KRİTİK ENDÜSTRİYEL ALTYAPI GÜVENLİĞİ III:
Finansman Hizmetlerinin Güvenliği

ARAŞTIRMA RAPORU EYLÜL 2022

thinktech
STM Teknolojik Düşünce Merkezi

STM ThinkTech

1. GİRİŞ

Finansal hizmetler sektörü, bankacılık, sigorta, para ve sermaye piyasaları dahil olmak üzere, yatırım ve paranın tahsisi ile ilgili ticari faaliyetleri kapsayan geniş bir sektör grubunu içermektedir[1]. Küresel finans sektörünün büyüklüğü hakkında, sektörün kapsamına ilişkin farklı yorumlardan ötürü çeşitli tahminler bulunmaktadır. Yine de tahminlerin çoğuna dayanarak, finansal hizmetler sektörünün dünya ekonomisinin yaklaşık yüzde 20-25'ini oluşturduğunu[1] ileri sürmek mümkündür. Bir tahmine göre, 2021'in sonunda finansal hizmetler sektörü, bir önceki yıla göre yüzde 9,9 oranında büyüyerek 22,5 trilyon dolara ulaşmıştır[2].

Türkiye'de finans sektörü büyük önem taşımaktadır. Türk finans sektörünün aktif büyüklüğü 2021 yılı sonunda 10,5 trilyon Türk lirasına ulaşmıştır[3]. Söz konusu miktar 2021 yılı sonu itibarıyla Türkiye'nin Gayri Safi Yurtiçi Hasılasının (GSYH) yüzde 130'undan fazladır. Dolayısıyla finansman kuruluşlarının güvenliği, ekonomik güvenliğin sağlanmasında öncelikli konulardan biridir. Ekonomik güvenlik, ulusal ekonominin bağımsızlığını, istikrarını ve dayanıklılığını, sürekli yenilenme ve kendini geliştirme yeteneğini sağlayan bir faktördür ve ulusal güvenlikle doğrudan bağlantılıdır. Zayıf ve verimsiz bir ekonomide savunma ve güvenliğin tam olarak sağlandığından söz edilemez. Bu nedenle finansman kuruluşları kritik altyapılar olarak görülmekte ve bahse konu yapıların özellikle uluslararası siber alandaki risklere karşı korunması büyük önem taşımaktadır.

Dünyada ve Türkiye'de kritik altyapıların mevcut durumunu ve temel eğilimlerini aktarmak; sözkonusu altyapılara yönelik tehditleri irdelemek ve bunları bertaraf etmek maksadıyla geliştirilen çözüm önerilerini sunmak için başlattığımız "Kritik Endüstriyel Altyapı Güvenliği" başlıklı Araştırma Raporu yazı dizimizin üçüncü bölümünde finansman hizmetlerinin güvenliği ele alınacaktır. Yazı dizimizin bu son bölümünde, ilk olarak finans sektörünün amiral gemisi olan bankacılık sektörünün Türkiye ve dünyadaki güncel durumu, yakın geleceğe ilişkin eğilimler, kritik altyapı olarak bankacılık sektörünün karşı karşıya olduğu riskler ve sektörün elastikiyetinin artırılması için önerilere göz atılacaktır.Daha sonra finans sektörünün ikinci büyük bileşeni olan para ve sermaye piyasalarının önemi ve güvenliği ele alınacaktır. Son olarak da kişi ve kurumların karşılaştıkları riskin sosyal transferi ile ekonomik büyümeyi, yeni girişimleri ve inovasyonu destekleyen sigorta sektörünün mevcut durumu, genel eğilimleri ve güvenliğine ilişkin tehditler incelenecektir.

2. BANKACILIK SİSTEMİ İLE İLGİLİ YAPILARIN GÜVENLİĞİ

Finansal hizmetlerin amiral gemisi bankacılık sektörüdür. Finansal sistem içinde bankacılık sektörü, gücü ve büyüklüğü açısından çok önemli bir yer tutmaktadır. Bankalar, temel olarak fon fazlası olanlardan toplanan kaynakların, fon talebi olanlara kredi olarak verilmesine aracılık eden finansal kuruluşlardır. Böylece bankalar tasarruflar ve yatırımlar arasında en uygun şekilde değişimin gerçekleşmesini sağlayan kuruluşlar olarak önemli bir görevi yerine getirmektedirler[4].

Ancak bankacılık sektörünün ülke ekonomisindeki rolü çok daha kapsamlıdır: Bankacılık sistemi, içinde bulunduğu ekonomik yapının istikrarlı ve güvenilir bir şekilde hem büyümesine katkı sağlamakta hem de oluşabilecek iç ve dış etkenli finansal risklere karşı dayanaklılığı artırmaktadır. Bankacılık sektörünün sağlıklı işleyişi fon dağılımının güvenliği ve ulaşılabilirliğini sağlaması açısından, ekonomik sistemin işleyişini kolaylaştırmaktadır[5].

Bankacılık sektöründe meydana gelebilecek zafiyetler, ülke ekonomisinde derin finansal sorunlara, adaletsizliklere yol açabilir. Bir ülkenin bankacılık sisteminin risklerinin iyi yönetilememesi ve elastikiyetinin sağlanamaması, bu kritik sektörün aynı zamanda küresel finansal krizlerden daha fazla zarar görmesine sebep olabilir. Bankacılık sisteminin finansal sistem için stratejik ve hassas konumu, risk yönetimini sadece sektör için değil, ülke ekonomisi içinde stratejik hâle getirmektedir.

Bu bölümde dünyada ve Türkiye'de bankacılık sektörünün mevcut durumu, sektörün geleceğine dair öngörüler ve karşı karşıya bulunduğu riskler irdelenecektir.

2.1 Küresel Bankacılık Sektörünün Dünya Ekonomisindeki Yeri

Küresel bankacılık sektörünün büyüklüğü net olarak belli değildir. Dünyada tam olarak kaç banka olduğu konusunda sadece tahminler bulunmaktadır. Dolayısıyla bankaların varlıkları ve küresel ekonomideki payı da tahminlere dayanmaktadır.

Küresel bankacılık sektörünün, 2021'in ilk çeyreğinde 7,3 trilyon avroluk piyasa değeri olduğu tahmin edilmiştir[6]. Küresel piyasa kapitalizasyonun, bir başka deyişle dünyadaki her borsada işlem gören şirketlerin toplam değerinin 56 trilyon dolar olduğu tahmin edilmiştir. Bu metrikleri kullanarak bankacılık sektörünün küresel ekonominin yüzde 14'ünü oluşturduğunu söylemek mümkündür[7].

Ancak bu, eksik bir ölçümdür çünkü yalnızca hisseleri borsada işlem gören bankaları ölçmektedir. Halka açılmamış bankalar, yatırım bankaları veya devlete ait bankalar ile bankacılık lisansına sahip sadece çevrimiçi hizmet veren "FinTech" şirketleri hakkında bilgi içermemektedir. Değerlendirilmeye değer başka bir istatistik ise yönetim altındaki varlıklardır. Yönetim altındaki varlıklar, bir yatırım şirketi tarafından müşterileri için yönetilen varlıkların toplam miktarını gösteren bir rakamdır. Boston Consulting Group'a göre, 2020'de küresel bankacılık sektörünün yönetimi altındaki varlıklar 103 trilyon dolara ulaşmıştır[8]. Küresel varlıkların toplamının 431 trilyon dolar olarak tahmin edildiği düşünüldüğünde, bankacılık ve yatırım sektörünün, dünya varlıklarının dörtte birinden biraz azını oluşturduğu söylenebilir[9].

Farklı rakamlara rağmen, ifade edilen paylar bankaların küresel ekonomideki önemine işaret etmektedir. Bankaların temel işlevleri, bir ülke, bir bölge veya dünya genelinde mevcut tasarrufların finansman ihtiyacı olan ekonomik birimlere mümkün olan en iyi şekilde tahsis edilmesini sağlamaktır. Bankalar gelişmekte olan ülkelerde farklı görevler de üstlenebilmektedir. Dünya Bankasının altını çizdiği üzere, "Güçlü finansal sistemler oluşturmak, ekonomik büyüme ve kalkınmanın temelidir" ve bu "yoksulluğu azaltma ve paylaşılan refahı teşvik etme misyonunu gerçekleştirmek için esastır."

Dünya Bankasına göre güçlü finansal sistemler[10]:

- Finansal istikrarı sağlar, dolayısıyla istihdam yaratır ve üretkenliği artırır.
- Finansal hizmetlere erişimi kolaylaştırarak genel refahı artırır ve eşitsizliklerin azaltılmasına da katkıda bulunur.
- Çeşitli kritik öneme sahip altyapıların (yollar, enerji santralleri, okullar, hastaneler, konutlar vb.) finansmanını sağlayarak ülke kalkınmasında önemli rol oynarlar.

Bankalar ve diğer finans kuruluşları, kendileri kritik altyapı oldukları gibi diğer kritik altyapıların elastikiyetinin artırılması için de gerekli finansmanın sağlanmasına katkıda bulunmaktadır. Örneğin 2014 yılında, ABD'nin New Jersey eyaleti, başta enerji ve su olmak üzere kritik altyapıların güvenliği ve elastikiyetini artıracak projelere finansman sağlayacak bir banka kurmuştur[11].

