinin farklılık gösterebileceğini ortaya koymaktadır.

Eğitim durumu üzerine elde edilen bulgulara bakıldığında, Oktay ve Çakır (2012) ve Tekerek ve Tekerek (2013) çalışmaları eğitim seviyesi arttıkça siber güvenlik farkındalığının arttığını göstermiştir. Bu çalışmada ise, Eğitim Durumu değişkeni ile SGFÖ'nün sadece geneline verilen cevaplar arasında istatistiki olarak anlamlı bir farklılaşma olduğu görülmüştür. Bu bulgu, Eğitim durumu ile siber güvenlik farkındalığı arasında belirgin bir ilişki olduğunu göstermektedir. Yüksek eğitim seviyesine sahip bireylerin siber güvenlik tehditlerine karşı daha fazla bilgiye sahip olma eğiliminde olduklarını göstermektedir. Bu durum, eğitim programlarının ve farkındalık kampanyalarının, siber güvenlik bilincinin artırılması açısından önemli bir rol oynadığını ortaya koymaktadır.

Çalışma süresi üzerine elde edilen bulgulara bakıldığında, Çalışma süresi değişkeni ile siber güvenlik farkındalığı ölçeği üzerinden verilen cevaplar arasında anlamlı bir farklılık bulunmuştur. Bu sonuç, katılımcıların çalışma sürelerinin, siber güvenlik konusundaki farkındalık düzeyleri üzerinde belirgin bir etki yarattığını göstermektedir. Diğer bir deyişle, bireylerin çalışma deneyimlerinin süresi arttıkça, siber güvenlik bilgisi ve farkındalık seviyelerinde önemli değişiklikler gözlemlenmektedir. Bu durum, daha uzun süreli çalışma deneyiminin, siber güvenlik konusunda daha yüksek bilinç ve bilgi düzeyi ile ilişkili olduğunu ortaya koymaktadır.

İşletmedeki pozisyon üzerine elde edilen bulgulara bakıldığında, İşletmedeki Pozisyon değişkeni ile SGFÖ'nün geneline verilen cevaplar arasında istatistiki olarak anlamlı bir farklılaşma olmadığı görülmüştür. Bu sonuç, katılımcıların işletmedeki

görev ya da pozisyonlarına bağlı olarak siber güvenlik konusundaki farkındalık seviyelerinde belirgin bir değişiklik olmadığını ortaya koymaktadır.

- ***Bilgisayar güvenliğinin sağlanmasının önemi:*** Çalışanlar, bilgisayar güvenliğinin sağlanmasının önemini vurgulamaktadır. Bu durum, katılımcıların bilgisayar güvenliğine ciddi bir şekilde odaklandıklarını ve dijital tehditlere karşı yüksek bir duyarlılığa sahip olduklarını göstermektedir. Ayrıca, bireylerin siber güvenlik kültürünü benimsedikleri ve bu alandaki farkındalık seviyelerinin yüksek olduğu söylenebilir. Bu bağlamda, şirketlerin bilgisayar güvenliğini sağlamak amacıyla kapsamlı bir organizasyonel güvenlik politikası geliştirmeleri ve düzenli eğitim programları uygulamaları gerektiği sonucuna varılmaktadır.
- ***Şifre güvenliği ve saklanması:*** Şirket çalışanları, şifrelerini büyük bir özenle saklamaktadır. Bu durum, katılımcıların kişisel güvenliklerine önem verdiklerini ve şifrelerini kötü niyetli saldırılardan korumak için gerekli önlemleri aldıklarını göstermektedir. Şifre güvenliğine gösterilen bu yüksek dikkat, katılımcıların dijital ortamda kendilerini koruma bilincine sahip olduklarını ve potansiyel siber tehditlere karşı proaktif bir yaklaşım benimsediklerini göstermektedir. Bu da, bireylerin güvenlik alışkanlıklarının olgunlaştığını ve düzenli olarak bu alışkanlıkları uyguladıklarını ortaya koymaktadır.
- ***Karmaşık şifrelerin oluşturulması:*** Çalışanlar, şifre oluştururken semboller, sayılar ve büyük harfler gibi karmaşık ögeler içeren, tahmin edilmesi güç şifreleri tercih etmektedir. Bu, katılımcıların güvenli şifre oluşturma konusunda bilgiye sahip olduklarını ve bu alanda bilinçli bir yaklaşım benimsediklerini göstermektedir. Karmaşık şifreler seçmek, kullanıcıların güvenlik risklerini azaltmalarına katkı sağlamaktadır ve bu, katılımcıların dijital güvenlik kültürünü güçlü bir şekilde benimsediklerinin bir göstergesi olarak değerlendirilebilir. Ayrıca, kullanıcıların güçlü şifreler seçme alışkanlıklarının yerleştiği ve bu konuya dikkat ettikleri anlaşılmaktadır.
- ***Şifre paylaşmama alışkanlığı:*** Çalışanlar, şifre paylaşmama konusunda kararlı bir tutum sergilediklerini göstermektedir. Şifre paylaşımının

yasaklanması, temel bir güvenlik ilkesi olarak kabul edilmektedir ve bu tutum, siber güvenlik bilincinin yüksek olduğunu göstermektedir. Ayrıca, kişisel verilerin gizliliği ve güvenliği konusunda verilen önemin arttığını işaret etmektedir. Şifre paylaşmama alışkanlığının yerleşmesi, organizasyondaki güvenlik politikalarına olan bağlılığı ve bu politikaların kabulünü de göstermektedir.

- ***E-posta gönderiminde şifreleme kullanımı ile ilgili***, katılımcıların e-posta güvenliği konusunda yeterince dikkatli olmadıklarını ya da şifreleme yöntemlerine dair bilgi eksikliklerinin bulunduğunu gösterebilir. Şifreleme, e-posta içeriklerinin güvenliğini sağlayarak bilgi sızıntılarını engellemeye yönelik kritik bir güvenlik önlemidir. Bu bağlamda, katılımcıların şifrelemeye yönelik güvenlik önlemlerini yeterince dikkate almadıkları anlaşılmaktadır. E-posta güvenliği konusunda organizasyonlar düzeyinde daha fazla eğitim ve farkındalık çalışması yapılması gerektiği görülmektedir.
- ***Çalışanların işletmelerinin siber güvenlik durumu hakkında düzenli bilgi akışının sağlanmadığını ifade etmeleri***, önemli bir güvenlik zafiyetine işaret etmektedir. Siber güvenlik, yalnızca teknik önlemlerle sınırlı kalmamalı, aynı zamanda çalışanların sürekli olarak bilgilendirildiği ve güvenlik tehditlerinin yönetildiği bir süreç olmalıdır. Bu durumda, siber güvenliğin etkili bir şekilde yönetilmesi, kurum içi iletişim süreçlerinin güçlü olmasına ve güvenlik tehditlerinin yanı sıra savunma stratejilerinin düzenli olarak paylaşılmasına dayanır.
- ***Yeni çalışanlara yönelik siber güvenlik eğitimlerinin verilmemesi***, organizasyonun siber güvenlik farkındalık programlarının eksik veya yetersiz olduğuna dair önemli bir göstergedir. Siber güvenlik eğitimi, çalışanların dijital tehditlere karşı hazırlıklı olmalarını sağlayarak, organizasyonun genel güvenliğini artıran kritik bir faktördür. Bu tür eğitimlerin eksikliği, şirketin siber güvenlik stratejisinin zayıf olduğunu ve organizasyonun siber tehditlere karşı daha savunmasız hale gelmesine neden olduğunu gösterir. Bu durum, siber güvenlik önlemleri ve çalışan farkındalığının güçlendirilmesi gerektiğine işaret etmektedir.

Bazı temel siber güvenlik önlemlerinin organizasyon içinde yeterince uygulanmadığı ya da farkındalık eksikliklerinin olduğu sonucuna ulaşılmıştır. Özellikle e-posta şifrelemesi, dosya erişim kontrolleri ve siber güvenlik eğitimi gibi kritik güvenlik önlemlerinin eksikliği, organizasyonların dijital tehditlere karşı daha savunmasız hale gelmesine yol açabilmektedir. Organizasyonun siber güvenlik kültürünün henüz olgunlaşmadığını ve temel güvenlik önlemlerinin tam olarak uygulanmadığını ortaya koymaktadır. Bu da, organizasyonel güvenlik stratejilerinin güçlendirilmesi ve çalışanların güvenlik bilincinin artırılması gerektiğine işaret etmektedir. Bu bağlamda, işletmelerin siber güvenlik politikalarını yeniden gözden geçirmeleri, çalışanlara yönelik düzenli eğitim programları düzenlemeleri ve güvenlik önlemlerini daha etkin bir şekilde güçlendirmeleri önerilmektedir.

Cinsiyet farklılıklarına dayalı farkındalık farklılıkları göz önünde bulundurularak, erkek ve kadın katılımcılara yönelik daha özel eğitim programları geliştirilebilir. Eğitim içerikleri, erkek ve kadınların ilgisini çekecek ve onların güvenlik anlayışına uygun materyallerle zenginleştirilebilir. Eğitimlerin etkinliğini sürekli olarak izlemek ve cinsiyete dayalı farklılıkları anlamak için anketler ve testler gibi araçlarla geri bildirim alınabilir. Böylece programların iyileştirilmesi sağlanabilir. Farklı yaş gruplarına yönelik özel eğitim programları tasarlanabilir. Gençler için daha dinamik ve interaktif, yaşlılar için ise daha temel güvenlik önlemleri ve dijital okuryazarlık üzerine odaklanan programlar oluşturulabilir. Yaşlı bireyler için anlaşılır ve basitleştirilmiş dijital güvenlik rehberleri hazırlamak, onların güvenli internet kullanımı konusunda daha bilinçli olmalarına yardımcı olabilir. Çalışanların deneyim düzeyine bakılmaksızın, tüm sektörlerde sürekli ve düzenli siber güvenlik eğitimlerinin verilmesi zorunlu hale getirilebilir. Çalışanların siber güvenlik konusunda daha fazla bilgi edinmesi için şirket içi farkındalık artırma programları düzenlenebilir. Bu tür programlar, çalışanların hem teknik hem de pratik düzeyde siber güvenlik becerilerini geliştirmelerine yardımcı olabilir. İşletme içinde pozisyonları ne olursa olsun, çalışanlara ileri düzey siber güvenlik eğitimleri ve sertifikasyon fırsatları sunulabilir. Bu sayede, farkındalık düzeyleri artırılabilir ve çalışanlar siber güvenlik tehditlerine karşı daha hazırlıklı hale getirilebilir.

Bütün bu bilgiler doğrultusunda, sonuç olarak araştırmada kurulan;

"H1: Çalışanların siber güvenlik farkındalık düzeyleri cinsiyete göre farklılık göstermektedir.",

"H2: Çalışanların siber güvenlik farkındalık düzeyleri yaşa göre farklılık göstermektedir.",

"H3: Çalışanların siber güvenlik farkındalık düzeyleri eğitim seviyesine göre farklılık göstermektedir.",

"H4: Çalışanların siber güvenlik farkındalık düzeyleri işletmedeki çalışma süresine göre farklılık göstermektedir.",

"H5: Çalışanların siber güvenlik farkındalık düzeyleri işletmedeki pozisyonuna göre farklılık göstermektedir." hipotezlerinden H1, H2, H3, H4 hipotezleri kabul edilmiş ve H5 hipotezi reddedilmiştir.

Nicel araştırma safhasının tamamlanmasından sonra gerçekleştirilen nitel araştırma sürecine yönelik elde edilen sonuçlar aşağıda yer almaktadır.

- ***Farkındalık Seviyesinin Düşüklüğü****:* Katılımcıların bir kısmının herhangi bir plan ya da eğitimin olmadığını belirtmesi, siber güvenlik farkındalığının henüz yeterince yaygınlaşmadığını göstermektedir. Özellikle insani faktörler, farkındalık eksikliğinin en önemli bileşeni olarak öne çıkmaktadır. Çalışanların siber güvenlik konusunda bilinçsiz olması, eğitim eksikliği ve konuya direnç göstermesi, insan kaynaklı zorlukların ağırlığını vurgulamaktadır.
- ***Teknik Altyapının Yetersizlikleri****:* Gelişen tehditler, açıkların takip edilmesi, yedekleme sistemlerinin eksikliği ve felaket senaryolarının planlanmasındaki yetersizlikler gibi teknik zorluklar, siber güvenlik altyapısında ciddi iyileştirme ihtiyaçları olduğunu göstermektedir. Bu durum, işletmelerin hızla değişen tehdit ortamına adapte olmakta zorlandığını ve teknik kapasitenin artırılması gerektiğini ortaya koymaktadır.
- ***İnsani ve Teknik Faktörlerin Birlikte Etkisi****:* Hem insan hem de teknik faktörlerin birbirini destekleyerek siber güvenlik risklerini artırdığı görülmektedir. Örneğin, yetişmiş uzman eksikliği ve personelin güvenlik

politikalarına uyum sağlayamaması, teknik sistemlerin etkinliğini sınırlamaktadır. Şifre güvenliği bilinçsizliği ya da açıkların takip edilmemesi gibi sorunlar, insan ve teknik faktörlerin birbirine bağımlı olduğunu göstermektedir.

- ***Eğitim ve Bilgilendirme İhtiyacı:*** Farkındalık eğitimlerinin artırılması, uygulamalı ve örnekli eğitimlerin verilmesi gibi öneriler, eğitim eksikliğinin birincil çözüm alanı olduğunu ortaya koymaktadır. Katılımcıların çoğu, farkındalık ve bilgi eksikliğinin hem çalışanlar hem de yöneticiler arasında giderilmesi gerektiğini düşünmektedir.
- ***Planlama ve Önleme Çalışmalarında Eksiklik:*** Siber saldırılara karşı acil durum planlarının varlığından bahsedenler olsa da, birçok katılımcının bu alanda eksik ya da hiç planının olmadığı görülmektedir. Bu durum, işletmelerin olası bir saldırıya karşı yeterince hazırlıklı olmadığını ve proaktif yaklaşımlar geliştirmesi gerektiğini göstermektedir.
- ***Güvenlik Politikalarının Geliştirilmesi Gerekiyor***: Veri güvenliği, e-posta güvenliği, şifreleme politikaları gibi kritik konulara dair teknik önlemler alınması gerektiği vurgulamaktadır. Katılımcıların bu yöndeki yorumları, daha güçlü güvenlik duvarları, düzenli testler ve güncellemeler gibi teknik uygulamaların önemini ortaya koymaktadır.

Bu bulgular, işletmelerin siber güvenlik konusunda hala gelişime açık olduğunu, farkındalık ve teknik altyapının iyileştirilmesi gerektiğini göstermektedir. İnsani ve teknik zorlukların birlikte ele alınması, kapsamlı eğitimlerin düzenlenmesi, sistemlerin güncellenmesi ve düzenli testlerle bu eksikliklerin giderilmesi gerekmektedir. Hem insani hem de teknik önlemlerin eş zamanlı olarak hayata geçirilmesi, işletmelerin siber tehditlere karşı daha dirençli olmasını sağlayacaktır.

Nicel ve nitel veriler arasında yapılan karşılaştırmalar, siber güvenlik uygulamaları ve stratejilerindeki eksikliklerin farklı boyutlarını ortaya koymaktadır. Nicel veriler, çalışanların şifre güvenliği, karmaşık şifreler oluşturma ve şifre paylaşmama gibi konularda yetersiz bir farkındalığa sahip olduklarını gösterirken, nitel veriler bu bilinç eksikliğinin daha geniş bir farkındalık sorunu olduğunu vurgulamaktadır. Ayrıca, nicel verilerde çalışanlara siber güvenlik eğitimlerinin verilmediği ve e-posta

gönderimlerinde şifreleme kullanılmadığı gibi somut güvenlik zafiyetleri ortaya konulurken, nitel veriler, bu eksikliklerin teknik altyapı yetersizliklerinden ve güvenlik politikalarının eksikliğinden kaynaklandığını belirtmektedir. İnsani faktörlerin, örneğin güvenlik alışkanlıkları ile teknik altyapı arasındaki etkileşim de her iki veri setinde vurgulanmış olup, bu faktörlerin birlikte nasıl bir güvenlik açığı yarattığına dikkat çekilmektedir. Bununla birlikte, güvenlik politikalarının geliştirilmesi gerektiği ve düzenli bilgi akışının sağlanmaması gibi organizasyonel eksiklikler, her iki veri türü tarafından da dile getirilmiştir. Sonuç olarak, nicel veriler belirli güvenlik ihlallerini ve eksiklikleri somut bir şekilde ölçerken, nitel veriler bu eksikliklerin organizasyonel ve stratejik düzeyde daha geniş sorunlara işaret ettiğini göstermektedir. Bu iki veri türü, siber güvenlik sorunlarının etkili bir şekilde ele alınabilmesi için hem somut uygulamalar hem de geniş stratejiler geliştirilmesi gerektiğini ortaya koymaktadır.

Çalışanların siber güvenlik farkındalığını artırmak için düzenli eğitimler, seminerler ve farkındalık kampanyaları düzenlenmeli, yöneticilerin liderliğinde bir siber güvenlik kültürü oluşturulmalıdır. Teknik altyapının güçlendirilmesi amacıyla güvenlik duvarları, saldırı tespit sistemleri ve şifreleme gibi önlemler güncellenmeli, yazılım güncellemeleri ve güvenlik açıkları düzenli olarak takip edilmelidir. Ayrıca, felaket kurtarma planları hazırlanmalı ve kritik verilerin yedeklenmesi sağlanmalıdır. İnsani faktörlerin etkili yönetimi için yetişmiş siber güvenlik uzmanları istihdam edilmeli ve çalışanlara uygulamalı eğitimlerle güvenlik politikalarına uyum teşvik edilmelidir. Eğitimler, gerçek yaşam senaryolarına dayalı simülasyonlarla pekiştirilerek sürekli izlenmeli ve iyileştirilmelidir. Siber saldırılara karşı acil durum müdahale planları oluşturulmalı, düzenli siber güvenlik testleri yapılmalıdır. Ayrıca, veri güvenliği politikaları gözden geçirilerek şifreleme, dosya erişim kontrolleri ve diğer güvenlik önlemleri güçlendirilmeli ve e-posta güvenliği ile kimlik doğrulama sistemleri etkinleştirilmelidir.

KAYNAKÇA

ACAR, D. D. D., ÖMÜRBEK, Y. D. D. N., & ÖMÜRBEK, A. G. D. V. (2004). Gıda sektöründe kurumsal kaynak planlaması (ERP) üzerine bir araştırma, Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 9(1).

ACILAR, A. (2009). İşletmelerde bilgi güvenliği ve örgüt kültürü. *Organizasyon ve Yönetim Bilimleri Dergisi*, *1*(1), 34-46.

ACILAR, A. (2009). Kobi'lerde bilişim teknolojileri güvenliği sorunu: Tehditler ve önlemler, Afyon Kocatepe Üniversitesi. İ.İ.B.F. Dergisi, XI(I), 1-16.

ADEWOLE, E. G., & UMORU, T. A. (2021). Perceived influence of business environment on small and medium scale enterprises success in Nigeria. *European Journal of Business and Management Research, 6*(6), 195-200.

ADIR, A. E. (2019). *Kurumlar İçin Siber Güvenlik Laboratuvarı Altyapısının Oluşturulması*, Yüksek Lisans Tezi, Karatay Üniversitesi, Konya.

AKARSU, Y., KURT, S. VE ALACAHAN, N. D. (2020). OECD ülkelerinde bilgi ve iletişim teknolojilerinin işgücü verimliliği üzerine etkisi. Journal of Life Economics, 7(4), 309-322.

AKİNDE, O. K., ILORİ, A. O., AFOLAYAN, A. O., & ADEWUYİ, O. B. (2021). Review of computer malware: detection and preventive strategies. *Int. J. Comput. Sci. Inf. Secur.(IJCSIS)*, *19*, 49.

AKSOĞAN, M., BAYER, H., GÜLADA, M. O., & ÇELİK, E. (2019). İletişim Fakültesi Öğrencilerinin Siber Güvenlik Farkındalığı: İnönü Üniversitesi Örneği. *Kesit Akademi Dergisi*, (13), 271-288.

AKSOY, A. D. (2014). Tüketimin dijitalleşmesi. *Hacettepe Üniversitesi Tüketici-Pazar-Araştırma-Danışma Test ve Eğitim Merkezi Tüketici Yazıları IV,* 46-64.

AKSOY, B. (2012). Bilgi Teknolojileri ve Yeni Çalışma İlişkileri. Ege Academic Review, 12(3).

AKSOY, C. (2024). İşletmelerin Dijital Dönüşümü ve Dijital Liderlik Yaklaşımı. *Kalite ve Strateji Yönetimi Dergisi*, *4*(1), 1-29.

AKTAŞ, A.(2024). 2024'te Her Gün Ne Kadar Veri Üretiliyor?, https://www.linkedin.com/pulse/2024te-her-g%C3%BCn-ne-kadar-veri-%C3%BCretiliyor-ali-akta%C5%9F-fumwf/, (07.11.2024).

AKUNDİ, A., EURESTİ, D., LUNA, S., ANKOBİAH, W., LOPES, A., & EDİNBAROUGH, I. (2022). State of Industry 5.0—Analysis and identification of current research trends. *Applied System Innovation*, 5(1), 27.

AL NUAİMİ, E., AL NEYADİ, H., MOHAMED, N., & AL-JAROODİ, J. (2015). Applications of big data to smart cities. *Journal of Internet Services and Applications, 6*(1), 1-15.

ALAM, S. S., KHATİBİ, A., ISMAİL, H., & AHMAD, I. (2005). Perceived benefits of e-commerce adoption in the electronic manufacturing companies in Malaysia. *Journal of Social Sciences*, *1*(3), 188-193.

ALAVİ, M., & LEİDNER, D. E. (2001). Knowledge management and knowledge management systems: Conceptual foundations and research issues. *MIS q.*, *25*(1), 107-136.

ALÇİN, S. (2016). Üretim için yeni bir izlek: Sanayi 4.0. *Journal of Life Economics*, 3(2), 19-30.

AL-FAR, A., QUSEF, A., & ALMAJALİ, S. (2018). Measuring impact score on confidentiality, integrity, and availability using code metrics. In *2018 International Arab Conference on Information Technology (ACIT)*, 1-9.

ALİOĞLU, S. D. (2019). Siber Saldırılar ve Ülkelerin Siber Güvenlik Politikaları. İstanbul Bilgi Üniversitesi, Yüksek Lisans Tezi, İstanbul.

ALMARABEH, H., & SULİEMAN, A. (2019). The impact of cyber threats on social networking sites. *International Journal of Advanced Research in Computer Science*, *10*(2).

ALTUNOK, E., VE VURAL, A. F. (2011). Bilişim Suçları. *Kamu İç Denetçileri Derneği*(8),

ALTUNTAŞ, E. Y. (2018). Dijital dönüşüm uygulamalarının kurumların marka değeri üzerindeki etkisi. *Ege Üniversitesi İletişim Fakültesi Medya ve İletişim Araştırmaları Hakemli E-Dergisi*, (2), 1-18.

AMİN, D., & GOVİLKAR, S. (2015). Comparative study of augmented reality SDKs. *International Journal on Computational Science & Applications*, 5(1), 11-26.

ANDREESSEN, M., (2011). Why software is eating the world.The Wall Street Journal, https://www.wsj.com/articles/SB10001424053111903480904576512250915629460, (13.10.2024).

ANLEY, C. (2002). “Advanced SQL Injection In SQL Server Applications”, Next Generation Security Software Publication, Surrey,

ANNUAL NUMBER OF RANSOMWARE ATTACKS WORLDWİDE FROM 2017 TO FİRST HALF 2023”, 23 Nisan 2024.

https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/, (15/12/2024).

ANTUNES, M., MAXİMİANO, M., GOMES, R., & PİNTO, D. (2021). Information security and cybersecurity management: A case study with SMEs in Portugal. *Journal of Cybersecurity and Privacy*, *1*(2), 219-238.

APULU, I., & LATHAM, A. (2010). Benefits of information and communication technology in small and medium sized enterprises: a case study of a Nigerian SME.

ARIS, A., OKTUG, S. F., & YALÇIN, S. B. Ö. (2015). Nesnelerin Interneti Güvenligi: Servis Engelleme Saldırıları Internet-of-Things Security: Denial of Service Attacks. In *23th Signal Processing and Communications Applications Conference (SIU)*.

ARITÜRK, M. (2015). Bilgi farkındalığı ve bilgi güvenliğinin karşılaştırılması. XVII. Akademik Bilişim Konferansı Bildirileri (ss. 178-185). Eskişehir.

ARPACİ, I., & SEVİNC, K. (2022). Development of the cybersecurity scale (CS-S): Evidence of validity and reliability. *Information Development*, *38*(2), 218-226.

ARROYABE, M. F., ARRANZ, C. F., DE ARROYABE, I. F., & DE ARROYABE, J. C. F. (2024). Exploring the economic role of cybersecurity in SMEs: A case study of the UK. *Technology in Society*, *78*, 102670.

ARSHAD, A., REHMAN, A.U., JAVAİD, S., ALİ, T.M., SHEİKH, J.A., AZEEM, M. (2021). A systematic literature review on phishing and anti-phishing techniques. Pakistan J.Eng. Tech. 4 (1), 163–168.

ARSLAN, K. (2020). Eğitimde yapay zekâ ve uygulamaları. *Batı Anadolu Eğitim Bilimleri Dergisi*, 11(1), 71-88.

ASHTON, K. (2009). That ‘internet of things’ thing. RFID journal, 22(7), 97-114.

ASLAY, F. (2017). Siber saldırı yöntemleri ve Türkiye’nin siber güvenlik mevcut durum analizi. *International Journal of Multidisciplinary Studies and Innovative Technologies*, *1*(1), 24-28.

ATASEVER, S., ÖZÇELİK, İ., & SAĞIROĞLU, Ş. (2019). Siber Terör ve DDoS. *Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, *23*(1), 238-244.

ATICI, E. (2023). *Simülasyon destekli eğitimin okul yöneticilerinin problem çözme ve karar verme becerileri ile simülasyon uygulamasına yönelik tutumları üzerindeki etkisi*, Yüksek Lisans Tezi, Fırat Üniversitesi, Elazığ.

ATILGAN, D. (2009). Bilgi yönetimi kavramı ve gelişimi. *Türk Kütüphaneciliği*, *23*(1), 201-212.

ATTİYA, I., & ZHANG, X. (2017). Cloud computing technology: Promises and concerns. International Journal of Computer Applications, 159(9), 32-37.

AYTEKİN, A. (2015). *Türkiye"nin siber güvenlik stratejisi ve eylem planının değerlendirilmesi*. Yüksek Lisans Tezi, Bilişim Sistemleri Anabilim Dalı, Gazi Üniversitesi, Ankara.

BADA, M., & NURSE, J. R. (2019). Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). *Information & Computer Security*, *27*(3), 393-410.

BAL, H. Ç., & ERKAN, Ç. (2019). Industry 4.0 and competitiveness. *Procedia Computer Science*, 158, 625-631.

BAO, Y. F. (2016). Analysis of the learning evaluation of distance education based on the Internet of Things. *World Transactions on Engineering and Technology Education*, 14(1), 168-172.

BARTOCK, M., CİCHONSKİ, J., SOUPPAYA, M., WİTTE, G., & SCARFONE, K. (2016). Guide for cybersecurity event recovery.

BAŞALAN, B. (2021). *İşe alım sürecinde işgören temininin dijital dönüşümü üzerine bir uygulama* Yüksek lisans tezi, Marmara Üniversitesi, İstanbul.

BAŞKALE, H. (2016). Nitel araştırmalarda geçerlik, güvenirlik ve örneklem büyüklüğünün belirlenmesi. Dokuz Eylül Üniversitesi Hemşirelik Fakültesi Elektronik Dergisi, 9(1), 23–28.

BAY, M. (2016). What is cybersecurity. *French Journal for Media Research*, *6*, 1-28.

BAYKARA, M., DAŞ, R., & KARADOĞAN, İ. (2013). Bilgi güvenliği sistemlerinde kullanılan araçların incelenmesi. In *1st International Symposium on Digital Forensics and Security (ISDFS'13)*, 20, 21.

BAYRAK, M. (2020). Abd ile Birleşik Krallık'ın Ab Ve Nato Çerçevesinde Siber Alanlarının Tarihsel Analizi. *Cyberpolitik Journal*, *5*(9), 22-51.

BAYRAKTAR, E., & KALELİ, F. (2007). Sanal gerçeklik ve uygulama alanları. Akademik Bilişim, 1(6).

BAZRAFSHAN, Z., HASHEMİ, H., FARD, S. M. H., & HAMZEH, A. (2013). A survey on heuristic malware detection techniques. In *The 5th conference on information and knowledge technology*, 113-120.

BHARADWAJ, A., EL SAWY, O. A., PAVLOU, P. A., & VENKATRAMAN, N. V. (2013). Digital business strategy: Toward a next generation of insights. *MIS Quarterly*, 37(2), 471-482.