Kalkınma ve sürdürülebilir ekonomideki önemli rolleri küçümsenemez olmakla birlikte, dünya genelinde bankaların büyük bölümünün öncelikle kâr amacı güden kuruluşlar olduğu unutulmamalıdır. Bankaların kârlılığı ile ekonomik büyüme arasında doğrudan bir bağlantı bulunmaktadır[12]. Bankacılık sektörü, ekonomik büyüme için ihtiyaç duyulan fon ve tasarrufların toplanmasını ve dolayısıyla çoğu sektörde yeni girişimlerin ortaya çıkmasını sağlamaktadır. Artan bu tasarruflar, sermaye birikimine olumlu etki yaparak, kredi mekanizması aracılığıyla ekonomik büyüme ve istihdam yaratılmasını sağlamaktadır.

Ancak diğer yandan bankacılık sektörü ile ekonomik büyüme arasındaki ilişki her zaman aynı yönde olmamaktadır. ABD'de patlak veren ve tüm dünyaya yayılan 2008 küresel finansal krizi bu ilişkiyi olumsuz etkilemiş, teknolojinin ve küresel ekonomik ilişkilerin gelişmesi bu krizlerin yayılma hızını artırmıştır. 2008 krizinden sonra bankaların sağlığı ve güvenilirliği kamu otoriteleri tarafından büyük önem verilerek izlenmektedir. Hemen hemen tüm ülkeler bankacılık sektörü üzerindeki kontrollerini artırmış ve bu duruma yönelik yeni tedbirler almıştır. Zira 2008 krizi bankacılık sistemlerinin başarısızlığının küresel çapta ekonomik paniğe neden olabileceğini ve ülke ekonomilerine ciddi zarar verebileceğini göstermiştir.

Küresel olarak bankalar, krizin ardından COVID-19 pandemisine kadar enerjilerini esas olarak zorunlu yasal sermayelerini yeniden oluşturmaya, düzenleyici sınırları onarmaya, dijitalleşmeye yatırım yapmaya, üretkenlik ve verimlilik kazanımları elde etmeye harcamışlardır. Bunun sonucu olarak pandemiye rağmen kârlılıklarını artırabilmişlerdir[13]. Ne var ki, daha pandemi tam olarak bitmeden patlak veren Rusya-Ukrayna Savaşı bankalar için de görünümü olumsuza çevirmiştir. Avrupa Merkez Bankasının 2022'nin Mayıs ayında uyardığı üzere, savaşın enerji fiyatları, enflasyon ve büyüme üzerindeki etkisi mevcut kırılganlıkları artırmıştır[14]. Artan maliyetler ve düşen taleple ortaya çıkan stagflasyon, geri ödenmeyen kredi riskini artırarak dünyayı yeni bir finans krizine sürükleyebilir.

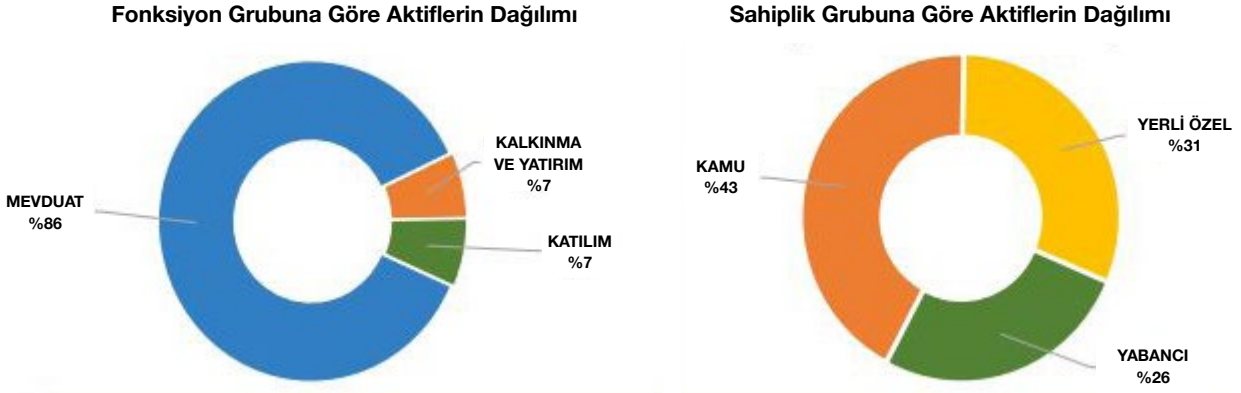
2.2 Türkiye'de Bankacılık Sektörünün Ekonomideki Yeri

Bir ülkenin bankacılık sisteminin ekonomik ve teknolojik gücü ile büyüklüğü, ekonomik dalgalanmalara karşı dayanıklılığını artırmasının yanında sermayeye kolay ulaşımı sağlayabilmektedir.

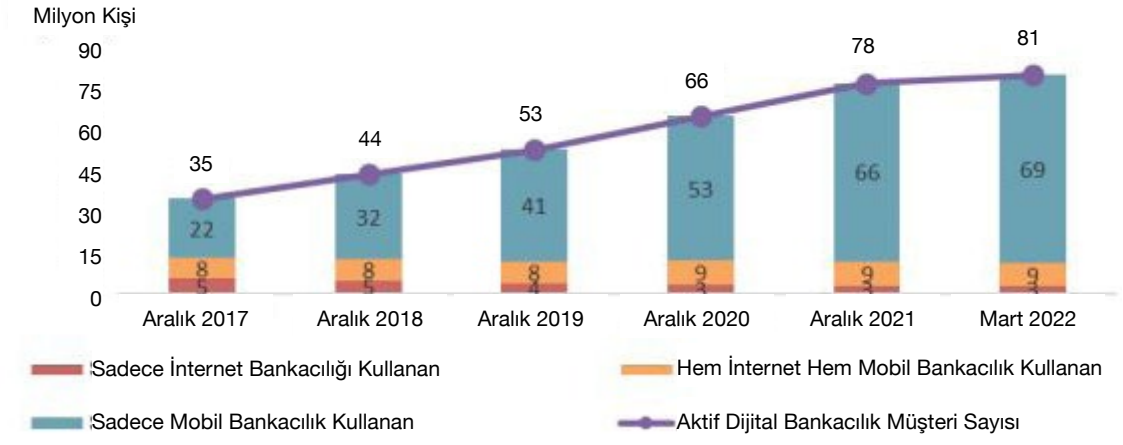
Türkiye'de kamu bankalarının yanı sıra, yerli ve yabancı sermayeli özel bankaların faaliyet gösterdiği dinamik bir bankacılık sektörü bulunmaktadır. Mart 2022 itibarıyla Türkiye'de 34'ü mevduat, 16'sı kalkınma ve yatırım ve altısı katılım bankası olmak üzere toplam 56 banka faaliyet göstermektedir[15]. Buna 1 Ocak 2022 itibarıyla faaliyet izni verilen ve sadece dijital kanallarda hizmet sunabilecek dijital bankalar dahil değildir[16]. Söz konusu bankaların toplam 11.105 şubesi ve 201.597 personeli bulunmaktadır. Türkiye'de bankaların aktif büyüklüğü 2021 yılında, bir önceki yıla göre yüzde 51 oranında artarak 9,215 trilyon TL'ye çıkmıştır. Aynı dönemde bankaların toplam mevduatı bir önceki yıla kıyasla yüzde 53 artışla 5,303 trilyon TL'ye, kredi büyüklüğü ise bir önceki yıla kıyasla yüzde 37 artışla 4,901 trilyon TL seviyesine ulaşmıştır. Sektörün toplam aktif büyüklüğünün GSYH'ye oranı yüzde 122'den yüzde 128'e yükselmiştir. Bankaların sermaye yeterlilik oranı yüzde 18,39 olarak gerçekleşmiş, net dönem kârı ise bir önceki yıla göre yüzde 59 artarak 93 milyar TL'ye ulaşmıştır[3].

Türkiye'de bankacılık sektörünün güçlü yönlerinden biri, ileri düzeyde dijitalleşmiş olmasıdır. Teknoloji alanında yaşanan gelişmeler bankaların geleneksel bankacılık anlayışlarından vazgeçmelerini ve dijital yeniliklerin örgüt yapılarına entegre edilmesini sağlamıştır. Türk bankacılık sektöründe 1987 yılında kurulan ilk ATM cihazı ile başlayan dijitalleşme süreci, 1991 yılında telefon bankacılığının hizmete sunulması ile devam etmiştir. 2000'li yıllarda internet kullanımının hızlı bir şekilde artması bankaları internet siteleri kurmaya zorlamış ve internet bankacılığı hizmeti müşterilerin kullanımına sunulmuştur. 2006 yılında akıllı telefonların kullanılmaya başlanması bankacılık hizmetlerinin dijitalleşmesi açısından bir devrim niteliğinde olmuş ve bankalar tarafından mobil bankacılık uygulamaları geliştirilmiştir. Bu raporda yer alan istatistikler, Türkiye Bankalar Birliği üyesi ve internet bankacılığı hizmeti veren 27 banka ile mobil bankacılık hizmeti veren 22 banka verisinden oluşmaktadır. Ocak-Mart 2022 dönemi içinde toplam (bireysel ve kurumsal) aktif dijital bankacılık müşteri sayısı 80 milyon 927 bin kişiye ulaşmıştır. Bu sayının 2 milyon 667 bin kişisi "sadece internet bankacılığı" işlemi yaparken, 69 milyon 493 bin kişisi "sadece mobil bankacılık" işlemi yapmıştır. Hem internet hem mobil bankacılık işlemi yapan kullanıcı sayısı ise 8 milyon 767 bin kişidir[17].

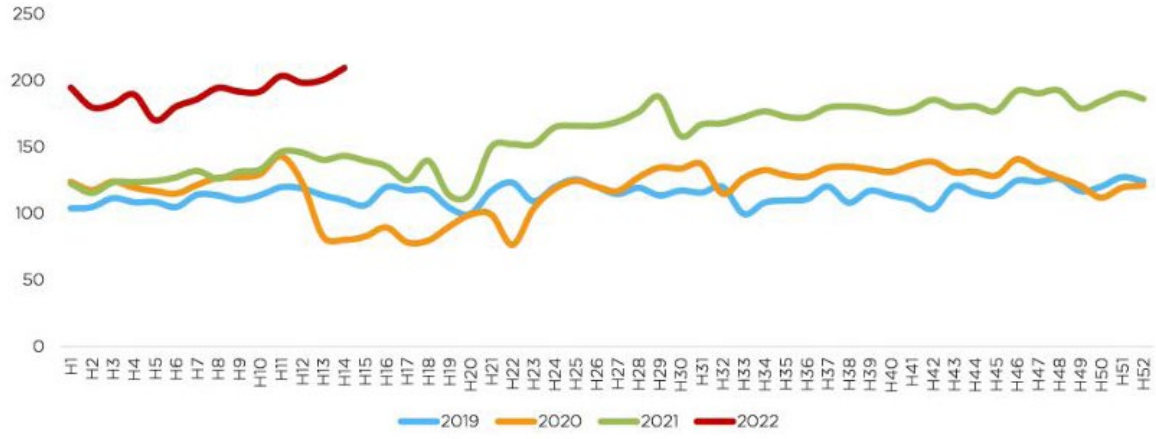
Bu uygulamaların dışında 2012 yılında QNB Finansbank bünyesinde oluşturulan Enpara.com markası, dijital



Şekil 1: Türkiye'de faaliyet gösteren bankaların fonksiyon ve sahiplik durumuna göre dağılımı[15].



Şekil 2: Türkiye'de internet ve mobil bankacılık kullanımın yıllar içinde seyri[17].



Şekil 3: Türkiye'de kredi ve banka kartı işlem adedi (2019-2022; milyon adet)[20].

bankacılık anlamında Türk bankacılık sektöründeki ilk dijital banka olarak gösterilmektedir. 2021 yılı sonu itibarıyla Enpara.com'un 3 milyon bireysel müşteriye, 34,9 milyar TL mevduat büyüklüğüne ve 10,9 milyar TL kredi büyüklüğüne ulaştığı ifade edilmektedir[18].

Türkiye'de kredi kartı kullanımı da yaygındır. Bankalararası Kart Merkezi (BKM) verilerine göre Mart 2022 itibarıyla Türkiye'de kredi kartı sayısı 88 milyondan fazladır ve ülke nüfusunu aşmıştır[19]. Kredi ve banka kartlarıyla yapılan işlemlerin sayısı ve tutarı, özellikle pandemi döneminde sıçrama kaydetmiştir (Şekil 3).

Türk bankacılık sisteminin elastikiyet düzeyine ilişkin olarak ise farklı görüşler bulunmaktadır. Türkiye'de bankacılık sektörü yakın tarihte ciddi krizler yaşamıştır. Ülkemizde uygulanan yanlış ekonomi politikaları, finansal sistemin zemininin sağlam olmayışı ve siyasi belirsizlik ortamının etkisiyle yaşanan Kasım 2000 ve Şubat 2001 krizleri; finansal sistemin ve ekonominin çöküşüyle sonuçlanmıştır[21]. Kriz sonrasında bankacılık sektörü yeniden yapılandırılmış, yapılan yanlışlardan ders alınma yoluna gidilmiştir. 2008 yılında ABD'de başlayıp tüm dünyayı etkisi altına alan 2008 krizinden Türkiye ekonomisi de olumsuz etkilenmiş, ancak finans sektörü krizin üstesinden en az hasarla gelebilmiştir[21]. Ne var ki 2018 yılından sonra yurtiçi ve uluslararası dinamiklerin etkisiyle Türkiye'de bankacılık sektörünün yeni bir kırılgan döneme girdiği ifade edilmektedir[5], [22]. Yine de 2021 yılı sonunda lirada yaşanan hızlı değer kaybı sermaye yeterliliği konusunda endişelere yol açmakla birlikte, ülkemizde bankacılık sektörünün, operasyonel ve sermaye yapısının güçlü olması sayesinde bu değişime ayak uydurulabileceği şeklinde yorumlanmaktadır[16].

2.3 Küresel Bankacılıkta Genel Eğilimler

Bankacılık ekonomik faaliyetlerin canlı ve çeşitlenmiş olduğu ülkelerde değer zincirlerinin vazgeçilmez unsurlarıdır. Yaşanan büyük finans krizleri bankalara duyulan güveni törpülemiş olmakla birlikte, dünya genelinde bankacılık hizmetlerine erişim artmaktadır. Uluslararası Para Fonu (IMF) tarafından yayınlanan "Finansal Erişim Anketi 2021"[23], COVID-19 pandemisinin öncesinde dünyada finansal hizmetlere erişimin artış eğiliminde olduğuna, düşük ve orta gelir grubundaki ülkelerde her 1.000 kişi başına düşen banka hesabı sayısının hızla arttığına işaret etmektedir. Bu artışın önemli faktörlerinden biri dijital hizmetlerin gelişmesidir. Özellikle düşük ve orta gelir grubundaki ülkelerde cinsiyet, eğitim durumu, coğrafi koşullar gibi sebeplerle finansal hizmetlere erişimi kısıtlı olan alt grupların, dijital finansal hizmetlerin kullanımının genişlemesiyle finansal hizmetlere erişimi mümkün kılınmıştır.

Finansal Erişim Anketi sonuçlarına göre, araştırmanın yapıldığı dönemde, düşük ve orta gelir grubu ülkelerde fiziksel banka şubesi sayısı 2013 seviyelerinde seyrederken, yüksek gelir grubu ülkelerde fiziksel banka şubesi sayısında düşüş gözlenmesi, dijital finansal hizmetler adaptasyonun hızlı olduğunu göstermektedir. 2015-2020 yılları arasında düşük ve orta gelir grubu ülkelerde internet ve dijital bankacılık kanalları üzerinden gerçekleşen işlem hacmi büyük artış göstermiştir[23].

Son yıllarda artan e-ticaret hacmi ile yaygınlaşmaya başlayan dijital ödeme yöntemleri COVID-19 etkisiyle büyük bir ivme kazanmıştır. 2020 yılında dünya genelinde yapılan e-ticaret ödemelerinin yüzde 44,5'i dijital/mobil cüzdan ile yapılmıştır[24]. Dijital/mobil cüzdanın arkasından yüzde 22,8 ile kredi kartı ödemeleri ve yüzde 12,3 ile banka kartı ödemeleri gelmektedir.

Yapılan değerlendirmeler bankacılık hizmetlerinde dijitalleşmenin hız kesmeden devam edeceği, geleneksel bankaların yanı sıra yeni oyuncuların dijital hizmetler sunmaya başlayabileceği ve finans dünyasında merkezi bir rol üstlenebileceği yönündedir. Nihayetinde bankacılık, fiziksel mekânlar olmaktan çıkabilir veya düşük miktarlı işlemlerin ATM'den halledildiği, diğer tüm işlemlerin çevrimiçi hâle geldiği bir finansal hizmet kolu hâline dönüşebilir.

2.3.1 Hızlanan Dijital Dönüşüm

Bankacılık, dünya genelinde dijitalleşme oranının en yüksek olduğu sektörlerden biridir. COVID-19 pandemisi bu süreci daha da hızlandırmış; özellikle çevrimiçi bankacılık hizmetleri genel bankacılık faaliyetlerinin önemli

bir bölümünü teşkil eder olmuştur. İnternet üzerinden verilen bankacılık hizmetlerine akıllı telefon uygulamalarıyla erişim hızla yaygınlaşmaktadır. Bir tahmine göre, dünya çapında bankacılık müşterilerinin yüzde 50'si, gelişmiş ülkelerde ise yüzde 70'i artık bir mobil uygulama kullanmaktadır[25].

Dijitalleşmenin hızlanması ve pandemi döneminde değişen müşteri alışkanlıkları nedeniyle şube bankacılığı gerilemektedir. Dünyada bankalar binlerce şubesini kapatmış veya kapatmayı planlamaktadır[26]. Dünya genelinde 44.000 kişi ile yapılan bir ankete göre, müşteriler bankacılık işlemlerini en çok cep telefonu uygulaması (yüzde 50), internet sitesi (yüzde 43), ATM (yüzde 29) ve telefon bankacılığı (yüzde 26) ile yapmayı tercih ettiklerini belirtmişlerdir[25]. Finans sektörü yaşamın genelindeki dijital dalgalanmada büyük rol oynamaktadır. Dünya çapında yaklaşık iki milyar tüketicinin çevrimiçi bankacılık kullandığı ve kullanımın 2024 yılına kadar en az iki buçuk milyara çıkacağı tahmin edilmektedir[27].