BIÇAKCI, S. (2019). Siber güvenlik ve savunma. Güvenlik Yazıları Serisi, (42), 1-8.

BIÇAKÇI, S. N. (2019). Nesnelerin interneti. Takvim-i vekayi, 7(1), 24-36.

BİLEK, B. T. (2012). Bilişim Suçları ve Üniversite Lisans Öğrencilerinin Bilişim Suçlarına Yönelik Görüşleri. Yüksek Lisans Tezi, Gazi Üniversitesi, Bilişim Enstitüsü Bilgisayar Eğitimi ABD, Ankara.

BİNGÖL, B. (2018). Yeni bir yaşam biçimi: Artırılmış gerçeklik (AG). Etkileşim, (1), 44-55.

BİRJE, M. N., CHALLAGİDAD, P. S., GOUDAR, R. H., & TAPALE, M. T. (2017). Cloud computing review: Concepts, technology, challenges and security. *International Journal of Cloud Computing*, 6(1), 32-57.

BLANKE, S. J., & MCGRADY, E. (2016). When it comes to securing patient health information from breaches, your best medicine is a dose of prevention: A cybersecurity risk assessment checklist. *Journal of healthcare risk management*, *36*(1), 14-24.

BLOEM, J., VAN DOORN, M., DUİVESTEİN, S., MAAS, R. & VAN OMMEREN, E. (2014). The fourth industrial revolution things to tighten the link between IT and OT. SOGETI, 1-40.

BMBF. 2012. "Zukunftsbild Industrie 4.0."

BORANDAG, E., & YÜCALAR, F. (2020). Arttırılmış Gerçeklik İle Scrum Task Board Uygulaması, Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi, 4(1), 1-12.

BOYUTKAT, 3D Yazıcı (Printer) ile Neler Yapılabilir? https://www.boyutkat.com/3d-yazici/3d-yaziciprinter-ile-neler-yapilabilir/ , (12.11.2024).

BOZGEYİK, A. (2018). *Gaziantep'te Faaliyet Gösteren Orta ve Büyük Ölçekli İşletmelerin Siber Güvenlik Yönetim Yaklaşımlarının Analizi.* Yayınlanmamış Doktora Tezi. Gaziantep: Hasan Kalyoncu Üniversitesi. Sosyal Bilimler Enstitüsü.

BOZKURT, A. (2014). Ağ toplumu ve bilgi. *Türk Kütüphaneciliği*, *28*(4), 510-525.

BOZKURT, A. A. (2024). *Siber Suçların İncelenmesi Ve Siber Güvenlik Kavramları,* Yüksek Lisans Tezi, İstanbul Topkapı Üniversitesi, İstanbul.

BRADLEY, J. M., & ATKİNS, E. M. (2015). Optimization and control of cyber-physical vehicle systems. *Sensors*, 15(12), 23020-23049.

BRENNEN, J. S., & KREİSS, D. (2016). Digitalization. *The international encyclopedia of communication theory and philosophy*, 1-11.

BRYKCZYNSKİ, B., & SMALL, B. (2003). Securing your organization's information assets. *The Journal of Defense Software Engineering*, *16*(5), 12-16.

BUCERZAN, D., & BEJAN, C. A. (2021). Blockchain. Today applicability and implications. *In Soft computing applications: Proceedings of the 8th International Workshop Soft Computing Applications* (SOFA 2018), I 8,152-164.

BUCH, R., GANDA, D., KALOLA, P. VE BORAD, N. (2017). World of cyber security and cybercrime. STM Journals. 4(2),18-23.

BURNS, A.C. ve BUSH, R.F. (2005), "Pazarlama Araştırması", 7. Basımdan Çeviri, Çeviri Editörü: OREL, F.D., Nobel Yayın.

BUYYA, R., YEO, C. S., VENUGOPAL, S., BROBERG, J., & BRANDİC, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems*, 25, 599-616.

BÜTÜN, M., BUDAK, V. Ö., SELÇUK, M., EMRE, İ. E., & ŞİMŞEK, İ. (2019). Eğitimde sanal gerçeklik uygulamalarında erişilebilirlik ve uyumluluk. *Eğitim Teknolojisi Kuram ve Uygulama*, 9(1), 251-275.

CABALLERO, A. (2013). Information Security Essentials for IT Managers: Protecting Mission-Critical Systems. Computer and Information Security Handbook, 379–407.

CANBEK, G., & SAĞIROĞLU, Ş. (2006). Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme. *Politeknik Dergisi*, *9*(3), 165-174.

CARMEN, H. (2018). Understanding blockchain technology and how to get involved. *In Proceedings of the 14th International Scientific Conference eLearning and Software for Education*, 1-9.

CARMİGNİANİ, J., FURHT, B., ANİSETTİ, M., CERAVOLO, P., DAMİANİ, E., & IVKOVİC, M. (2011). Augmented reality technologies, systems and applications. *Multimedia Tools and Applications*, 51, 341-377.

CBDDO. (2024). Siber Güvenlik. https://cbddo.gov.tr/siber-gvenlik/ (Erişim Tarihi: 13.11.2024).

CHACON, S., & STRAUB, B. (2014). *Pro Git* (2nd ed.). Apress.

CHANG, V., BAUDİER, P., ZHANG, H., XU, Q., ZHANG, J., & ARAMİ, M. (2020). How blockchain can impact financial services: The overview, challenges and recommendations from expert interviewees. *Technological Forecasting and Social Change*, 158, 120166.

CHANİAS, S., & HESS, T. (2016). Understanding digital transformation strategy formation: Insights from Europe's automotive industry. *Journal of Strategic Information Systems*, 25(2), 120-140.

CHEN, M., MAO, S., & LİU, Y. (2014). Big data: A survey. *Mobile Networks and Applications*, 19, 171-209.

CHERKASOVA, V. A., & SLEPUSHENKO, G. A. (2021). The impact of digitalization on the financial performance of Russian companies. *Finance: Theory and Practice*, 25(2), 128-142.

CHİEW, K. L., YONG, K. S. C., & TAN, C. L. (2018). A survey of phishing attacks: Their types, vectors and technical approaches. *Expert Systems with Applications*, *106*, 1-20.

CLARK, D. D. (2010). Characterizing cyberspace: Past, present and future (ECIR Working Paper No. 2010-3). MIT Political Science Department. Version: Author's final manuscript.

COMREY, A. L., & LEE, H. B. (1992). A first course in factor analysis. Erlbaum.

CONTİ, M., DRAGONİ, N., & LESYK, V. (2016). A survey of man in the middle attacks. *IEEE communications surveys & tutorials*, *18*(3), 2027-2051.

CRESWELL, J. W. (2003). Research design: Qualitative, quantitative, and mixed methods approaches. Thousand Oaks, CA: Sage Publications.

CRESWELL, J. W. (2009). Research design: Qualitative, quantitative, and mixed methods approaches (3rd ed.). Thousand Oaks, CA: Sage Publications.

CRESWELL, J. W., VE PLANO CLARK, V. L. (2011). Designing and conducting mixed methods research (2nd ed.). Thousand Oaks, CA: Sage Publications.

CRİDLAND, C. (2008). The history of the internet: the interwoven domain of enabling technologies and cultural interaction. *NATO Security Through Science Series E Human and Societal Dynamics*, *34*, 1.

CYBER SECURİTY FOR SMBS: NAVİGATİNG COMPLEXİTY AND BUİLDİNG RESİLİENCE – https://www.sage.com/en-gb/company/digital-newsroom/2023/10/12/cyber-security-for-navigating-complexity-and-building-resilience/

CYBERMAG (2020). Şirketlerin %76'sı Siber Saldırı KURBANI. https://www.cybermagonline.com/sirketlerin-76si-siber-saldiri-kurbani (22.12.2024).

ÇAHMUTOĞLU, E. (2020). Siber uzayda güç ve siber silah teknolojilerinin küresel etkisi. *Analytical Politics*, *1*(1), 63-79.

ÇALHAN, A., & CİCİOĞLU, M. (2022). Remote health monitoring system modeling for cyber-physical systems. In *2022 30th Signal Processing and Communications Applications Conference* (SIU),1-4.

ÇALIK, T., & SEZGİN, F. (2005). Küreselleşme, bilgi toplumu ve eğitim. *Kastamonu Eğitim Dergisi*, *13*(1), 55-66.

ÇELEBİ, F., & BULUT, Y. (2016). Kurumsal Kaynak Planlaması (Erp) Ve Erp Yazılımı Kullanan Bir İşletmenin İncelenmesi. Akademik Bakış Uluslararası Hakemli Sosyal Bilimler Dergisi, (57), 166-177.

ÇELİK, S., & ÇELİKTAŞ, B. (2018). Güncel Siber Güvenlik Tehditleri: Fidye Yazılımlar. *CyberPolitik Journal*, *3*(5), 105-132.

ÇELİK, Ş. (2013). Stuxnet saldırısı ve Abd'nin siber savaş stratejisi: uluslararası hukukta kuvvet kullanmaktan kaçınma ilkesi çerçevesinde bir değerlendirme. *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, *15*(1), 137-175.

ÇELİKBİLEK, İ. (2016). *TCP SYN seli saldırısının etkilerini azaltmak için yeni syn çerezleri gerçeklemesi*, Yüksek Lisans Tezi, İstanbul Şehir Üniversitesi, İstanbul.

ÇOKBİLDİK, A. C. (2017). Siber Uzay ve İnsan Hakları. *Cyberpolitik Journal*, *3*(5), 133-157.

ÇOKOKUMUŞ, B. (2012). Dijital ortamda kültür ve sanat. International Journal of New Trends in Arts, Sports &Science Education, 1(3), 51-66.

DANİEL, B. (2015). Big data and analytics in higher education: Opportunities and challenges. *British Journal of Educational Technology*, 46(5), 904-920.

DAS, K. (2019). The role and impact of ICT in improving the quality of education: An overview. *International Journal of Innovative Studies in Sociology and Humanities*, *4*(6), 97-103.

DAVİDSSON, P., HAJİNASAB, B., HOLMGREN, J., JEVİNGER, Å., & PERSSON, J. A. (2016). The fourth wave of digitalization and public transport: Opportunities and challenges. Sustainability, 8(12), 1248.

DEMCHENKO, Y., GROSSO, P., LAAT, C., & MEMBREY, P. (2013). Addressing big data issues in scientific data infrastructure. In *2013 International Conference on Collaboration Technologies and Systems* (CTS), 48–55.

DEMİRCAN, C. (2019). *Implications Of Cyber Weapons İn Cybersecurity: A Case Study Of Stuxnet And Duqu*, Yüksek Lisans Tezi, Anadolu Üniversitesi, Eskişehir.

DEMİROL, D., DAŞ, R., & BAYKARA, M. (2013). SQL enjeksiyon saldırı uygulaması ve güvenlik önerileri. In *1st International Symposium on Digital Forensics and Security (1. Uluslararası Adli Bilişim ve Güvenlik Sempozyumu)* (pp. 62-66).

DERYA, H. (2018). Endüstri devrimleri ve endüstri 4.0. *GÜ İslahiye İİBF Uluslararası E-Dergi*, 2(2), 1-20.

DHELİM, S., HUANSHENG, N., CUİ, S., JİANHUA, M., HUANG, R., KEVİN, I., & WANG, K. (2020). Cyberentity and its consistency in the cyber-physical-social-thinking hyperspace. *Computers & Electrical Engineering*, *81*, 106506.

DİCLE, S. Z. (2022). Ortadaki Adam Saldırısı (MITM). *Avrupa Bilim ve Teknoloji Dergisi*, (42), 100-107.

DİGİTALOCEAN. https://www.digitalocean.com/ (31.12.2024).

DODZİUK, H. (2016). Applications of 3D printing in healthcare. *Kardiochirurgia i Torakochirurgia Polska/Polish Journal of Thoracic and Cardiovascular Surgery*, 13(3), 283-293.

DOĞAN, A. (2016). Artırılmış gerçeklik teknolojileriyle desteklenmiş hikâye kitabı okuma deneyimi. *Medeniyet Sanat Dergisi,* 2(2), 121-137.

DOĞAN, K., & ARSLANTEKİN, S. (2016). Büyük veri: Önemi, yapısı ve günümüzdeki durum. *Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi*, 56(1), 15-36.

DOĞRU, Ö. (2020). *İnsan Sinir Sisteminin Ortaokul Altıncı Sınıf Öğrencilere Öğretiminde 3d Simülasyon Kullanımı* ,Yüksek Lisans Tezi, Ege Üniversitesi, İzmir.

DURMUŞ, H. (2015). *Otonom Robot Ve Kontrol Birimi Tasarımı,*Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi, İstanbul.

DURMUŞ, R., & KASIMOĞLU, M. (2022). İşletmelerde dijitalleşmeye yönelik olarak kurumsal yönetim çerçevesinin oluşturulması: Küçük ve orta ölçekli işletmeler üzerine bir araştırma. *İstanbul Kent Üniversitesi İnsan ve Toplum Bilimleri Dergisi*, 3(2), 16-36.

DURNA, E. C. (2021). *Sanal gerçeklik ve artırılmış gerçeklik teknolojilerinin turist tatmini üzerine etkileri: Çanakkale tarihi yarımada örneği,* Yüksek Lisans Tezi, Sakarya Uygulamalı Bilimler Üniversitesi, Sakarya.

EKEN, H. (2013). Mobil ve Web Uygulamalarının Yazılım Güvenliği. *XV. Akademik Bilişim Konferansı*, 513-518.

ELMRABİT, NEBRASE & ZHOU, HUİYU & LANDECK, JORGE. (2020). D2.6 Design and Implementation of a Data Security Framework.

ELRADİ, M. D., MOHAMED, M. H., & ALİ, M. E. (2021). Ransomware attack: rescue-checklist cyber security awareness program. *Artificial Intelligence Advances*, *3*(1), 57-62.

ERCAN, İ., VE KAN, İ. (2004). Ölçeklerde güvenirlik ve geçerlik. Uludağ Üniversitesi Tıp Fakültesi Dergisi, 30(3), 211–216.

ERDİL, O., İMAMOĞLU, S. Z., & KESKİN, H. (2003). Küçük ve orta boy işletmelerde (KOBİ'lerde) ürün yeniliği ve Ar-Ge faaliyetleri, *Öneri Dergisi*, 5(19), 21-29.

EREN, K. (2017). *Bulut bilişim teknolojileri ve NoSQL veritabanları kullanarak Türkiye'de terör olaylarının incelenmesi,* Yüksek Lisans Tezi, Sakarya Üniversitesi Sosyal Bilimler Enstitüsü, Sakarya.