2.3.2 FinTech'in Yükselişi Sürecektir

Son yıllarda FinTech'ler ve yapay zekâ alanında yaşanan hızlı teknolojik gelişmeler bankacılık sektörünün hizmet sunum biçimini bambaşka bir düzeye taşımıştır. Finansal Teknoloji anlamına gelen FinTech terimi; yapay zekâ, blok zinciri, sanal gerçeklik (VR), bulut teknolojileri ve veri bilimi gibi teknolojileri geleneksel finansa entegre eden "bankacılık lisansına sahip" teknoloji şirketleri için kullanılmaktadır. Özellikle teknolojik yenilikleri benimseyen banka müşterilerinin artık herhangi bir banka şubesine ihtiyaç duymadığı gözlenmektedir. Bu nedenle İngiltere, ABD ve Çin gibi ülkelerdeki bankacılık sektörlerinde şubesiz dijital bankacılık döneminin başladığı ve bu bankaların gerek müşteri sayılarının gerekse büyüklüklerinin geleneksel bankalarla rekabet edebilecek düzeylere ulaştığı gözlenmektedir. Mart 2021 itibariyle sadece FinTech faaliyeti gösteren ve piyasa değeri bir milyar doları geçen 83 şirket olduğu belirtilmektedir[28]. Gelecekte söz konusu rakamın daha da artması beklenmektedir. 28,3 trilyon dolar potansiyele sahip olduğu tahmin edilen FinTech alanına Facebook, Apple, Google ve Amazon gibi büyük teknoloji firmalarının da yatırım yapmaya hazırlandığı ileri sürülmektedir[29]. Dünya bankacılık sektöründe bir trend hâline gelen bu yeni nesil bankacılık sistemine Türk bankacılık sektörü de kayıtsız kalmamış ve Bankacılık Düzenleme ve Denetleme Kurumunun (BDDK) Aralık 2021'de yayınladığı "Dijital Bankaların Faaliyet Esasları ile Servis Modeli Bankacılığı Hakkında Yönetmelik" ile FinTech bankacılığına izin verilmiş ve esasları belirlenmiştir[30].

2.3.3 Operasyonel Elastikiyete Odaklanmak

Küresel ekonomide sık sık ortaya çıkan belirsizlik, salgın hastalıklar, sıklığı ve şiddeti artan doğal felaketler, karmaşıklaşan rekabet ortamı, düşen müşteri güveni ve diğer nedenlerin bankacıları gelecek yıllarda, mali ve kurumsal yapılarını şoklara karşı dayanıklı kılmaya yönelteceğini tahmin etmek mümkündür. Finansal kurumlar pandemiye yanıt olarak iş yüklerini ve hacimlerini yeni kanallara, operasyonlara ve ortaklara yönlendirirken, elastikiyet sektörün en önemli önceliği haline gelmiştir. Finansal kurumların piyasa beklentilerini, düzenleyici gereklilikleri ve kurumsal etik hedefleri karşılamaya yönelik girişimleri başlatabilmeleri için uygulanabilir sürdürülebilirlik modellerinin arayışı sürmektedir[31].

2.3.4 Gelişen Dijital Varlıklar

Blok zinciri uygulamaları küresel ekonomiye kripto para ve dijital varlık kavramını armağan etmiştir[32]. Dünyada yüzlerce kripto para geliştirilmiştir ve bunların piyasa değerinin Haziran 2022 itibarıyla 1 trilyon dolar olduğu ifade edilmektedir[33].

Metaverse[34] ortamında değişim aracı olarak Non Fungible Token (Değiştirilemez Jeton/Nitelikli Fikri Tapu -NFT) kullanımı giderek artmaktadır. NFT'ler sanat eserleri, videolar, internet sayfaları, görseller, sosyal medyada oluşturulan hikâyeler ve benzeri şeyleri temsil eden dijital varlıklardır. NFT'ler, diğer kripto para birimleri gibi blok zinciri üzerinde şifrelenmiş hâlde bulunmakta ve çevrimiçi ortamda kripto paralar karşılığında satılabilmektedir. 2021 yılı sonu itibarıyla NFT pazarının 41 milyar dolar büyüklüğe ulaştığı tahmin edilmektedir[32].

Dünya genelinde kripto paralar ve dijital varlıklara duyulan ilgi merkez bankalarını da bu tür birimler geliştirmeye yöneltmiştir. Haziran 2022 itibarıyla dünyada 105 merkez bankasının dijital para birimi geliştirme çalışması bulunduğu bildirilmektedir[35]. Bunlardan 10'u dijital para birimlerini tedavüle sürmüşlerdir. Türkiye Cumhuriyet Merkez Bankası da 2021 yılında "Dijital Türk Lirası" geliştirmek üzere ASELSAN, HAVELSAN ve TÜBİTAK-BİLGEM ile mutabakata varmıştır[36]. Ancak kripto paralar ve dijital varlıkların yasal finans sistemine nasıl katılacağı henüz belirsizliğini korumaktadır. Dünya genelinde yasal ve düzenleyici çerçeveler hâlâ hazırlık aşamasındadır. Dijital varlıklar doğası gereği adem-i merkeziyetçi bir yapıda olduğu için bunların yasal çerçevesini oluşturmak oldukça güçtür ve bu amaçla ortaya konulan girişimler, dijital alana kaymış servetlerin bir anda büyük değer yitirmesi gibi ciddi bir risk getirmektedir. Öte yandan dijital varlıkların başarılı olması için, son derece karmaşık bir altyapıya gömülü güvenli bağlantıya, birlikte çalışabilirliğe ihtiyaçları vardır ve bunun varlığından söz etmek henüz mümkün değildir[31].

2.4 Kritik Altyapı Olarak Bankacılık Sektörü Riskleri

Kritik altyapı olarak finans sektörü, diğer kritik altyapılar gibi, kasıtlı (savaş, iç çatışmalar, terör saldırısı, suç amaçlı saldırılar, sabotajlar) ve kasıtsız (doğal afetler, küresel iklim değişikliği, başta elektrik olmak üzere diğer kritik altyapılardaki aksaklıklar) risklerle karşı karşıyadır. Ancak Bölüm 2.2 ve 2.3'te özetlenmeye çalışıldığı gibi, genel olarak finans sektörü ileri derecede dijitalleşmiştir ve başta bankacılık olmak üzere sektör bileşenlerinin fiziki varlıkları giderek silikleşmektedir. Finans sektörü temelde iki ana riskle karşı karşıya bulunmaktadır. Birincisi küresel, bölgesel ve bir ülkeye özgü ekonomik istikrarı bozabilecek krizlerdir. İkincisi ise dijital risklerdir.

2.4.1 Ekonomik Krizler

Yurtiçinden ya da dünyanın başka bir yerinden kaynaklanan nedenlerle finansal varlıkların değerinde ani bir düşüş, ulusal ve hatta küresel bir finansal krize neden olabilmektedir[37]. Dünya ekonomisinde çeşitli nedenlerden ötürü çok sayıda ekonomik kriz ortaya çıkmıştır. Dünya Bankası tarafından yapılan araştırmaya göre, 19'uncu yüzyılın ortalarından itibaren dünya ekonomisinin 14 kez büyük resesyona girdiği, dünya ekonomilerinin yüzde 20'lere varan oranlarda küçüldüğü görülmüştür[38]. Söz konusu krizlere dünya savaşları, petrol krizleri, pandemi, bölgesel gerginlikler ve borçlanma şokları neden olmuştur. Türkiye, cumhuriyetin ilanından günümüze kadar geçen sürede ekonomiyi ciddi şekilde sarsan pek çok krizle karşı karşıya kalmıştır. Şiddetleri değişiklik göstermekle birlikte 1958, 1978, 1994, 1998 krizlerinin ardından 2000-2001 ve 2008 ekonomik krizleri yaşanmıştır[39].

2.4.2 Siber Riskler

Finans sektörünün ikinci önemli riski dijital risklerdir. Siber saldırılar ve dijital altyapıdan kaynaklanan aksaklıklar günümüzde başta bankacılık olmak üzere tüm finans sektörünün en önemli riski niteliğindedir. KMPG'nin 135 banka CEO'su ile 2021 yılında yaptığı bir ankete göre, banka yöneticileri açısından en büyük risk siber güvenlik riskleridir. Ankete katılanlar, bankalarının dijital elastikiyetini artırmak için;

- Siber güvenlik ve diğer teknoloji risklerine karşı personelin vasıflarının geliştirilmesine odaklanacaklarını (yüzde 48),
- Güvenli ve dirençli bulut tabanlı teknoloji altyapısına yatırım yapacaklarını (yüzde 44),
- Güvenlik ve teknoloji risk yönetimini derli toplu hâle getirmek ve optimize etmek için otomasyonu benimseyeceklerini (yüzde 41),
- Yönetimi büyük bir vaka meydana geldiğinde operasyonel direnç ve toparlanma kabiliyetine sahip olacak şekilde güçlendireceklerini (yüzde 48),
- Güçlü bir dijital ve siber risk kültürü oluşturacaklarını (yüzde 41) söylemişlerdir.

Siber güvenlik ortamı sürekli değişmekte ve tehditler her zamankinden daha karmaşık hâle gelmektedir. Bilişim sistemlerini yoğun biçimde kullanmakta olan ve bunlara ileri seviyede bağımlı olan bankacılık ve finans sektöründe siber saldırının yaratabileceği zarar riski diğer sektörlerin karşı karşıya olduğundan daha yüksektir. Büyük miktarlarda para kayıpları, bankaları ve diğer finansal kuruluşlarını tehlikeye atabilir ve dolayısıyla bir bütün olarak ekonominin istikrarının bozulmasına neden olabilir.