EREN, M. (2023). *Bankacılık ödeme Sistemlerinde Siber güvenlik farkındalığı: Türk bankacılık sektöründe farkındalığın Belirleyicileri üzerine Bir Uygulama*, Yüksek Lisans Tezi, Marmara Üniversitesi, İstanbul.

ERENER, Ş., & BOZ, S. (2021). Modern üretim tekniklerinde eklemeli imalat sistemlerinin yeri ve kullanım alanları, *Turkish Journal of Fashion Design and Management,* 3(1), 47-56.

ERENLER, Y. (2019). Kobilerin Yazılım İhtiyacının Araştırılması ve Yazılım Sektörü Girişimcilerinin Desteklenmesi https://www.mevka.org.tr/assets/upload/dosyalar/DsyizvYqs91202161151PM.pdf.

ERGEN, Y. (2018). Büyük veri, sosyal medya ve etik: Facebook örneğinde bir değerlendirme. *Ege Üniversitesi İletişim Fakültesi Yeni Düşünceler Hakemli E-Dergisi,* (10), 53-64.

ESET SMB DİGİTAL SECURİTY SENTİMENT REPORT 2024 - https://www.eset.com/apac/cybersecurity-for-smb-report-2024/ (27.12.2024).

ESMAEİLİAN, B., BEHDAD, S., & WANG, B. (2016). The evolution and future of manufacturing: A review., *Journal of Manufacturing Systems*, 39, 79-100.

FARASH, M. S., TURKANOVİĆ, M., KUMARİ, S., & HÖLBL, M. (2016). An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment, *Ad Hoc Networks*, 36, 152-176.

FELİCİANO-CESTERO, M. M., AMEEN, N., KOTABE, M., PAUL, J., & SİGNORET, M. (2023). Is digital transformation threatened? A systematic literature review of the factors influencing firms' digital transformation and internationalization. *Journal of Business Research*, 157, 113546.

FERNANDEZ DE ARROYABE, J. C., ARROYABE, M. F., FERNANDEZ, I., & ARRANZ, C. F. (2024). Cybersecurity resilience in SMEs. A machine learning approach. *Journal of Computer Information Systems*, *64*(6), 711-727.

FIRAT, S. Ü., & FIRAT, O. Z. (2017). Sanayi 4.0 devrimi üzerine karşılaştırmalı bir inceleme: Kavramlar, küresel gelişmeler ve Türkiye. *Toprak İşveren Dergisi*, 114(2017), 10-23.

FİTZGERALD, M., KRUSCHWİTZ, N., BONNET, D., & WELCH, M. (2014). Embracing digital technology: A new strategic imperative. *MIT Sloan Management Review*, 55(2). Retrieved from https://sloanreview.mit.edu/projects/embracing-digital-technology/

FLEİSCH, E. (2010). What is the Internet of Things? *When things add value* (Auto-ID Labs White Paper WP-BIZAPP-053). Auto-ID Lab St. Gallen, Switzerland.

FORTE, D., & POWER, R. (2007). The ultimate cybersecurity checklist for your workforce. *Computer Fraud & Security*, *2007*(9), 14-19.

FOSTER, I., ZHAO, Y., RAİCU, I., & LU, S. (2008). Cloud computing and grid computing 360-degree compared. In Proceedings of the Grid Computing Environments Workshop (GCE 2008), 1-10, IEEE.

FRENCH, R. M. (2000). The Turing test: The first 50 years. *Trends in Cognitive Sciences,* 4(3), 115-122.

FULANTELLİ, G., & ALLEGRA, M. (2003). Small company attitude towards ICT based solutions: some key-elements to improve it. *Journal of Educational Technology & Society*, *6*(1), 45-49.

GABA, D. M. (2004). The future vision of simulation in health care. BMJ Quality & Safety, 13(suppl 1), i2-i10.

GABAÇLI, N. VE UZUNÖZ, M. (2017). IV. Sanayi Devrimi: Endüstri 4.0 ve Otomotiv Sektörü. Uluslararası Politik, Ekonomik ve Sosyal Araştırmalar Kongresi, Bildiriler Kitabı, Cilt:2 Ekonomik Araştırmalar, 149-174.

GANAL, S. (2016). İstismar Kitleri ve Etki Analizi, Yüksek Lisans Tezi, Süleyman Demirel Üniversitesi, Isparta.

GARBER, L. (1999). Melissa virus creates a new type of threat. *Computer*, *32*(06), 16-19.

GARTNER GLOSSARY (2024). https://www.gartner.com/en/information-technology/glossary adresinden alındı.

GAVAZ, Berkay. "Ddos Nedir?", Acarnet, 27 Ağustos 2021, https://www.acarnet.com/blog/ddos-nedir/, (Erişim Tarihi: 16.12.2024).

GEİSBERGER, E., & BROY, M. (EDS.). (2015). *Living in a networked world: Integrated research agenda Cyber-Physical Systems (agendaCPS)*. Herbert Utz Verlag.

GENÇOĞLU, M. T. (2021). Siber Olaylara Müdahale ve Analiz Süreci. *Fırat Üniversitesi Mühendislik Bilimleri Dergisi*, *33*(2), 471-479.

GHAFORY, I. (2024). https://www.endustri40.com/siber-fiziksel-sistemler (12.11.2024).

GİNSBERG, M.(2012). Essential of Artificial İntelligence. San Franscisco: Morgan Kaufmann Publishers, 3-5.

GOODMAN, S. E. (2008). Critical information infrastructure protection. *NATO Security Through Science Series E Human And Societal Dynamics*, 34, 24.

GOUTAM, R. K. (2015). Importance of cyber security. *International Journal of Computer Applications*, 111(7), 14-17.

GÖÇEN, A. (2022). Eğitim bağlamında metaverse. *Uluslararası Batı Karadeniz Sosyal ve Beşerî Bilimler Dergisi*, 6(1), 98-122.

GÖKMEN, Ö. F., VE AKGÜN, Ö. E. (2015). Bilgisayar ve öğretim teknolojileri eğitimi öğretmen adaylarının bilişim güvenliği eğitimi verebilmeye yönelik yeterlilik algılarının incelenmesi. İlköğretim Online, 14(4), 1208-1221.

GÖKREM, L., & BOZUKLU, M. (2016). Nesnelerin interneti: Yapılan çalışmalar ve ülkemizdeki mevcut durum, *Gaziosmanpaşa Bilimsel Araştırma Dergisi*, (13), 47-68.

GÖMÜKPINAR, B. (2022). Türkiye'de yükseköğretim kurumlarında dijital dönüşüm, Yüksek Lisans Tezi, Selçuk Üniversitesi, Konya.

GRECH, A., & CAMİLLERİ, A. F. (2017). Blockchain in education. Publications Office of the European Union.

GRUİA, L. A., BİBU, N., NASTASE, M., ROJA, A., & CRİSTACHE, N. (2020). Approaches to digitalization within organizations. *Review of International Comparative Management/Revista de Management Comparat International*, 21(3).

GUPTA, B., MİTTAL, P., & MUFTİ, T. (2021). A review on Amazon Web Services (AWS), Microsoft Azure & Google Cloud Platform (GCP) services. In Proceedings of the 2nd International Conference on ICT for Digital, Smart and Sustainable Development, ICIDSSD 2020, 27-28 February 2020, Jamia Hamdard, New Delhi, India.

GÜLDÜREN, C., ÇETİNKAYA, L., VE KESER, H. (2016). Ortaöğretim öğrencilerine yönelik bilgi güvenliği farkındalık ölçeği (BGFÖ) geliştirme çalışması. İlköğretim Online, 15(2).

GÜNDOĞDU, S. (2023). Uluslararası Politikada Bir Etki Aracı Olarak Siber Güvenlik ve Türkiye'nin Siber Güvenlik Politikası Uygulaması: Ulusal Siber Olaylara Müdahale Merkezi (USOM). Fırat Üniversitesi Sosyal Bilimler Dergisi, 33, 3, 1325-1337.

GÜNGÖR, M. (2015). Ulusal bilgi güvenliği: Strateji ve kurumsal yapılanma. T.C Kalkınma Bakanlığı Uzmanlık Tezi, Ankara.

GÜNGÖR, U., & GÜNEY, O. (2017). Uluslararası İlişkilerde Güvenliğin Dönüşümü Çerçevesinde Bilgi Güvenliği ve Siber Savaş. *Karadeniz Araştırmaları*, *14*(55), 131-146.

GÜNTAY, V. (2017). ULUSLARARASI SİSTEM VE GÜVENLİK AÇISINDAN DEĞİŞEN SAVAŞ KURGUSU; SİBER SAVAŞ ÖRNEĞİ. *Güvenlik Bilimleri Dergisi*, *6*(2), 81-108.

GÜNTAY, V. (2018). Siber güvenliğin uluslararası politikada etki aracına dönüşmesi ve uluslararası aktörler. *Güvenlik Stratejileri Dergisi*, *14*(27), 79-111.

GÜR, Y. E., AYDEN, C., & YÜCEL, A. (2019). Yapay zekâ alanindaki gelişmelerin insan kaynaklari yönetimine etkisi. *Fırat Üniversitesi Uluslararası İktisadi ve İdari Bilimler Dergisi*, *3*(2), 137-158.

GÜRKAYNAK, M., & İREN, A. A. (2011). Reel dünyada sanal açmaz: Siber alanda uluslararasi ilişkiler. *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, *16*(2), 263-279.

GÜRKAYNAK, M., & İREN, A. A. (2011). Reel dünyada sanal açmaz: Siber alanda uluslararasi ilişkiler. *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, *16*(2), 263-279.

HABİBOV, A. (2024). *Dijitalleşme Sürecinde İşletmelerde Değişen Yeni Normların Rekabet Üstünlüğüne Etkisi*, Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi, İzmir.

HAİG, Z. (2021). Relationships between Cyberspace Operations and Information Operations. Advances in Military Technology, 16(1), 91–105.

HAKİ, E. H. (2007). *İnternet Protokolü Üzerinden Ses İletiminde Hizmet Kalitesinin Analizi*, Yüksek Lisans Tezi, Yıldız Teknik Üniversitesi, İstanbul.

HANSEN, L., & NİSSENBAUM, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International studies quarterly*, *53*(4), 1155-1175.

HASAN, S., ALİ, M., KURNİA, S., & THURASAMY, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, *58*, 102726.

HAUGELAND, J. (1989). Artificial intelligence: The very idea. MIT press.

HEİETS, I., LA, J., ZHOU, W., XU, S., WANG, X., & XU, Y. (2022). Digital Transformation of Airline Industry. Research in Transportation Economics, 92, 101186.

HENKOĞLU, T. (2015). *Hassas Bilgi Varlıklarının ve Kişisel Verilerin Hukuksal Düzenlemeler İle Korunması Ve Bu Kapsamda Üniversiteler İçin Bilgi Güvenliği Politikasının Geliştirilmesi,* Doktora Tezi, Hacettepe Üniversitesi, Ankara.

HENRİETTE, E., FEKİ, M., & BOUGHZALA, I. (2016). Digital Transformation Challenges. MCIS, 33, 1–8. http://aisel.aisnet.org/mcis2016http://aisel.aisnet.org/mcis2016/33.

HİNDUJA, S., & PATCHİN, J. W. (2012). Bullying beyond the schoolyard: preventing and responding to cyberbullying. *Security Journal*, *25*, 88-89.

HİNİNGS, B., GEGENHUBER, T., & GREENWOOD, R. (2018). Digital innovation and transformation: An institutional perspective. Information and Organization, 28(1), 52-61.

HUANG, D. L., RAU, P. L. P., & SALVENDY, G. (2010). Perception of information security. *Behaviour & Information Technology*, *29*(3), 221-232.

HUBERMAN, B. A. (2016). Ensuring trust and security in the industrial IoT: The internet of things (Ubiquity symposium). *Ubiquity,* 1-7.

HUSSİEN, A. A. (2020). How many old and new big data v's characteristics, processing technology, and applications (BD1). *International Journal of Application or Innovation in Engineering & Management*, 9(9), 15-27

HUYNH-THE, T., GADEKALLU, T. R., WANG, W., YENDURİ, G., RANAWEERA, P., PHAM, Q. V., & LİYANAGE, M. (2023). Blockchain for the metaverse: *A review. Future Generation Computer Systems*, 143, 401-419.

IDİKA, N., & MATHUR, A. P. (2007). A survey of malware detection techniques. *Purdue University*, *48*(2), 32-46.

ILCUS, A. M. (2018). Impact of digitalization in business world. *Revista de Management Comparat Internaţional*, 19(4), 350-358.

ITU-T. (2014). A cybersecurity indicator of risk to enhance confidence and security in the use of telecommunication/information and communication technologies. https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1208-201401-I!!PDFE&type=items

İÇTEN, T., & BAL, G. (2017). Artırılmış gerçeklik üzerine son gelişmelerin ve uygulamaların incelenmesi. Gazi University Journal of Science Part C: Design and Technology, 5(2), 111-136.

İRAZ, R. (2004). Organizasyonlarda Karar Verme ve İletişim Sürecinin Etkinliği bakımından Bilgi Teknolojilerinin Rolü. *Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, (11), 407-422.

İZCİ, M. (2023). *Türkçe Öğretmenlerinin Bilgi Ve İletişim Teknolojileri Entegrasyonu Yeterliklerinin Çeşitli Değişkenler Açısından İncelenmesi (Trabzon İli Örneği)*, Yüksek Lisans Tezi, Giresun Üniversitesi, Giresun.

JANNAİ, D., MERON, A., LENZ, B., LEVİNE, Y., & SHOHAM, Y. (2023). Human or Not? A gamified approach to the Turing test. arXiv preprint arXiv:2305, 20010.

JONES, P., BEYNON-DAVİES, P., & MUİR, E. (2003). Ebusiness barriers to growth within the SME sector. *Journal of Systems and Information Technology*, *7*(1/2), 1-25.

KAPAN, A.A. (2024). *Bilgi ve İletişim Teknolojileri ve Ekonomik Büyüme İlişkisi: Türkiye Örneği*, Yüksek Lisans Tezi, Fırat Üniversitesi, Elâzığ.

KAPLAN, Ş., & COŞGUN, N. 3 Boyutlu (3D) Yazıcı Teknolojisinin Yapı Sektöründe Kullanımının Örnek Yapılar Üzerinden İncelenmesi.

KARA, M. (2007). *Siber Saldırılar- Siber Savaşlar Ve Etkiler*, Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi, İstanbul.

KARAASLANOĞLU, F. (2023). *Dijital Dönüşümün Finansal Performansa Etkisi: Bist İmalat Sanayi İşletmeleri Üzerine Bir Araştırma,* Doktora Tezi, Anadolu Üniversitesi Sosyal Bilimler Enstitüsü, Eskişehir.

KARABULUT, B. (2015). Bilgi toplumu çağında dijital yerliler, göçmenler ve melezler. *Pamukkale Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, (21), 11-23.

KARAKAYA, M. (2022). Kurumsal güvenlik için siber tehditlerin incelenmesi ve saldırı senaryoları, Yüksek lisans tezi, Sakarya Üniversitesi, Sakarya.

KARAYILMAZLAR, S., AŞKIN, A., & ÇABUK, Y. (2007). Küçük ve orta ölçekli işletmelerin tarihsel gelişimi ve tanımlama kriterleri. *ÇOMU Girişimcilik ve Kalkınma Dergisi*, 2(1).

KARBUZ. N. (2019). Bilgi Toplumu Sürecinde Kamu Eğitim Yöneticilerine Yönelik Hizmet İçi Eğitim Politikalarındaki Değişim, Yüksek Lisans Tezi, Sakarya Üniversitesi, Sakarya.

KARİMİ, J., & WALTER, Z. (2015). The role of dynamic capabilities in responding to digital disruption: A factor-based study of the newspaper industry. *Journal of Management Information Systems*, *32*(1), 39-81.

KASA, H., & ARSLAN, G. (2020). Endüstri 4.0 kapsamında teorik bir analiz: Türkiye örneği. *Elektronik Sosyal Bilimler Dergisi*, 19(76), 1810-1826.

KASS, R. A., & TİNSLEY, H. E. A. (1979). Factoranalysis. Journal of LeisureResearch, 11(2), 120-138.

KAUR, N., & SOOD, S. K. (2017). Dynamic resource allocation for big data streams based on data characteristics (5 V's). *International Journal of Network Management*, 27(4), e1978.

KELLER, S., POWELL, A., HORSTMANN, B., PREDMORE, C., & CRAWFORD, M. (2005). Information security threats and practices in small businesses. *Information systems management*, *22*(2).

KESAYAK, B. (2024). https://www.endustri40.com/endustri-tarihine-kisa-bir-yolculuk/ (15.11.2024).

KESKİN, A., & CANBAZ, S. (2014). KOBİ'lerde çalışanların mobbinge maruz kalma durumları: Kırklareli ilinde bir araştırma. *İstanbul Gelişim Üniversitesi Sosyal Bilimler Dergisi*, *1*(2), 161-196.

KESKİN, D. A., & GÖZENMAN, S. (2019). Hile Riski Açısından Sosyal Mühendislik. *TIDE AcademIA Research*, *1*(2), 281-306.

KESTEL, M. VE AKBIYIK, C. (2016). Siber Zorbalığın Öğrencilerin Akademik Sosyal ve Duygusal Durumları Üzerindeki Etkisinin İncelenmesi. Mersin Üniversitesi Eğitim Fakültesi Dergisi, 844-859.

KHAN, M. I., TANWAR, S., & RANA, A. (2020). The need for information security management for SMEs. In *2020 9th International Conference System Modeling and Advancement in Research Trends (SMART)*, 328-332.

KHATİBİ, A., THYAGARAJAN, V., & SEETHARAMAN, A. (2003). E-commerce in Malaysia: perceived benefits and barriers. *Vikalpa*, *28*(3), 77-82.

KHODADADİ, F., DESTJERDİ, A. V., & BUYYA, R. (2016). Internet of things: An overview. In A. V. Destjerdi & R. Buyya (Eds.), *Internet of things* (pp. 3-27). Elsevier.

KILCI, D. (2020). Dijital dönüşüm ve Endüstri 4.0. LinkedIn. https://www.linkedin.com/pulse/dijital-d%C3%B6n%C3%BC%C5%9F%C3%BCm-ve-end%C3%BCstri-40-deniz-k%C4%B1lc%C4%B1/(31.12.2024).

KILINÇ, F., & EYÜPOĞLU, C. (2023). AĞ ORTAMINDAKİ SALDIRI TÜRLERİ: SALDIRI SENARYO ÖRNEKLERİ. *İstanbul Ticaret Üniversitesi Teknoloji ve Uygulamalı Bilimler Dergisi*, *6*(1), 99-109.

KISSEL, R. (2013) "Glossary of Key Information Security Terms", NISTIR 7298, 58.

KİZİLTAN, M. B. (2007). *5237 sayılı Türk ceza kanununda bilişim sistemine girme, sistemi engelleme ve bozma suçları*, Yüksek Lisans Tezi, İstanbul Üniversitesi, İstanbul.

KLİNE, P. (1994). An easy guide to factor analysis. New York: Routledge.

KŐ, A., FEHÉR, P., & SZABÓ, Z. (2019). Digital transformation – A Hungarian overview. *Economic and Business Review*, 21(3), 3.

KOCA, D. (2020). Sanayi devrimlerinin tarihsel arka planı ve işgücü becerileri üzerindeki yansımaları. *OPUS International Journal of Society Researches*, 16(31), 4531-4558.

KOÇ, T. C. & TEKER, S. (2019). Industrial revolutions and its effects on quality of life. PressAcademia Procedia, 9(1), 304-311.

KONYA YATIRIM. (n.d.). Ekonomik durum https://www.konyadayatirim.gov.tr/konya/ekonomik-durum (05.11.2024).

KORKMAZ, YAKUP (2010). "Bulut Bilişim: Türkiye İçin Fırsatlar", TÜBİTAK http://ebookbrowsee.net/korkmaz-bulut-bilisim-ppt-d30735781

KÖRPE, E. (2021). Dijital dönüşüm ile yeni finans çağı ve gelecek yaklaşımları. *Uluslararası Bankacılık Ekonomi ve Yönetim Araştırmaları Dergisi*, 4(2), 108-131.

KRAUS, S., DURST, S., FERREİRA, J. J., VEİGA, P., KAİLER, N., & WEİNMANN, A. (2022). Digital transformation in business and management research: An overview of the current status quo. *International Journal of Information Management*, 63, 102466.

KTO. (2010). KOBİ'lerin yapısı raporu. Konya Ticaret Odası. https://www.kto.org.tr/d/file/kobilerin_yapisi_rapor.pdf (05.11.2024).

KTO. (2023). KOBİ'lerin kredi okuryazarlığı. Konya Ticaret Odası. https://www.kto.org.tr/d/file/2023-26-kobilerin-kredi-okuryazarligi.pdf(05.11.2024).

KTO. (n.d.). Konya'nın ihracat rakamları. Konya Ticaret Odası. https://www.kto.org.tr/bilgi-bankasi/dts/konyanin-ihracat-rakamlari (05.11.2024).

KUMAR, U., KASWAN, M. S., KUMAR, R., CHAUDHARY, R., GARZA-REYES, J. A., RATHİ, R., & JOSHİ, R. (2023). A systematic review of Industry 5.0 from main aspects to the execution status. *The TQM Journal*, ahead-of-print.

KURNAZ, A. (2021). A Review on Usage Areas of Blockchain Technology in Architecture. *International Journal of Scientific and Technological Research, no*.

KURNAZ, S., & ÖNEN, M. (2019). Avrupa Birliği'ne Uyum Sürecinde Türkiye'nin Siber Güvenlik Stratejileri. *International Journal of Politics and Security*, 1(2), ss. 82-103.

KURUÜZÜMCÜ, R. (2007). Bir dijital ortam ve sanat formu olarak sanal gerçeklik, *Sanat Dergisi,* (12), 93-96.

KUTUP, N. (2011). Nesnelerin interneti; 4H her yerden, herkesle, her zaman, her nesne ile bağlantı. *XVI. Türkiye'de İnternet Konferansı*, *11*, 151-156.

KÜTÜPHAN-E TÜRKİYE PROJE OFİSİ. (2014). Çeviri Yazılar / Reader Letters. *Türk Kütüphaneciliği, 28*(3), 399-401.

L'HEUREUX, A., GROLİNGER, K., ELYAMANY, H. F., & CAPRETZ, M. A. (2017). Machine learning with big data: Challenges and approaches. *Ieee Access*, *5*, 7776-7797.

LAVROV, V. V., SPİRİN, N. A., GURİN, I. A., RYBOLOVLEV, V. Y., & KRASNOBAEV, A. V. (2017). Software for decision-making support in blast-furnace operation. Steel in Translation, 47, 538-543.

LEE, J., ARDAKANİ, H. D., YANG, S., & BAGHERİ, B. (2015). Industrial big data analytics and cyber-physical systems for future maintenance & service innovation. *Procedia cirp*, *38*, 3-7.

LEE, K. (2012). Augmented reality in education and training. *TechTrends*, *56*, 13-21.

LEGNER, C., EYMANN, T., HESS, T., MATT, C., BÖHMANN, T., DREWS, P., ... & AHLEMANN, F. (2017). Dijitalleşme: iş ve bilgi sistemleri mühendisliği topluluğu için fırsat ve zorluk. *İş ve bilgi sistemleri mühendisliği* , *9* , 301-308.

LEWİS, J. A. (2002). *Assessing the risks of cyber terrorism, cyber war and other cyber threats* (p. 12). Washington, DC: Center for Strategic & International Studies.

Lİ, F., NUCCİARELLİ, A., RODEN, S. AND GRAHAM, G. (2016). How smart cities transform operations models: A new research agenda for operations management in the digital economy. Production Planning & Control, 27(6), 514-528.

LİEW, A. (2013). DIKIW: Data, information, knowledge, intelligence, wisdom and their interrelationships. *Business Management Dynamics*, *2*(10).

LİN, B., ZAGALSKY, A., STOREY, MA, & SEREBRENİK, A. (2016). Geliştiriciler neden tembellik ediyor: Yazılım ekiplerinin tembelliği nasıl kullandığını anlamak. Bilgisayar destekli işbirlikli çalışma ve sosyal bilişim yoldaşı üzerine 19. acm konferansının bildirilerinde, 333-336.

LİU, D. Y., CHEN, S. W., & CHOU, T. C. (2011). Resource fit in digital transformation: Lessons learned from the CBC Bank global e-banking project. *Management Decision*, *49*(10), 1728-1742.

LLOYD, G. (2020). The business benefits of cyber security for SMEs. Computer fraud & security, 2020(2), 14-17.

LUPTON, D. (2020). ‘Better understanding about what's going on’: young Australians’ use of digital technologies for health and fitness. *Sport, Education and Society*, *25*(1), 1-13.

MAGAZZİNO, C., PORRİNİ, D., FUSCO, G., & SCHNEİDER, N. (2021). Investigating the link among ICT, electricity consumption, air pollution, and economic growth in EU countries. *Energy Sources, Part B: Economics, Planning, and Policy*, *16*(11-12), 976-998.

MALLİK, A. (2019). Man-in-the-middle-attack: Understanding in simple words. *Cyberspace: Jurnal Pendidikan Teknologi Informasi*, *2*(2), 109-134.

MANYİKA, J., CHUİ, M., BUGHİN, J., DOBBS, R., ROXBURGH, C., VE HUNG BYERS, A. (2011). Big data the next frontier for innovation, competition and productivity. McKinsey Global Institute.

MARANGOZ, M., & ÖZBERK, T. M. İ. (2019). Kobi’lerin Dış Pazarlara Açılmasında İnternetin Önemi Ve Karşılaştıkları Sorunların Değerlendirilmesi. *İktisadi İdari ve Siyasal Araştırmalar Dergisi*, *4*(8), 1-20.

MARMARA ÜNİVERSİTESİ (2015), Aldatıcı E-Posta Mesajları Hk. https://bidb.marmara.edu.tr/notice/aldatici-e-posta-mesajlari-hk/ (16.12.2024).

MARTİN, A. (2008). Digital literacy and the “digital society”. *Digital literacies: Concepts, policies and practices*, *30*(151), 1029-1055.

Masum, E. (2017). *Dağıtık servis dışı bırakma saldırılarının incelenmesi ve korunma yöntemleri*, Yüksek Lisans Tezi, Ankara Universitesi, Ankara.

MATT, C., HESS, T., & BENLİAN, A. (2015). Digital Transformation Strategies. Business & Information Systems Engineering, 57(5), 339-343.

MCCARTHY, J. (1988). Mathematical logic in artificial intelligence. *Daedalus*, 297-311.

MECEK, G. (2020). Küçük ve orta büyüklükteki işletmelerin (KOBİ) uluslararası tanımlama ölçütleri ve kavramlaştırılması. Ekonomi İşletme Siyaset ve Uluslararası İlişkiler Dergisi, 6(1), 29-55.

MELL, P. (2011). The NIST Definition of Cloud Computing. *Recommendations of the National Institute of Standards and Technology*.

MERCAN ALKAN, A. (2023). Sigorta Sektöründe Siber Riskler. Tokat Gaziosmanpaşa Üniversitesi Turhal Uygulamalı Bilimler Fakültesi Dergisi, 1(1), 41-50.

MERCİER-LAURENT, E. (2020). Intelligence articielle 4.0 pour l'Industrie 4.0. *1024: Bulletin de la Société Informatique de France*, *15*, 127-137.

MIDIK, Ö., & KARTAL, M. (2010). SİMÜLASYONA DAYALI TIP EĞİTİMİ. *Marmara Medical Journal*, *23*(3).

MİAH, S. J., CAMİLLERİ, E., & VU, H. Q. (2022). Big Data in healthcare research: a survey study. *Journal of Computer Information Systems*, *62*(3), 480-492.

MİJWEL, M. M. (2015). History of Artificial Intelligence Yapay Zekânın T arihi. *Computer Science,(2015)*, 3-4.

MİLES, M. B., VE HUBERMAN, A. M. (1994). Qualitative data analysis: An expanded sourcebook. Thousand Oaks, CA: Sage Publications.

MİLGRAM, P., & KİSHİNO, F. (1994). A taxonomy of mixed reality visual displays. *IEICE TRANSACTIONS on Information and Systems*, *77*(12), 1321-1329.

MİLGRAM, P., & KİSHİNO, F. (1994). A taxonomy of mixed reality visual displays. *IEICE TRANSACTIONS on Information and Systems*, *77*(12), 1321-1329.

MİLGRAM, P., DRASCİC, D., GRODSKİ, J. J., RESTOGİ, A., ZHAİ, S., & ZHOU, C. (1995, February). Merging real and virtual worlds. In *Proceedings of IMAGINA,* 95, 218-230.

MİLOŠEVİĆ, N. (2013). History of malware. *arXiv preprint arXiv:1302.5392*.