Siber saldırganların finansal kurumlar tarafından kullanılan bilgi ve iletişim teknolojisi sistemlerini baltalama, bozma ve devre dışı bırakma yeteneği, finansal istikrar için bir tehdittir ve daha fazla dikkat gerektirmektedir. Siber suçlular, saldırılarını gerçekleştirmek için çeşitli araç ve teknikler kullanmaktadır (Tablo 1). Finans kuruluşları ile onların açıklarını durmaksızın arayan siber saldırganlar arasında her gün bir savaş yaşanmaktadır[40]. Daha fazla zarar görmek istemeyen finans kurumlarının her zaman tetikte olmaları gerekmektedir. Nitekim IBM'in "Veri İhlalinin Maliyeti 2021" Raporuna göre, finans sektöründe sadece bir veri ihlalinin ortalama maliyeti 5,72 milyon doları bulmaktadır[54]. Saldırganlar, teknolojiye geniş erişime sahip olup, bu kabiliyet onlara sınırların ötesinde faaliyet gösterme, finansal firmalara ve merkez bankalarına kâr amacıyla ya da sadece kesintiye uğratmak için saldırma olanağı tanımaktadır.

Saldırıların görülme sıklığındaki artış, artan kayıplar ve finansal sistemin işleyişinde ciddi bozulma potansiyelinin olması, siber riski tüm finansal kurumlar için merkezi bir risk yönetimi sorununa yükseltmiştir. Trend Micro'nun bir raporuna göre, yalnızca 2021'in ilk yarısında bankacılık sektöründeki fidye yazılımı saldırıları, yüzde 1.318 gibi büyük bir oranda artış göstermiştir[55]. Bu rakam diğer sektörlere göre oldukça yüksektir. ABD Merkez Bankasının New York şubesine göre bankacılık sektörü diğer sektörlere kıyasla yüzde 300 daha fazla siber saldırıya maruz kalmaktadır[56]. Saldırganlar, büyük küçük demeden her türlü finansal kuruluşu hedef almaktadır. COVID-19 krizi, ekonomik ve finansal faaliyetlerin sürekliliğini sağlamak için dijital sistemlerin ve bağlanabilirliğin korunmasının hayati önemi konusundaki farkındalığı artırmıştır.

2.4.3 Çalışanların Yarattığı Riskler

Günümüzde finans kuruluşlarına yönelik siber saldırı ve birçok siber güvenlik olayının, hâlen görevde veya yakın zamanda ayrılan çalışanlarca gerçekleştirildiğine tanık olunmaktadır. 2020'de yapılan bir araştırmaya göre, içeriden saldırılar daha yaygın, tespit edilmesi daha zor ve daha zararlı hâle gelmektedir[57]. Bir başka araştırmaya göre ise finans sektörü yüzde 16 ile içeriden gelen tehditlerde sektörler arasında lider konumdadır[58].

Finans sektörü çalışanları, kasıtlı veya kasıtsız olarak kesintilere ve kritik veri kaybına neden olabilmektedir. Örneğin, ABD'nin New York eyaletinde bir kredi kooperatifi, Eylül 2021'de işten çıkarılan bir personelin neden olduğu veri ihlaline maruz kalmıştır[59]. İşten çıkarılan çalışan, kısa süre sonra kurumsal sistemlere girmeyi başarmış ve 40 dakika içinde 21,3 GB'lık şirket verisini silmiştir.

IBM'in 2021 yılında yayınladığı Veri İhlalinin Maliyeti Raporu, kötü niyetli çalışanların yol açtığı maliyetin oldukça yüksek olduğunu göstermektedir. Rapora göre, içeriden kötü niyetli birinin neden olduğu bir ihlalin tespit edilmesi 212 gün, kontrol altına alınması ise 75 gün sürmektedir. Rapora göre kurum içi ihlaller finans sektörü açısından en maliyetli üçüncü saldırı türüdür[54].

Pandemi döneminde uzaktan çalışma, ofisten ve uzaktan çalışanları birleştiren hibrid çalışma modelleri ve bulut tabanlı yazılım teknolojileri yoğunlukla kullanılmaya başlanmıştır. İşletmeler, uzaktan erişim, iletişim ve işbirliğini mümkün kılan yeni teknolojileri hızla benimsemek zorunda kalmıştır. Sonuç olarak, yeni çalışma modelleri Bilişim Teknolojileri (BT) sistemlerinin karmaşıklığını artırmakta ve saldırılar için daha fazla açık kapı bırakmaktadır. 2021 yılı sonu ile 2022 yılı başında 11 ülkede yapılan ankete yanıt veren 1.100 BT yöneticisinin yüzde

Siber Saldırı Tekniği	Tanımı	Verdiği Zarara İlişkin Güncel Örnekler
Oltalama (Phishing)	Sahte e-posta veya kopya web sitesi kullanılarak tanınmış ve güvenilir bir kurumu taklit ederek; sistemi kullanan kişilerin adını, parolasını, banka hesap numarasını veya kredi kartı numarasını ele geçirme faaliyetidir. Rasgele hedeflere yönelik olduğu gibi hedef gözeterek (spare-phishing) de yapılabilmektedir.	2021'de dünya genelinde bankalara karşı düzenlenen siber saldırıların yüzde 46'sında ilk önce oltalama yöntemi kullanılmıştır[41]. 2019 yılında oltalama saldırıların yaklaşık yarısında finans sektörü hedef alınmıştır[42].
Kötücül Yazılım (Malware)	Bilgisayar kullanıcılarının haberi olmaksızın, kullandıkları bilgisayarlara sızmak ve bu bilgisayarlara zarar vermek amacıyla kodlanmış yazılımların genel adıdır. Solucanlar (worms), truva atı virüsler (trojan), fidye yazılımları (ransomware) ve casus yazılımları (spyware) en bilinen kötücül yazılım türleridir.	ABD'de sadece 2021 yılının ilk yarısında kayıtlara geçen fidye ödemeleri 590 milyon doları bulmuştur[43]. Aralık 2021'de ABD'nin Flagstar bankasından fidye almak isteyen saldırganların 1,5 milyon müşterinin bilgilerini ele geçirdiği ortaya çıkmıştır[44]. Ekvador'un en büyük bankası Pichincha, Ekim 2021'de fidye amaçlı olduğu tahmin edilen bir siber saldırı nedeniyle uzun süre ne şubeleri ne de ATM'lerinden hizmet verebilmiştir[45].
Hizmeti Engelleme (DoS/ DDoS) Saldırıları	Siber saldırılar ile resmi bir kuruluşun ya da şirketin bilgi iletişim ağlarını kilitlemek ve verdiği hizmeti engellemeye çalışmaktır. Günümüzde hizmeti engelleme saldırılarının büyük çoğunluğu virüslerle "zombi bilgisayar" (BOTNET) hâline getirilen birden çok bilgisayar kullanılarak gerçekleştirilmektedir.	Küresel bankacılık sektörüne yönelik DDos saldırıları 2018-2020 döneminde yüzde 200 artmıştır[46]. Aralık 2015'te Türkiye'de büyük bankaları hedef alan büyük bir DDoS saldırısı kredi kartı işlemlerini aksattı[47]. Aralarında Garanti Bankasının da bulunduğu Türkiye'nin büyük şirketlerine Ekim 2019'da düzenlenen bir DDoS saldırısı, zamanında müdahale ile atlatılmıştır[48]. Haziran 2021'de büyük bir DDoS saldırısından Almanya'daki 800'ün üzerinde kooperatif finansmanı kuruluşu etkilenmiştir[49].
İnternet Uygulamasına Saldırılar	Bankaların internet sitelerine yönelik siber saldırılardır. Kötü amaçlı yazılımlarla, bankaların internet sitelerine girişin engellenmesi, müşteri hesaplarından tasarrufların çalınması, kart bilgileriyle alışveriş yapılması ve müşteri bilgilerinin çalınarak bankadan fidye istenmesi söz konusu olabilmektedir.	2020'de dünya çapında finans şirketlerinin internet sitelerine 736 milyondan fazla internet sitesi saldırısı (bu türden saldırıların yüzde 12'si) düzenlenmiştir[46].
Gelişmiş Kalıcı Tehdit Saldırıları (Advanced Persistent Threat-APT)	Yetkisiz bir ağa erişildikten sonra, tespit edilmeden orada uzun süre kalınan saldırı çeşididir. APT saldırılarında esas amaç verilerin çalınması ya da ele geçirilmesi değildir. Buradaki asıl amaç, erişilen ağda uzun süre kalınarak bu ağa veya kuruluşa zarar vermektir. APT saldırıları, finans alanında bilhassa SWIFT işlemlerine sızma ve yüklü miktarda fonun izinin takibi zor şekilde çeşitli kanallarla saldırganlara aktarılması şeklinde tezahür etmektedir.	2021 yılının üçüncü çeyreğinde bankacılık sektörüne yönelik saldırıların yüzde 37'sini APT saldırıları oluşturmuştur (Küresel bankacılık sektörüne yönelik DDoS saldırıları 2018-2020 döneminde yüzde 200 artmıştır)[46]. Ocak 2015'te Ekvador'un Banco del Austro bankasının çalışanlarının kullanıcı adı ve parola bilgileri ele geçirilerek SWIFT transfer istekleri değiştirilmiş ve 12 milyon dolar para transferi gerçekleştirilmiştir[50]. Şubat 2016'da Bangladeş Merkez Bankasını hedef alan, Kuzey Koreli olduğu ileri sürülen saldırganlar SWIFT para transfer ağına erişerek bankayı 81 milyon dolar zarara uğratmıştır[51]. Ekim 2017'de saldırganların Tayvan'ın Far Eastern International Bank tarafından oluşturulan sahte SWIFT mesajları ile çalınan 60 milyon doların bir kısmı takip edilemezken, miktarın çoğu geri alınmıştır[52]. Aralık 2017'de Rus Bankası Globex State Bank tarafından şüpheli transferlerin tespit edilmesiyle birlikte planlanan 940.000 dolarlık soygun 100.000 doların çalınmasıyla sonuçlanmıştır[53].
Sahte İnternet Siteleri ve Mobil Uygulamaları	Banka ve diğer finans kuruluşlarının internet ve mobil uygulamalarının taklit edilip kullanıcıları kandırarak bilgilerini ele geçirmeyi amaçlayan saldırılardır.	2015'ten bu yana mobil uygulama dolandırıcılık işlemleri yüzde 600'ün üzerinde artmıştır. Dijital dolandırıcılık kayıplarının yüzde 89'u hesap ele geçirmelerden kaynaklanmaktadır[27].

Tablo 1: Küresel finans sektörünü hedef alan siber saldır türleri ve güncel örnekler.

53'ü pandemi döneminde uzaktan çalışma nedeniyle en az beş siber güvenlik ihlali ile karşılaştıklarını[60] bildirmişlerdir. Ankete katılanların yüzde 43'ü söz konusu saldırılarda bir milyon doların üzerinde zarar gördüklerini bildirmişledir.

2.4.4 Üçüncü Tarafların Yarattığı Riskler

Fidye yazılımı saldırıları genellikle kripto varlıklar biçimindeki fidye ödeme talepleriyle birleşmektedir. Saldırganlar, verileri tehlikeye atmak veya çalmak, hizmetleri kesintiye uğratmak veya fidye ödemeleri talep etmek amacıyla tedarik zincirindeki ve üçüncü taraf sağlayıcılardaki güvenlik açıklarından giderek daha fazla yararlanmaktadır.

BT hizmet sağlayıcılarına ve satıcılarına yönelik tedarik zinciri tehditleri, özel bir endişe kaynağıdır. Saldırganlar, bu hizmet sağlayıcıları ve BT satıcılarını, hizmetlerini veya yazılımlarını kullanan diğer kurumlara ulaşmak için hedef almaktadır. Tedarik zinciri saldırıları genellikle çok sayıda kurumu tehlikeye atmakta ve ardından onlardan fidye talep etmek için kullanılmaktadır. Etkilenen kurumlar bu tür saldırıları gecikmeli olarak tespit ederse veya öğrenirse, sonuçları çok büyük olabilir. Bu nedenle BT ortamlarındaki tüm yazılım ve donanımların izlenmesi ve yalnızca en kritik üçüncü taraf sağlayıcılarına odaklanılması gerekmektedir. Kritik bilgilerin hizmet sağlayıcılarla paylaşılmaması büyük önem taşımaktadır.

Çoğu finansal kurum, dijital operasyonlarını yerine getirmek için üçüncü taraf hizmet sağlayıcılarına güvenmektedir. Finans kuruluşlarının güvenlik sistemleri siber saldırılara karşı çok dirençli olsa bile, üçüncü taraf hizmet sağlayıcıları onların siber güvenlik zincirinde zayıf bir halka olabilir. Zira tehdit aktörleri, yazılım geliştiricilerini giderek daha fazla hedef almaktadır. Siber saldırganlar, finans kuruluşlarına yazılım sağlayan kuruluşların ürünlerine sızabilmektedir. Finans kuruluşları yasal ve güvenli olduğuna inandıkları yazılımları yükler veya güncellerken zararlı yazılımların güvenlik duvarlarını aşmasına da neden olmaktadır.

Son zamanların en önemli saldırılarından biri olan SolarWinds ihlali, bir tedarik zinciri saldırısı olmuştur[61]. Saldırganlar 2019 yılında ABD merkezli işletmelere yönelik bilişim hizmetleri sunan SolarWinds firmasının ağına sızmış ve yönetim yazılımına kötü amaçlı yazılım bulaştırarak bankalar ve devlet kurumları dahil binlerce şirketi hedef almıştır. SolarWinds ihlali, finansal hizmetler sektörünün siber güvenlik üzerinde çok az kontrole sahip olduğu veya hiç kontrolü olmayan üçüncü taraf tedarikçilere ve hizmet sağlayıcılara güvenmelerinin bir sonucu olarak siber saldırılara ve kesintilere karşı potansiyel savunmasızlığını ortaya koymuştur.

Dünya genelinde finans kuruluşları, geniş bir coğrafyaya yayılmış şubeleri ve birimleri arasında eşgüdümü sağlamak, bilişim maliyetlerini azaltmak ve inovasyonu hızlandırıp müşterilere yeni çözümleri daha yaygın biçimde sunmak gibi amaçlarla üçüncü taraflardan bulut bilişim hizmetleri almaktadır[62]. Üçüncü taraf BT hizmetlerine, bilhassa bulut bilişim hizmetlerine başvuran finansman kuruluşlarının sayısının 2030 yılına kadar daha da artması beklenmektedir[63]. Söz konusu üçüncü taraf BT hizmet sağlayıcıları ya daha geniş kitlelere ya da belirli iş kolları veya sektöre yönelik uzmanlaşmış hizmet vermektedir. Her türlü işletmeye hizmet verenler genellikle düşük güvenlik düzeyine ancak daha geniş bir erişim alanına sahiptir. Uzmanlaşmış hizmetler verenler ise yüksek güvenlik standartlarına sahip olmakla birlikte, bu durum genellikle belli bir ölçeğe ulaşmak isteyen işletmeler için kısıtlayıcı olmaktadır[62]. Üçüncü taraf tedarikçiler tarafından oluşturulan siber güvenlik risklerinin gelecekte daha önemli bir konu hâline gelmesi beklenmektedir.

2.5 Bankaların Siber Risklere Karşı Alabileceği Tedbirler

Finans sektörü, Bilgi ve İletişim Teknolojilerine (BİT) büyük ölçüde bağımlıdır. Bir siber saldırı, kritik işlevlerin sağlanmasını bozabilir, likiditeyi tehdit edebilir ve finansal sistemin bütünlüğünü bozabilir.

Finans sektöründe siber güvenliğin güçlendirilmesi finansal istikrar için bir önceliktir. Finans sektörü, siber tehdit aktörleri için yüksek profilli bir hedeftir ve siber riskler, potansiyel sınır ötesi yayılmalar nedeniyle ulusal ve küresel finansal sistemlerin istikrarı için bir tehlikedir. Bu nedenle siber güvenlik tedbirlerinin en üst düzeyde alınması büyük önem taşımaktadır.

Literatürde bankacılık sektörünün siber güvenliğinin sağlanması için çok sayıda öneri sunulmaktadır. Söz konusu önerileri bankacılık sektöründeki aktörlerin bireysel önlemleri olarak iki bölümde incelemek mümkündür.

2.5.1 Finans Sektörünün Geneline Yönelik Ulusal ve Uluslararası Tedbirler

Siber saldırıların büyük kısmının birden fazla kuruluşu hedef alması ve saldırıların önemli bölümünün sınır ötesi kaynaklı olması, finans sektörüne yönelik siber riskleri kurumların bireysel kabiliyetlerinin ötesine taşımaktadır. Bu nedenle ulusal ve uluslararası düzeyde birtakım düzenlemelere ve mekanizmalara ihtiyaç duyulmaktadır.

Uluslararası Para Fonunun (IMF) Para ve Sermaye Piyasaları departmanının 2019 yılında yayınladığı "Siber Güvenlik Risk Denetimi (Cybersecurity Risk Supervision)", finansal kuruluşların siber saldırılar karşısında elastikiyetinin sağlanması için bir dizi tedbir öne sürmektedir[64]. Bunlardan bazıları aşağıda özetlenmiştir:

- **Finansal İstikrar Analizi:** Siber riskin, kilit finansal ve teknolojik ara bağlantıların haritalandırılması (siber haritalama), ağ analizi ve stres testi yoluyla finansal istikrar analizine daha iyi dahil edilmesi, anlama yeteneğini geliştirecek ve böylece riski azaltacaktır. Potansiyel etkiyi ölçmek, müdahaleye odaklanmaya ve soruna daha güçlü bir bağlılığı teşvik etmeye yardımcı olacaktır. Bu alandaki çalışmalar, kısmen veri eksiklikleri nedeniyle henüz gelişme aşamasındadır. Ancak riskin artan önemini yansıtmak için hızlandırılmalıdır.
- **Düzenleme ve Denetleme:** Kamunun ve bağımsız bir kuruluşun düzenleyici ve denetleyici olarak tesis edilmesi, farklı uygulamalar arasındaki uyum ve tutarlılığı artırırken uyum maliyetlerini azaltacak ve daha güçlü sınır ötesi işbirliği ve bilgi paylaşımı için

bir platform oluşturacaktır. Uluslararası kuruluşlar, uluslararası düzeyde aktif finansal kurumlara daha fazla kesinlik sağlamak için düzenleyici ve denetleyici uygulamaların birleştirilmesine ilişkin çalışmaları koordine etmeye başlamıştır. Ulusal düzeyde düzenlemeler ise farklılıklar göstermektedir. Tutarlı düzenlemeye dayalı olarak küresel düzeyde artan denetim dikkati, sınır ötesi riskin ele alınmasına ve ortak bir soruna ortak yaklaşımların teşvik edilmesine yardımcı olacaktır.