MONOSTORİ, L., KÁDÁR, B., BAUERNHANSL, T., KONDOH, S., KUMARA, S., REİNHART, G., & UEDA, K. (2016). Üretimde siber-fiziksel sistemler. *Cirp Yıllıkları* , *65* (2), 621-641.

MOON, Y. B. (2007). Enterprise Resource Planning (ERP): a review of the literature. International journal of management and enterprise development, 4(3), 235-264.

MOURTZİS, D., ANGELOPOULOS, J., & PANOPOULOS, N. (2022). A Literature Review of the Challenges and Opportunities of the Transition from Industry 4.0 to Society 5.0. *Energies*, *15*(17), 6276.

MÜSLÜMOV, A. (2002). Küreselleşme sürecinde Türkiye ekonomisinde KOBİ'lerin yeri: finansman, ekonomik sorunları ve çözüm önerileri. 21. Yüzyılda KOBİler: Sorunlar, Fırsatlar ve Çözüm Önerileri Sempozyumu 3 - 4 Ocak 2002. Gazimagusa: Doğu Akdeniz Üniversitesi.

NAVANİ, D., JAİN, S., & NEHRA, M. S. (2017, December). The internet of things (IoT): A study of architectural elements. In *2017 13th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS)* (pp. 473-478). IEEE.

NEZGİTLİ, S., VE GÖKÇEARSLAN, Ş. (2022). Kamu kurumu ve özel sektöre yönelik bilgi güvenliği farkındalığı üzerine bir inceleme. Instructional Technology and Lifelong Learning, 3(1), 19-44.

NGO, F. T., AGARWAL, A., GOVİNDU, R., & MACDONALD, C. (2020). Malicious software threats. *The Palgrave handbook of international cybercrime and cyberdeviance*, 793-813.

NGOMA, M. L. (2019). *Cybersecurity Awareness in South African Public Sector Organisations* (Master's thesis, University of Johannesburg (South Africa)).

NİCKOLOV, E. (2008). Modern trends in the cyber attacks against the critical information infrastructure. Regional Cybersecurity Forum, 7-9.

ODABAŞ, H. (2008). "Bilgi yönetimi ve yüksek öğrenim kurumlarında kurumsal açık erişim", XIII. Türkiye'de İnternet Konferansı, ODTÜ, Ankara: 1-2.

OECD (2024). The Oecd's Contrıbutıon To Polıcıes To Optımıse The Dıgıtal Transformatıon. https://one.oecd.org/document/C/MIN(2024)10/en/pdf (05.10.2024).

OĞUZ, B. (2009). *Metin Madenciliği Teknikleri Kullanılarak Kulak Burun Boğaz Hasta Bilgi Formlarının Analizi,* Yüksek Lisans Tezi, Akdeniz Üniversitesi, Antalya.

OKTAY, S., VE ÇAKIR, R. (2012). İlköğretim öğretmelerinin teknoloji kullanımları ve teknolojiye yönelik tutumları arasındaki ilişkinin incelenmesi. X. Ulusal Fen Bilimleri ve Matematik Eğitimi Kongresi'nde sunulan bildiri.

OLCAY, T. (2022). *Bilgi Toplumunun İstihdam Üzerine Etkilerinin Türkiye Perspektifinden Değerlendirilmesi*, Doktora Tezi, Dokuz Eylül Üniversitesi, İzmir.

OMRANİ, N., REJEB, N., MAALAOUİ, A., DABİĆ, M., & KRAUS, S. (2022). Drivers of digital transformation in SMEs. *IEEE transactions on engineering management*.

OTTİS, R., AND LORENTS, P. (2010). "Cyberspace: Definition and Implication," in Proceeding of the 5th International Conference Information Warfare and Security, Ohio, USA: The Air Force Institute of Technology, 267–269.

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

ÖNAÇAN, M. B. K., & ATAN, H. (2016). Siber güvenlikte lisansüstü eğitim: Deniz harp okulu örneği. *Trakya Üniversitesi Mühendislik Bilimleri Dergisi*, *17*(1), 13-21.

ÖZCAN, A. (2021). Büyük veri: Fırsatlar ve tehditler. *Trt Akademi*, *6*(11), 10-31.

ÖZDEN, E. (2021). *Kurumsal bilgi yönetimi teknolojik eğilimler*, Eğitim Yayınevi.

ÖZGÜNER KILIÇ, H., ÇAKMAK, A. Ç., & FİDAN, Y. (2015). KOBİ'lerde yönetim ve pazarlama sorunları: Karabük örneği. *Girişimcilik ve Kalkınma Dergisi*.

ÖZHAVZALI, M., & ERDURAN, T. (2019). Bilgi İletişim Teknolojilerinin Gelişime Göre Büro Yönetimi ve Yönetici Asistanlığı Programının Durumunun Araştırılması. *Ekonomi İşletme Siyaset ve Uluslararası İlişkiler Dergisi*, *5*(2), 144-155.

ÖZSOYLU, A. F. (2017). Endüstri 4.0, Çukurova Üniversitesi İİBF Dergisi, 21(1), 41-64.

ÖZTUNÇ, Y. M. (2022). *ABD ve Türkiye'de Siber Güvenlik Politikalarının Karşılaştırmalı Analizi*, Yüksek Lisans Tezi, Ufuk Üniversitesi, Ankara.

ÖZTÜRK, Ö. (2009). E-Postalarda Spam Sorunu ve Çözüm Önerileri. Uzmanlık Tezi. Ankara: Bilgi Teknolojileri ve İletişim Kurumu.

PAJUNEN, N. (2017). 'Overview of Maritime Cybersecurity', South-Eastern Finland University of Applied Sciences.

PAMUK, N. S., & SOYSAL, M. (2018). Yeni sanayi devrimi endüstri 4.0 üzerine bir inceleme. *Verimlilik Dergisi*, (1), 41-66.

PARKER, S. (2000). Knowledge is like light–information is like water. *Information Development*, *16*(4), 233-238.

PARVİAİNEN, P., TİHİNEN, M., KÄÄRİÄİNEN, J., & TEPPOLA, S. (2017). Tackling the digitalization challenge: how to benefit from digitalization in practice. *International journal of information systems and project management*, *5*(1), 63-77.

PATEL, K. K. VE PATEL, S. M. (2016). Internet of things-IOT: Definition, characteristics, architecture, enabling technologies, application & future challenges. International Journal of Engineering Science and Computing, 6(5), 6122- 6131.

PATRİCK, S. (2002). Numerical simulation of electric power steering (EPS) system. *KOYO Engineering Journal English Edition*, *16*, 52-56.

RAHİM, N. H. A., HAMİD, S., MAT KİAH, M. L., SHAMSHİRBAND, S., & FURNELL, S. (2015). A systematic review of approaches to assessing cybersecurity awareness. *Kybernetes*, *44*(4), 606-622.

RAJA, R., MUKHERJEE, I., & SARKAR, B. K. (2020). A systematic review of healthcare big data. *Scientific programming*, *2020* (1), 5471849.

RASHİD, S., & PAUL, S. P. (2013). Proposed methods of IP spoofing detection & prevention. *International Journal of Science and Research*, *2*(8), 438-444.

REDEKOP, B. (2016). *Generational differences in the factors affecting organizational cyber security awareness: A quantitative study* (Doctoral dissertation, Capella University). ProQuest Dissertations Publishing.

REHMAN, M.H., LİEW, C.S., ABBAS, A., JAYARAMAN, P.R., WAH, T.Y. AND KHAN, S.U. (2016), "Big data reduction methods: a survey", Data Science and Engineering, 1(4), 265-284.

RENAUD, K., & WEİR, G. R. (2016). Cybersecurity and the unbearability of uncertainty. In *2016 Cybersecurity and Cyberforensics Conference (CCC)*, 137-143.

ROSE, K., ELDRİDGE, S. VE CHAPİN, L. (2015). Nesnelerin interneti: Genel bir bakış. *İnternet topluluğu (ISOC)*, *80*(15), 1-53.

RUPP, M., SCHNECKENBURGER, M., MERKEL, M. BÖRRET, R. & HARRİSON, D.K. (2021). Industry 4.0: A Technological-Oriented Definition Based on Bibliometric Analysis and Literature Review. Journal of Open Innovation Technology, Market and Complexity, 7(68), 1-20. https://doi.org/10.3390/joitmc7010068

RUSSELL, S. J., & NORVİG, P. (2016). *Artificial intelligence: a modern approach*. Pearson.

RÜßMANN, M., LORENZ, M., GERBERT, P., WALDNER, M., JUSTUS, J., ENGEL, P., & HARNİSCH, M. (2015). Industry 4.0: The future of productivity and growth in manufacturing industries. *Boston consulting group*, *9*(1), 54-89.

SAAKSHİ NARULA, ARUSHİ JAİN, AND PRACHİ (2015) Cloud computing security: Amazon web service. In Proceedings of the 2015 International Conference on Advanced Computing Communication Technologies, 501–505.

SABBAGH, K., FRİEDRİCH, R. O. M. A. N., EL-DARWİCHE, B. A. H. J. A. T., SİNGH, M. I. L. I. N. D., & KOSTER, A. L. E. X. (2013). Digitization for economic growth and job creation: Regional and industry perspectives. *The global information technology report*, *2013*, 35-42.

SAEED, S. (2023). Digital Workplaces and Information Security Behavior of Business Employees: An Empirical Study of Saudi Arabia. *Sustainability*, *15*(7), 6019.

SAĞIROĞLU, Ş., & ALKAN, M. (Eds.). (2021). *Siber güvenlik ve savunma: Farkındalık ve caydırıcılık* (1. baskı). Grafiker Yayınları.

SALI, J. B. (2018). Verilerin Toplanması. Ali Şimşek (Ed.). Sosyal bilimlerde araştırma yöntemleri içinde (134- 161). Eskişehir: Anadolu Üniversitesi.

SANDİLAÇ, N. (2022). "Siber Suç, Siber Savaş ve Siber Terör Üçgeninde Siber Dünya." Bilişim Hukuku Dergisi 4, (1) 141-190.

SARAY, G. (2024). Üretimde Dijital Dönüşüm Etkinliğinin Değerlendirilmesi İçin Bir Performans Ölçüm Sistemi Geliştirilmesi, Yüksek Lisans Tezi, Necmettin Erbakan Üniversitesi, Konya.

SCHMALSTİEG, D., LANGLOTZ, T., & BİLLİNGHURST, M. (2011). Augmented Reality 2.0. In *Virtual Realities: Dagstuhl Seminar 2008*, 13-37, Springer Vienna.

SCHUCHMANN, D., & SEUFERT, S. (2015). Corporate learning in times of digital transformation: A conceptual framework and service portfolio for the learning function in banking organisations. *International Journal of Advanced Corporate Learning*, *8*(1).

SCHWAB, K. (2016). *Dördüncü sanayi devrimi*, Optimist Yayın Grubu.

SERAC, C. A. (2023). Dıgıtal Transformatıon Vulnerabılıtıes: Assessıng The Rısks And Strengthenıng Cyber Securıty. *The Annals Of The Unıversıty Of Oradea*, *32*(1st), 771.

SERİNİKLİ, N. (2018). Endüstri 4.0'in özel, kamu ve kooperatif sektörlerine etkisi. *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, *23*(Endüstri 4.0 ve Örgütsel Değişim Özel Sayısı), 1607-1621.

SEVİS, K. N., & SEKER, E. (2016). Cyber warfare: terms, issues, laws and controversies. In *2016 International Conference On Cyber Security And Protection Of Digital Services (Cyber Security),* 1-9.

SEVLİ, O. (2011). Bulut Bilişim ve Eğitim Alanında Örnek Bir Uygulama, Yüksek lisans Tezi, Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü, Isparta.

SHAHİ, C., & SİNHA, M. (2021). Digital transformation: challenges faced by organizations and their potential solutions. *International Journal of Innovation Science*, *13*(1), 17-33.

SHARİFABADİ MOROVATİ, A., ZİAEİAN, M., MİRFAKHRADİNİ, S.H. &ZANJİRCHİ, S.M. (2024). Toward Industry 4.0 in home appliance industry: challenges and future perspectives. Journal of Advances in Management Research, 21(3): 354-375. https://doi.org/10.1108/JAMR-03-2023-0070

SHARİFF, S. VE GOUİN, R. (2006). Cyber-dilemmas: Gendered hierarchies, new technologies and cyber-safety in schools. Atlantis: Critical Studies in Gender, Culture Social Justice, 31 (1), 27-37.

SHERMAN, W. R., & CRAİG, A. B. (2018). Understanding Virtual Reality: Interface, Application, and Design (Second Edition). Cambridge, MA: Morgan Kaufmann.

SİEVER, B., & ROGERS, M. P. (2016). A Hands-On Introduction to the Internet of Things. In *Proceedings of the 47th ACM Technical Symposium on Computing Science Education*, 715-715.

SİN TAN, K., CHOY CHONG, S., LİN, B., & CYRİL EZE, U. (2010). Internet-based ICT adoption among SMEs: Demographic versus benefits, barriers, and adoption intention. *Journal of enterprise information management*, *23*(1), 27-55.

SİNGH, A., & JAİN, A. (2018). Study of cyber attacks on cyber-physical system. In *Proceedings of 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT)*, 26-27.

SİPONEN, M. T. (2001). Five dimensions of information security awareness. *SIGCAS Comput. Soc.*, *31*(2), 24-29.

ŚLUSARCZYK, B. (2018). Industry 4.0–are we ready?. *Polish Journal of Management Studies*, *17*(1), 232-248.

SMİTH, B. L. (2001). The third industrial revolution: Policymaking for the Internet. *Colum. Sci. & Tech. L. Rev.*, *3*, 1.

SMİTH, P. K., MAHDAVİ, J., CARVALHO, M., FİSHER, S., RUSSELL, S., & TİPPETT, N. (2008). Cyberbullying: Its nature and impact in secondary school pupils. Journal of Child Psychology and Psychiatry, 49(4), 376-385.

SMİTHERS, T. (1997). Autonomy in robots and other agents. *Brain and cognition*, *34*(1), 88-106.

SOŁEK-BOROWSKA, C. (2018). The use and benefits of information communication technology by Polish small and medium sized enterprises. *Online Journal of Applied Knowledge Management,* 6(1), 211–225.

SOLİS, B., LİEB, R., & SZYMANSKİ, J. (2014). The 2014 state of digital transformation. Altimeter Group.

SOLMAZ, S. B. (2023). Siber Güvenlik Tarihindeki Dönüm Noktaları: Tehditlerin Evrimi Ve Savunma Stratejileri. *Orta Doğu ve Orta Asya-Kafkaslar Araştırma Ve Uygulama Merkezi Dergisi*, *3*(1), 1-9.