- **Müdahale ve Kurtarma:** Siber saldırılar artık finansal ortamın kalıcı bir özelliğidir. Finansal kurumlar giderek daha fazla müdahale ve kurtarmaya, bir başka deyişle saldırıyı püskürtmeye veya sınırlamaya ve başarılı bir saldırının ardından operasyonları hızla sürdürme becerisine sahip olmaya odaklanmaktadır. Çeşitli dijital önlemlerin alınması, yazılım ve sistemlerin zamanında bakımı anlamında "siber hijyenin" sağlanması kritik önem kazanmıştır. Ancak müdahale ve kurtarma, finans sektörünün kritik önemi nedeniyle sadece finansal kuruluşlara bırakılmamalıdır. Finansal veriler için ulusal düzeyde müdahale ve kurtarma mekanizması oluşturulmalı ve hatta siber saldırıların çoğunlukla sınır ötesi olaylar olması nedeniyle, uluslararası müdahale ve kurtarma düzenlemeleri oluşturmalıdır. Bu tür mekanizmalar ulusal ve küresel finans sektörünün elastikiyetini büyük ölçüde artıracaktır.
- **Bilgi Paylaşımı:** Tehditlere, siber saldırılara, özel sektör ve kamu sektöründeki müdahalelere ilişkin bilgilerin daha fazla paylaşılması, gerekli çalışmaların çoğunu kolaylaştıracaktır. Ancak paylaşmanın önünde ciddi engeller bulunmaktadır. Ulusal güvenlik endişeleri ve veri koruma yasaları kritik bazı bilgileri paylaşma becerisini baltalamıştır. Bu kısıtlamalar dahilinde çalışan bilgi paylaşım protokolleri ve uygulamaları geliştirmek için daha fazla çaba gösterilmesi gerekmektedir. Ortak sınıflandırma kullanan bilgi paylaşımı için küresel olarak kabul edilmiş bir şablon, ortak bilgi paylaşım platformlarının artan kullanımı ve güvenilir ağların genişletilmesi, paylaşım engellerini azaltabilir.
- **Siber Saldırıları Uluslararası Seviyede Önleme:** Saldırganları engellemeye ve caydırmaya yönelik uluslararası çabaları artırmak, tehdidi kaynağında azaltacaktır. Siber suçlarla mücadeleyi güçlendirmeye yönelik bilgi paylaşımı ve soruşturma protokolleri geliştirmeye yönelik devam eden çalışmalar olumlu olmakla birlikte henüz tamamlanmamıştır. Yenilenen ve sürdürülen çabalar olmadan, gelişmekte olan ekonomiler en savunmasız durumda kalırken, finans sektörüne yönelik maliyetler ve riskler artacaktır.
- **Kapasite Geliştirme:** Gelişmekte olan piyasa ekonomilerinde kapasite geliştirme, finansal istikrarı güçlendirebilir, finansal ve teknolojik katılımı destekleyebilir. Düşük gelirli ülkeler bu tehdide karşı özellikle savunmasızdır. COVID-19 krizi, bağlantının gelişmekte olan dünyada oynadığı belirleyici rolün altını çizmiştir; teknolojiden yararlanmak, kilit bir kalkınma hedefi olmaya devam edecek ve bununla birlikte, düşük maliyetli önleme tedbirlerinin benimsenmesi de dahil olmak üzere siber riskin ele alınmasını sağlama ihtiyacı artacaktır. Gelişmekte olan ekonomilerde kapasite geliştirme bu nedenle uluslararası finans kurumları ve diğer sağlayıcılar için bir öncelik olmalıdır.

2.5.2 Finans Sektörünün Kendi İçinde Siber Güvenlik Önlemlerine İlişkin Düzenlemeler ve Öneriler

Finans sektörü dünya genelinde kritik altyapı kabul edildiği için ülke ve ülke grupları hem düzenleyici mevzuatı oluşturmakta hem de yönerge ve kılavuzlarla finans sektörünün siber güvenliğinin sağlanması için önerilerde bulunmaktadırlar. IMF[65], Dünya Bankası[66] ve Avrupa Birliğinin Siber Güvenlik Ajansı (ENİSA)[67] finansal güvenlik konusunda, yönergeler, raporlar ve tavsiyelerde bulunduğu gibi ilgili risk yönetimi programlarına da çeşitli şekillerde destek vermektedir.

Türkiye'de de bankacılık sektöründe siber güvenliğin sağlanması amacıyla yakın dönemde pek çok düzenleme yapılmıştır. En son düzenleme Bankacılık Düzenleme ve Denetleme Kurumu (BDDK) tarafından hazırlanan ve Mart 2020'de yürürlüğe giren Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmeliktir[68]. Sözkonusu yönetmelik, Kişisel Verilerin Korunması Kanunu (2016), BDDK tarafından bilişim güvenliğine ilişkin yayınlanan diğer yönetmelikler, Bilgi Teknolojileri ve İletişim Kurumunun Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı[69] ve Cumhurbaşkanlığı Dijital Dönüşüm Ofisinin Bilgi ve İletişim Güvenliği Rehberi'ne[70] uygun olarak hazırlanmıştır.

Yönetmelikte bilgi sistemlerinin yönetimi ile elektronik bankacılık hizmetlerinin sunulmasında ve bunlara ilişkin risklerin yönetiminde esas alınacak asgari usul ve esaslar ile tesis edilmesi gereken bilgi sistemleri kontrolüne ilişkin hükümler yer almaktadır.

Yönetmelikte, Bilgi Sistemlerine İlişkin Risk Yönetimi ve Kontrollerin Tesisi'ne ilişkin ayrı bir kısım bulunmakta olup; bu bölüm, bilgi sistemleri yönetişimi, bilgi güvenliği yönetimi, sistem geliştirme ve değişiklik yönetimi, bilgi sistemleri sürekliliği ve erişilebilirlik yönetimi, dış hizmet alımı ve bilgi sistemleri iç kontrol ve iç denetim faaliyetleri alt bölümlerinden oluşmaktadır. Buna göre bankalar;

- Bilgi Sistemleri (BS) strateji planı, BS Strateji Komitesi ve BS Yönlendirme Komitesi oluşturmak (Madde 4),
- Bilgi varlıklarının envanterini çıkarıp sınıflandırmak (Madde 6),
- Bilgi teknolojileri kullanmanın getirdiği risk ve tehditleri belirleyip risk analizi ve her bir riske ilişkin eylem planlarını hazırlamak (Madde 7),
- Verilerin taşındığı, iletildiği, işlendiği, saklandığı ve yedek olarak tutulduğu ortamlarda gizliliğini sağlayacak önlemleri almak (Madde 9-13),
- Gerek kendi kurumsal ağı gerekse dış ağlardan gelebilecek tehditlere karşı gerekli kontrol sistemlerini tesis etmek (Madde 14),
- Tüm kullanıcı terminallerini (masaüstü, dizüstü, mobil cihazlar ve sunucular) güvenli konfigürasyona kavuşturmak (Madde 15),

- Güvenlik açıkları ve yama yönetimi süreci tesis etmek (Madde 16),
- Kritik bilgi sistemlerini, sistem merkezleri veya ağ odaları gibi güvenli, fiziksel erişimin kontrol altında tutulduğu alanlarda barındırmak (Madde 17),
- Kurumsal Siber Olaylara Müdahale Ekibi (SOME) oluşturmak, sızma testleri düzenlemek ve istihbarat paylaşmak (Madde 18),
- Banka personeline eğitimler vererek siber güvenlik farkındalığını artırmak (Madde 19),
- Bankada geliştirilen ya da dışarıdan tedarik edilen uygulamaları gerekli güvenlik kontrollerinden geçirmek (Madde 23),
- Dışarıdan alınacak hizmetlerin doğuracağı riskleri yeterli düzeyde değerlendirmekle (Madde 29) yükümlüdür.

Yönetmeliğin yayınlanmasından bir yıl sonra yapılan bir bilimsel araştırma, Türkiye'de bankacılık sektörünün önde gelen kuruluşlarının yönetmeliğin gereklilikleri doğrultusunda yapılanma içine girdiğini, denetim mekanizmalarını faaliyete geçirdiğini, çalışanlarına siber güvenlik farkındalığı sağlamak için yoğun eğitim faaliyetleri gerçekleştirdiğini göstermiştir[71]. Bu açıdan Türkiye'de bankacılık sektöründe bilgi sistemlerinin güvenliğine ilişkin olarak ve uluslararası standartları karşılayan güncel mevzuat düzenlemelerinin yapıldığını ve bankalar tarafında da sürece hemen adapte olunduğunu söylemek mümkündür.