SRAİ, J. S. VE LORENTZ, H. (2019). "Developing Design Principles for the Digitalisation of Purchasing and Supply Management". Journal of Purchasing and Supply Management, 25(1), 78-98.

SRİRAM, I., & KHAJEH-HOSSEİNİ, A. (2010). Research agenda in cloud technologies. *arXiv preprint arXiv:1001.3259*.

STATİSTA, "Annual Number of Ransomware Attacks Worldwide from 2017 to First Half 2023", 23 Nisan 2024. https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/, (Erişim Tarihi: 15/12/2024).

STENBACKA, C. (2001). Qualitative research requires quality concepts of its own. Management Decision, 39(7), 551–555.

STİENNON, RİCHARD. (2015). "A Short History of Cyber Warfare", in James A. Green (ed.), Cyber Warfare: A Multidisciplinary Analysis. London: Routledge, pp. 7–32.

STOJMENOVİC, I., & ZHANG, F. (2015). Inaugural issue of 'cyber-physical systems'. *Cyber-Physical Systems*, *1*(1), 1-4.

STOLTERMAN, E., & FORS, A. C. (2004). Information technology and the good life. *Information systems research: relevant theory and informed practice*, 687-692.

STYLİANOU, A., & TALİAS, M. A. (2017). Big data in healthcare: a discussion on the big challenges. *Health and Technology*, *7*(1), 97-107.

SUN, Z., & HUO, Y. (2021). The spectrum of big data analytics. *Journal of Computer Information Systems*, *61*(2), 154-162.

SÜREN, E. (2019). An Efficient And Novel Detection Technique For Next Generation Web-Based Exploitation Kits, Middle East Technıcal University, Ankara.

ŞAHİN, Y. (2009). *Bilgi Yönetimi ve Tedarik Zinciri Yönetimindeki Uygulamaları*, Doktora Tezi, Marmara Üniversitesi, İstanbul**.**

ŞAHİN, Z., & ÇANKAYA, F. (2018). KOBİ'lerde Sürdürülebilirlik Raporlaması ve Türkiye Örneği. *Anadolu Üniversitesi Sosyal Bilimler Dergisi*, *18*(4), 117-132.

ŞAHİNASLAN, E., KANDEMİR, R., & ŞAHİNASLAN, Ö. (2009). Bilgi güvenliği farkındalık eğitimi örneği. *Akademik Bilişim*, *9*, 189-194.

ŞAHİNASLAN, E., KANTÜRK, A., ŞAHİNASLAN, Ö. VE BORANDAĞ, E. (2009). *Kurumlarda bilgi güvenliği farkındalığı, önemi ve oluşturma yöntemleri*, Akademik Bilişim, 9, 11-13.

ŞAHİNASLAN, Ö. (2013). *Siber Saldırılara Karşı Kurumsal Ağlarda Oluşan Güvenlik Sorunu Ve Çözümü Üzerine Bir Çalışma*,Doktora Tezi, Trakya Üniversitesi, Edirne.

ŞENOL, M. (2020). *Türkiye'nin Ulusal Siber Güvenlik Strateji ve Politikalarının Oluşturulması Çerçevesinde Caydırıcılık*. İstanbul Teknik Üniversitesi Bilişim Enstitüsü, Doktora Tezi, İstanbul.

ŞİŞMAN, D. & ŞİŞMAN, M. (2019). Gelişmekte Olan Ülkeler (Brezilya, Hindistan Ve Çin Örnekleriyle) Ve Bilişim Sektörü,https://www.researchgate.net/publication/336460561_GELISMEKTE_OLAN_ULKELER_BREZILYA_HINDISTAN_VE_CIN_ORNEKLERIYLE_VE_BILISIM_SEKTORU_Developing_Countries_With_Examples_From_Brazil_India_And_China_And_Ict_Sector (E .T.: 29.12.2024).

TAGHİYEV, A. (2019). Yabancı Sermayeli *KOBİ'lerin Karşılaştığı Sorunlar: Oka Kapsamındaki Şehirlerde Faaliyet Gösteren Kobi 'ler Üzerine Araştırma*,Yüksek Lisans Tezi, Samsun On dokuz Mayıs Üniversitesi/Sosyal Bilimler Enstitüsü.

TAHİR, R. (2018). A study on malware and malware detection techniques. *International Journal of Education and Management Engineering*, *8*(2), 20.

TALARİ, S., SHAFİE-KHAH, M., SİANO, P., LOİA, V., TOMMASETTİ, A., & CATALÃO, J. P. (2017). A review of smart cities based on the internet of things concept. *Energies*, *10*(4), 421.

TANRIKULU, İ. (2015). The relationships between cyber bullying perpetration motives and personality traits: Testing uses and gratifications theory. Orta Doğu Teknik Üniversitesi, Eğitim Bilimleri Enstitüsü.

TAŞ, H. Y. (2018). Dördüncü sanayi devrimi'nin (endüstri 4.0) çalışma hayatına ve istihdama muhtemel etkileri. *OPUS International Journal of Society Researches*, *9*(16), 1817-1836.

TAŞLI, S. (2022). Bulut Teknolojisi Kullanan Hasta Takip Hizmetlerinde Mikroservis Temelli Uç Sistem Tasarımı ve Geliştirilmesi, Yüksek Lisans Tezi, Fırat Üniversitesi, Elazığ.

TAVŞANCIL, E. (2005). Tutumların ölçülmesi ve SPSS ile veri analizi. Ankara: Nobel.

TEİCHERT, R. (2019). Digital transformation maturity: A systematic review of literature. *Acta universitatis agriculturae et silviculturae mendelianae brunensis*.

TEKEREK, M., VE TEKEREK, A. (2013). A research on students' information security awareness. Turkish Journal of Education, 2(3).

TEKİN, E., & GÜNGÖR, B. (2024). *Kobi'ler (Ar-Ge, İnovasyon, Dijital Dönüşüm, Fsmh, Yeni Nesil Destekler ve Dış Ticaret)-Kobi İhracat Terimleri Sözlüğü İle*. Eğitim Yayınevi.

TEKİN, Z. (2018). "The Examination of Applications of Industry 4.0 in Enterprises by Content Analysis Method", Pressacademia, 7(44), 251-255.

TERLİZZİ, M. A., MEİRELLES, F. D. S., & VİEGAS CORTEZ DA CUNHA, M. A. (2017). Behavior of Brazilian banks employees on Facebook and the cybersecurity governance. *Journal of Applied Security Research*, *12*(2), 224-252.

TERZİ, M. (2018). *Bilgi İletişim Teknolojilerine Dayalı Oluşumlar ile Bu Oluşumların Uluslararası İlişkilere Güvenlik Bağlamındaki Etkisi:Siber Terörizm*. Kara Harp Okulu Bilim Dergisi, 73-108.

TJAHJONO, B., ESPLUGUES, C., ARES, E., & PELAEZ, G. (2017). What does industry 4.0 mean to supply chain?. *Procedia manufacturing*, *13*, 1175-1182.

TONGA, M. Y., & Tonga, M. (2022). Endüstri 4.0'a Genel Bir Bakış: Sanayinin Geleceği. *Gü İslahiye İİBF Uluslararası E-Dergi*, *6*(6), 40-60.

TOZAN, A. (2007). Otonom Mobil Robot, Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi, İstanbul.

TÖRNGREN, M., & SELLGREN, U. (2018). Complexity challenges in development of cyber-physical systems. *Principles of modeling: Essays dedicated to Edward A. Lee on the occasion of his 60th birthday*, 478-503.

TULİ, P., & SAHU, P. (2013). System monitoring and security using keylogger. *International Journal of Computer Science and Mobile Computing*, *2*(3), 106-111.

TUNAY, M. (2024). Dolandırıcılık Girişimleri ve Dolandırıcılıktan Korunma Yöntemleri. *Avrasya Sosyal ve Ekonomi Araştırmaları Dergisi*, *11*(2), 168-187.

TUNJİ-OLAYENİ, P., AİGBAVBOA, C., OKE, A. & CHUKWU, N. (2024). Research trends in industry 5.0 and its application in the construction industry. Technological Sustainability, 3 (1): 1-23.

TURHAN, O. (2006). Bilgisayar ağları ile ilgili suçlar (Siber Suçlar). *Devlet Planlama Teşkilatı Müsteşarlığı Hukuk Müşavirliği, Planlama Uzmanlığı Tezi, Ankara*.

TURİNG, A. (1950) Computing machinery and intelligence. Mind, 49(236), 433–460.

TUTORİALSPOİNT. (n.d.). Artificial intelligence tutorial. TutorialsPoint. https://www.tutorialspoint.com/artificial_intelligence/artificial_intelligence_tutorial.pdf (05.11.2024).

TÜBİSAD & DELOİTTE. (2018). Bilgi ve İletişim Teknolojileri Sektörü 2017 Pazar Verileri. Bilgi Teknolojileri ve İletişim Kurumu. Deloitte Danışmanlık A.Ş.

TÜRK DİL KURUMU. Büyük Türkçe Sözlük. Türk Dil Kurumu (internette), Erişim: 09.11.2024, https://sozluk.gov.tr/

TÜSİAD. (2017). Türkiye'nin Sanayide Dijital Dönüşüm Yetkinliği. 20 Ekim 2024 tarihinde https://tusiad.org/tr/yayinlar/raporlar/item/9864-tusiad-bcg-turkiye-nin sanayide-dijital-donusum-yetkinligi sayfasından erişilmiştir.

UDO, G. J., & EDOHO, F. M. (2000). Information technology transfer to African nations: An economic development mandate. *The Journal of Technology Transfer*, *25*(3), 329-342.

ULAŞTIRMA, T. C., & BAKANLIĞI, A. (2020). Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020–2023).

ULUÇAY, A., & KÜÇÜK, U. F. (2023). Tarih Öğretiminde Sanal Gerçeklik Ve Artırılmış Gerçeklik: Geçmişi Canlandırmak İçin Yeni Yollar. *Niğde Ömer Halisdemir Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, *5*(2), 113-129.

ULUSOY, R., & AKARSU, R. (2012). Türkiye'de KOBİ'lere yapılan destekler ve istihdam üzerindeki etkileri. *Kocaeli Üniversitesi Sosyal Bilimler Dergisi*, (23), 105-126.

URAL, A. VE KILIÇ, İ. (2013). Bilimsel araştırma süreci ve SPSS ile veri analizi. Ankara: Detay.

UTAKRİT, N., & UTAKRİT, N. (2021). Similarity and Dissimilarity between Information Security and Information Assurance. *Information Technology Journal*, *17*(2), 46-56.

UZUN HAZNECİ, Ö. (2019). Güncel artırılmış gerçeklik uygulamalarının eğitim alanında kullanımı üzerine bir inceleme. *Ondokuz Mayıs Üniversitesi Uluslararası*, *100*, 26-28.

ÜNAL, G., & ULUYOL, Ç. (2020). Blok zinciri teknolojisi. *Bilişim Teknolojileri Dergisi*, *13*(2), 167-175.

ÜNAL, T. (2022). *Dijital Dönüşümde Siber Liderlik: Nitel Bir Araştırma*, Yüksek Lisans Tezi, Türk Hava Kurumu Üniversitesi, Ankara.

ÜNAL, Y. (2009). Bilgi toplumunun tarihçesi. Tarih Okulu, 5, 123-144.

VERHOEF, P. C., BROEKHUİZEN, T., BART, Y., BHATTACHARYA, A., DONG, J. Q., FABİAN, N., & HAENLEİN, M. (2021). Digital transformation: A multidisciplinary reflection and research agenda. *Journal of business research*, *122*, 889-901.

VERMESAN, O., FRİESS, P., GUİLLEMİN, P., GUSMEROLİ, S., SUNDMAEKER, H., BASSİ, A., ... & DOODY, P. (2009). Internet of things strategic research roadmap. In *Internet of things-global technological and societal trends from smart environments and spaces to green ICT* , 9-52.

VİNOD, P., JAİPUR, R., LAXMİ, V., & GAUR, M. (2009). Survey on malware detection methods. In *Proceedings of the 3rd Hackers' Workshop on computer and internet security (IITKHACK'09)* (pp. 74-79).

VİTERA, J., HÖRCHER, F., GRİESCH, L., GOLTZ, K., RÖßLER, J., MEYER, J., & SANDKUHL, K. (2022). On the Importance of Digital Transformation for SME-Results from a Survey among German SME. In *BIR Workshops*, 56-69.

VRANA, J. VE SİNGH, R. (2021). Dijitalleştirme, dijitalleştirme ve dijital dönüşüm. *Tahribatsız değerlendirme el kitabı 4.0* , 1-17.

WALCZUCH, R., VAN BRAVEN, G., & LUNDGREN, H. (2000). Internet adoption barriers for small firms in the Netherlands. *European Management Journal*, *18*(5), 561-572.

WARNER, K. S., & WÄGER, M. (2019). Building dynamic capabilities for digital transformation: An ongoing process of strategic renewal. *Long range planning*, *52*(3), 326-349.

WÄSCHLE, M., THALER, F., BERRES, A., PÖLZLBAUER, F., & ALBERS, A. (2022). A review on AI Safety in highly automated driving. *Frontiers in Artificial Intelligence*, *5*, 952773.

WATSON, D. P., & SCHEİDT, D. H. (2005). Autonomous systems. *Johns Hopkins APL technical digest*, *26*(4), 368-376.

WE ARE SOCİAL . (2024). Dıgıtal 2024 : 5 Bıllıon Socıal Medıa Users . We Are Social : https://wearesocial.com/uk/blog/2024/01/digital-2024-5-billion-social-media-users/

WU, M., LU, T. J., LİNG, F. Y., SUN, J., & DU, H. Y. (2010). Research on the architecture of Internet of Things. In *2010 3rd international conference on advanced computer theory and engineering (ICACTE)*, 5,5-484.

WYATT, J. C. (2001). 10. Management of explicit and tacit knowledge. *Journal of the Royal Society of Medicine*, *94*(1), 6-9.

XU, L. D., XU, E. L., & Lİ, L. (2018). Industry 4.0: state of the art and future trends. *International journal of production research*, *56*(8), 2941-2962.

XU, Y., LİU, X., CAO, X., HUANG, C., LİU, E., QİAN, S., LİU, X., WU, Y., DONG, F., QİU, C.-W., QİU, J., HUA, K., SU, W., WU, J., XU, H., HAN, Y., FU, C., YİN, Z., LİU, M., … ZHANG, J. (2021). ARTİFİCİAL intelligence: A powerful paradigm for scientific research. The Innovation, 2, 100179.

YALÇIN, N., VE AVŞAR, A. (2018). *Sosyal Mühendislik Atakları ve Alınması Gereken Önlemler,* 20. Akademik Bilişim 2018 Konferansı Bildirileri, Karabük Üniversitesi, 77- 85.

YAPICI, O. Ö. ve YILDIRIM, G. (2021). "Endüstri 4.0'ın turizm alanındaki kavramları üzerine bir araştırma", *IBAD Sosyal Bilimler Dergisi,* 11, 394-412.

YAŞAR, H. (2014). *Kurumsal siber güvenliğe yönelik tehditler ve mücadele yöntemleri: Eylem planı örneği*, Yüksek Lisans Tezi, Gazi Üniversitesi, Ankara.

YAŞAR, H., VE ÇAKIR, H. (2015). Kurumsal Siber Güvenliğe Yönelik Tehditler ve Önlemleri. *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, 3, 488-507.

YAYLA, M. (2013). Hukuki bir terim olarak siber savaş. *Türkiye Barolar Birliği Dergisi*, *104*, 177-202.

YAYLA, M. (2014). Siber savaş ve siber ortamdaki kötü niyetli hareketlerden farkı. *Hacettepe Hukuk Fakültesi Dergisi*, *4*(2), 181-200.

YAZICIOĞLU, Y. VE ERDOĞAN, S. (2004). Spss Uygulamalı Bilimsel Araştırma Yöntemleri Ankara: Detay Yayıncılık.

YBARRA, M. L. VE MİTCHELL, K. J. (2004). Online aggressor/targets, aggressors, and targets: A comparison of associated youth cha racteristics. Journal of Child Psychology and Psychiatry, 45, 1308-1316.

YE, Y., Lİ, T., ADJEROH, D., & IYENGAR, S. S. (2017). A survey on malware detection using data mining techniques. *ACM Computing Surveys (CSUR)*, *50*(3), 1-40.

YEUNG, J. H. Y., SHİM, J. P., & LAİ, A. Y. K. (2003). Current progress of e-commerce adoption: small and medium enterprises in Hong Kong. *Communications of the ACM*, *46*(9), 226-232.

YILDIRIM, A. & ŞİMŞEK, H. (2004). SOSYAL Bilimlerde Nitel Araştırma Yöntemleri, Seçkin Yayıncılık, Ankara.

YILDIRIM, A. (2014). İnternetin görünen yüzü. *Karamanoğlu Mehmetbey Üniversitesi Sosyal ve Ekonomik Araştırmalar Dergisi*, *2014*(3), 51-59.

YILDIRIM, A., VE ŞİMŞEK, H. (2013). Sosyal bilimlerde nitel araştırma yöntemleri (9. baskı). Ankara: Seçkin Yayıncılık.

YILDIRIM, A., VE ŞİMŞEK, H. (2016). Sosyal bilimlerde nitel araştırma yöntemleri. Seçkin Yayıncılık.

YILDIRIM, B.F. VE ÖNAY, O. (2013). Bulut teknolojisi firmalarının bulanık AHP-Moora yöntemi kullanılarak sıralanması. İstanbul Üniversitesi İşletme Fakültesi Yönetim Dergisi, 24 (75), 59-81.

YILDIRIM, Ş. S., & DURUKAN, L. (2023). İmalatçı KOBİ'lerin Dijital Dönüşümü: KOSGEB Desteği Özelinde Nicel Bir Araştırma. *Çankırı Karatekin Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, *13*(3), 905-930.

YILMAZ, D. (2022). *Bilgi ve İletişim Teknolojilerinin Makroekonomik Faktörler Üzerindeki Etkileri,* Yüksek Lisans Tezi, Bilecik Şeyh Edebali Üniversitesi, Bilecik.

YILMAZ, E. N., GÖNEN, S., ŞANOĞLU, S., KARACAYILMAZ, G., & ÖZBİRİNCİ, Ö. (2021). Endüstri 4.0'ın gelişim sürecinde unutulan bileşen: Siber güvenlik. *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, *9*(4), 1142-1158.

YILMAZ, E., ŞAHİN, Y. L., VE AKBULUT, Y. (2016). Digital data security awareness of teachers. Sakarya University Journal of Education, 6(2), 26-45.

YILMAZ, M. (2009). Enformasyon ve Bilgi Kavramları Bağlamında Enformasyon Yönetimi ve Bilgi Yönetimi. *Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi*, *49*(1), 95-118.

YILMAZER, B., & SOLAK, S. (2020). Cloud computing based masked face recognition application, In 2020 Innovations in Intelligent Systems and Applications Conference (ASYU) (1-5). IEEE.

YİĞİT, M. F. VE SEFEROĞLU, S. S. (2019). Öğrencilerin siber güvenlik davranışlarının beş faktör kişilik özellikleri ve çeşitli diğer değişkenlere göre incelenmesi, Mersin Üniversitesi Eğitim Fakültesi Dergisi, 15(1): 186-215.

YOUNG, A., & ROGERS, P. (2019). A review of digital transformation in mining. *Mining, Metallurgy & Exploration*, *36*(4), 683-699.

YUEN, S. C. Y., YAOYUNEYONG, G., & JOHNSON, E. (2011). Augmented reality: An overview and five directions for AR in education. *Journal of Educational Technology Development and Exchange (JETDE)*, *4*(1), 11.

YÜKSEKBİLGİLİ, Z., & ÇEVİK, G. Z. (2018). Endüstri 4.0 bağlamında Türkiye'nin yerine ilişkin güncel ve gelecek eksenli bir analiz. *Finans Ekonomi ve Sosyal Araştırmalar Dergisi*, *3*(2), 422-436.

ZAFAR, R., YAFİ, E., ZUHAİRİ, M. F. VE DAO, H. (2016). BİG data: the nosql and RDBMS review. International Conference on Information and Communication Technology (ICICTM), (2016, 16-17 May) Kuala Lumpur, Malaysia, 120-126.

EKLER

ANKET FORMU

Sayın Katılımcı;

Bu anket, ***"Dijital Dönüşüm Sürecinde Siber Güvenlik Farkındalığı: Konya'da Bilişim Sektöründe Faaliyet Gösteren Kobiler Üzerine Bir Araştırma"*** *başlıklı Necmettin Erbakan Üniversitesi Sosyal Bilimler Enstitüsü Yönetim Bilişim Sistemleri Anabilim dalı Yüksek Lisans tez çalışmasında kullanılacaktır. Çalışmanınamacına ulaşması siz değerli katılımcılarımızın cevaplarına bağlıdır. Bu nedenle, soruları titizlikle okumanız ve cevaplamanız büyük önem taşımaktadır.*

Katılımınız ve değerli katkılarınız için şimdiden teşekkür ederim.

Prof. Dr. Mustafa KOCAOĞLU
Öğretim Üyesi

Tuğba ÇALIŞKAN
Yüksek Lisans Öğrencisi

A. KİŞİSEL BİLGİLER

Aşağıda bazı kişisel özelliklerinizin belirlenmesi amacıyla sorular sorulmaktadır. Size yöneltilen her soru için durumunuza en uygun seçeneğin karşısındaki yuvarlağın içerisine (X) işareti koyunuz.

1 Cinsiyetiniz?

( ) Kadın ( ) Erkek

2 Yaşınız?

( ) 18-25 Yaş Arası ( ) 26-33 Yaş Arası ( ) 34-41 Yaş Arası ( ) 42-49 Yaş Arası ( ) 50 Yaş ve Üzeri

3 Eğitim Durumunuz?

( ) İlköğretim ( ) Ortaöğretim (Lise) ( ) Ön Lisans ( ) Lisans ( ) Yüksek Lisans ( ) Doktora

4 İşletmedeki Toplam Çalışma Süreniz?

( ) Bir Yıldan Az ( ) 1-3 Yıl ( ) 3-5 Yıl ( ) 5-15 Yıl ( ) 15-25 Yıl ( ) 25 Yıldan Fazla

5 İşletmenizdeki Pozisyonunuz Nedir?

( ) Üst düzey yönetici (Genel Müd., Şirket Müd., Fabrika Müdürü, Genel Müdür Yardımcısı vb.)

( ) Orta düzey yönetici (Bölüm Md., Departman Md., Kısım Md. vb.)

( ) Alt Düzey yönetici (Şef, Md. Yrd., Vardiya Amiri vb.)

( ) Teknik çalışan

( ) İdari çalışan

B. SİBER GÜVENLİK FARKINDALIĞI

6. Siber güvenlik farkındalığı ile ilgili aşağıdaki ifadelere katılım düzeyinizi belirtiniz.

. *Lütfen, her bir ifadeye ilişkin katılım düzeyinizi belirtiniz.* **1-Kesinlikle Katılmıyorum 2-Katılmıyorum 3-Kararsızım 4-Katılıyorum 5.Kesinlikle Katılıyorum**	**Kesinlikle Katılmıyorum**	**Katılmıyorum**	**Kararsızım**	**Katılıyorum**	**Kesinlikle Katılıyorum**
1. İşletmemizde, bilgi güvenliğini artırmak amacıyla antivirüs ve kötü amaçlı yazılım yazılımları aktif olarak kullanılıyor.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
2. Yetki sahibi olmadığımız dosyalara erişimimiz işletmemiz tarafından engellenmektedir.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
3. İşletmemizde, yeni çalışanlara yönelik oryantasyon kapsamında siber güvenlik eğitimlerine yer verilmektedir.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
4. Bilgisayar ve bilgi güvenliği konusunda eğitim aldım.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
5. Bilgisayar becerilerimi güncellemek için eğitimlere katılmak benim için önemlidir.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
6. Bilgisayar güvenliğine dikkat edilmesinin önemli olduğunu düşünüyorum.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
7. İşletme yönetimimiz siber güvenlik konusunu çok ciddiye alır.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
8. İşletmemiz sık sık kurumun siber güvenlik durumuna ilişkin bilgiler gönderiyor.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**

9. Bilgisayarlar konusunda bilgili olduğumu düşünüyorum.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
10. Önemli bilgileri yedekleyip güvenliğini sağlarım.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
11. Şifrelerimi özenle korurum.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
12. Çalışanları çeşitli siber güvenlik tehditlerine karşı sürekli olarak uyarmanın motive edeceğine inanıyorum.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
13. Siber tehditlerin işletmemiz üzerinde olumsuz bir etkisi olabileceğine inanıyorum.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
14. İşletmemizde, korumamız gereken müşteri veya tedarikçi verilerine sahibiz.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
15. İşletmemizde kendi BT sistemlerine bağlantı sağlayan ya da bizim sistemlerimize bağlanmasına izin verdiğimiz tedarikçilerimiz veya müşterilerimiz var.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
16. İş yerindeki herkes şirketin paylaşılan dosya sunucularındaki herhangi bir dosyaya erişebilir.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
17. İşletmemizde, bilgisayarlarımızın kurulumu için özel Bilgi Teknolojileri destek personeli bulunmaktadır.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
18. İşletmemiz, siber güvenliği de içeren derinlemesine bir risk analizi yapmaktadır.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
19. Şifrelerimi oluştururken semboller, sayılar ve büyük harfler içeren tahmin edilmesi zor bir şifre seçiyorum.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
20. Hesaplarımın şifrelerini kimseyle paylaşmıyorum.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
21. Cihazlarımda yüklü olan güvenlik duvarını açık tutuyorum.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
22. İnternetten indirdiğim dosyaları antivirüs programı ile tarama yapmadan açmıyorum.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
23. Cihazlarımı düzenli olarak bir anti-virüs programı ile tararım.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
24. Tanımadığım kişilerden gelen e-postalara güvenmiyorum.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**

25. Bilinmeyen kaynaklardan gelen bağlantıları ve ekleri açmıyorum.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
26. Bilgisayarımda bir casus yazılım önleme aracı kullanıyorum.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
27. E-posta gönderirken şifreleme kullanıyorum.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
28. Olağandışı bilgisayar davranışlarını/yanıtlarını izlerim (örneğin bilgisayarın yavaşlaması veya donması, açılır pencereler vb.)	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
29. Casus yazılım ve kötü amaçlı yazılımlardan kurtulma konusunda kendime güveniyorum.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
30. Şifrelerin düzenli olarak değiştirilmesi gerektiğini düşünüyorum.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
31. Kişisel akılı telefonumu iş ile ilgili konularda da kullanıyorum.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
32. Dosyaları düzenli olarak yedekliyorum.	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**

YARI YAPILANDIRILMIŞ GÖRÜŞME FORMU

Sayın Katılımcı;

*Bu görüşme soruları, **"Dijital Dönüşüm Sürecinde Siber Güvenlik Farkındalığı: Konya'da Bilişim Sektöründe Faaliyet Gösteren Kobiler Üzerine Bir Araştırma"** başlıklı Necmettin Erbakan Üniversitesi Sosyal Bilimler Enstitüsü Yönetim Bilişim Sistemleri Anabilim dalı Yüksek Lisans tez çalışmasında kullanılacaktır. Yapmakta olduğum araştırma kapsamında görüşme sorularına verdiğiniz cevapları daha sağlıklı bir şekilde aktarabilmem ve zamanı daha iyi kullanabilmemiz için izniniz olursa ses kaydına almak istiyorum. Vereceğiniz cevaplar bilimsel veri olarak kullanılacak olup bilimsel araştırma dışında gizli tutulacaktır.*

Araştırmaya katılmayı kabul ettiğiniz ve değerli katkılarınız için şimdiden teşekkür ederim.

GÖRÜŞME SORULARI

1. İşletmeniz kaç yıldır faaliyette bulunmaktadır?
2. İşletmenizdeki pozisyonunuz nedir?
3. İşletmenizde kaç çalışan var?
4. Dijital cihazları ve interneti kullanma konusundaki beceri düzeyinizi nasıl değerlendirirsiniz?
5. Hassas verilere erişiminiz sınırlı mı?
6. Verilerinize kimler erişim sağlayabilir?
7. İşlemenizde siber güvenlik farkındalığından kim sorumlu?

8. İşletmenizde siber güvenlik farkındalığı girişimlerinin amacı nedir?
9. Çalışanlarınıza rutin olarak ne tür siber önleme eğitimi ve öğretimi sağlıyorsunuz?
10. Bir siber saldırı meydana gelirse acil durum planınız ne olur?
11. Siber güvenlik konusunda en çok zorlandığınız şey nedir?
12. İşletmenizde güvenlik farkındalığını artırmak için geliştirmek istediğiniz teknikler nelerdir?
13. Siber güvenlik farkındalığında hangi özelliklerin iyileştirilmesi gerekiyor?