3. FİNANS (PARA VE SERMAYE) PİYASALARININ GÜVENLİĞİ

Bankacılık dışında finans sektörünü kritik kılan unsurlardan biri finans piyasalarıdır. Finans piyasaları, "finansal varlıkların değiştirildiği yer veya değişim mekanizması" olarak tanımlanmaktadır[72].

Finans piyasaları para ve sermaye piyasaları olmak üzere iki grupta incelenmektedir:

3.1 Para Piyasaları

Para piyasaları, bir yıl veya daha kısa süreli fon arz ve talebinin karşılaştığı piyasalardır. Para piyasasından sağlanan fonlar kredi olarak işletmenin dönen varlıklarının finansmanında kullanılmaktadır. Para piyasasının araçları hazine bonoları, ciro edilebilir mevduat sertifikası, finansman bonosu, repo ve banka bonolarıdır[72].

Türkiye'de para piyasası temel olarak üç ayrı piyasadan oluşmuştur:

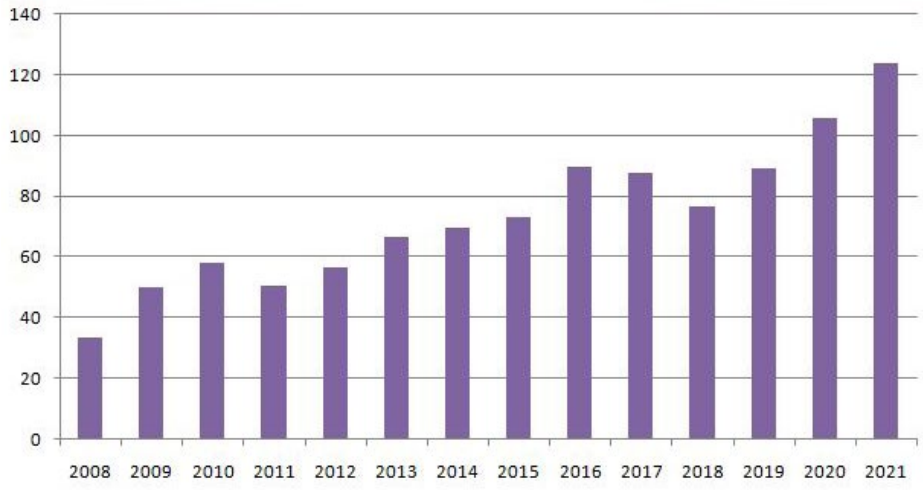
- **TCMB Bankalararası Para Piyasası:** Kısa vadeli fon arz edenlerle fon talep eden bankalar için 1986'da Türkiye Cumhuriyet Merkez Bankası (TCMB) garantörlüğünde kurulan piyasadır. TCMB 2002 yılında bu piyasada aracılık faaliyetlerine son vermiş, sadece kendisinin taraf olduğu işlemleri gerçekleştirmektedir[73].
- **Takasbank Para Piyasası:** Borsa İstanbul'da (BİST) işlem gören hisselerin büyük bölümünün fiziki olarak saklandığı ve aynı oranda paranın da el değiştirdiği Takasbank A.Ş. bankalara göre küçük olan aracı kurumların kısa vadeli finansman ihtiyacını karşılamak amacıyla bir para piyasası oluşturmuştur. Takasbank Para Piyasası, bankaların da ilgisini çekmiş ve büyük bir işlem hacmiyle çok fazla katılımcıya hizmet vermektedir[74]. Takasbank Para Piyasası işlem hacmi 2021 yılında 1 trilyon TL'ye yaklaşmıştır[75].
- **Bankalararası Para Piyasası:** Merkez Bankası veya Takasbank para piyasalarından yeterince fon bulamayan bankalar arasında karşılıklı güvene dayanarak oluşan, örgütlü olmayan bir piyasadır. Bankalar kendi aralarında, genellikle hazine bonolarını teminat olarak göstererek borçlanabilirler. Sistemin garantörü olmadığı için katılımcılar birbirinin riskini analiz ederler ve gayri resmi limitler tanırlar.

3.2 Sermaye Piyasaları

Sermaye piyasası, orta ve uzun vadeli (bir yıl ve daha uzun) fon arz ve talebinin karşılandığı piyasadır. Hisse senedi, bonolar, tahviller, gelir ortaklığı senetleri, varlığa veya ipoteğe dayalı menkul kıymetler ve ilgili türev araçlar sermaye piyasası araçlarını oluşturmaktadır[76]. Bu piyasada, tasarruflarını etkin bir şekilde değerlendirmek isteyen tasarruf sahipleri (fon arz edenler) ile bu tasarrufları en ekonomik biçimde kullanmak isteyen yatırımcılar (fon talep edenler) bulunmaktadır. Sermaye piyasası, bu iki kesimi bir araya getirerek fonların hızlı bir şekilde el değiştirmesini sağlamaktadır.

Sermaye piyasası birincil ve ikincil piyasalar olmak üzere iki piyasadan oluşmaktadır. Birincil piyasa, ilk kez dolaşıma çıkan menkul kıymetlerin işlem gördüğü, fon talebinde bulunan kesimin, fon ihtiyacını karşıladığı piyasadır. İkincil piyasa ise, daha önce alım satıma konu olan menkul kıymetlerin işlem gördüğü bir piyasadır. Sermaye piyasasının gelişebilmesi için, etkin bir ikincil piyasanın olması gerekir. İkincil piyasanın en önemli kurumu menkul kıymetler borsasıdır. Güvenilir bir ikincil piyasanın oluşması, menkul kıymetlerin likiditesini artırmakta, dolayısıyla sermaye piyasasının gelişmesine katkıda bulunmaktadır[77].

Sermaye piyasaları, sağlıklı ekonomilerin ayrılmaz unsurları hâline gelmiştir. Sağlıklı sermaye piyasalarından yararlanan müşteriler arasında sadece bireysel yatırımcılar değil, aynı zamanda kurumsal yatırımcılar, hükümetler ve şirketler de bulunmaktadır. Özsermaye ve borç yoluyla toplanan sermaye, işleri büyütmek, yeni mülk, ekipman, teknoloji yatırımlarını finanse etmek ve altyapı projelerini finanse etmek için kullanılabilir. Bu fon istihdam yaratır ve ekonomiye para akıtır. Ek olarak, bireyler ve işletmeler servet yaratmak için menkul kıymetlere yatırım yapabilir. Dolayısıyla söz konusu piyasalar, sermayenin serbest akışına ilişkin gerekli kanuni güvence sağlandığında, inovasyonun, istihdam yaratmanın, ekonomik kalkınmanın ve refahın artışında kilit rol oynamaktadır. Söz konusu nedenlerden dolayı borsalar, sermayenin tabana yayılması ve fon erişimini kolaylaştırma açısından gelişmekte olan ülkelerde sağlıklı bir mali



Şekil 4: Dünya genelinde hisseleri borsalarda işlem gören şirketlerin toplam piyasa değerindeki değişim (2008-2021, trilyon ABD doları)[75], [79].

piyasa oluşmasında önemli bir rol oynamakta ve kalkınmaya katkı sağlamaktadır[78].

Dünyada en aktif sermaye piyasaları, halka açılmaya hak kazanan kamu ve özel sektör işletmelerinin hisselerinin el değiştirdiği menkul kıymetler borsalarıdır. Menkul kıymetler borsaları, sadece ilgili ülkelerde değil, dünya genelinde siyasi ve ekonomik gelişmeleri yakından takip etmekte, bu anlamda dünya siyaseti ve ekonomisine yatırımcıların güveninin barometresi işlevini görmektedir. Bu açıdan bakıldığında yüksek riskli görünmekle birlikte menkul kıymetler borsaları büyük ilgi görmektedir. Nitekim dünyanın tüm menkul kıymetler borsalarında hisseleri işlem gören şirketlerin piyasa değeri 2008 yılında 33 trilyon dolara kadar gerilemişken[79], bu rakam 2021 yılı sonunda 124 trilyon dolara kadar çıkmıştır[75].

ABD borsalarındaki şirketler toplamda yaklaşık 52 trilyon dolarlık bir piyasa değerine sahiptir. Bu rakamın dünya borsalarının toplam piyasa değerinin yüzde 41'ine denk geldiği görülmektedir (Tablo 2). Avrupa'nın en büyüğü olan 7,3 trilyon dolar piyasa değeri ile Hollanda, Belçika, Fransa, Portekiz, Norveç ve İtalya borsalarını içeren Euronext Borsası ile Uzakdoğu bloğunda yer alan Şanghay, Japonya, Şenzhen ve Hong Kong borsaları piyasa değeri bakımından ABD borsalarının ardından gelmekte ve toplam piyasa değerinin yüzde 26'sını oluşturmaktadır.

Hisseleri Borsa İstanbul'da işlem gören şirketlerin piyasa değeri 2021 yılında 138 milyar dolar olarak belirlenmiştir. Borsa İstanbul, değer bakımından, 38'inci sırada yer almıştır. Karşılaştırma açısından, gelişmiş ülkelerdeki borsalarda işlem gören şirketlerin toplam piyasa değerinin, söz konusu ülke veya ülke gruplarının toplam GSYH'sinden fazla olduğu görülmektedir. Dünyanın 2021 yılı toplam GSYH'sinden 96 milyar dolar[80] civarında olduğu dikkate alındığında, dünya borsalarında şirketlerin

Borsaların Piyasa Değeri (2021)					
		Ülke	**Piyasa Değeri (milyar dolar)**	**Piyasa Değeri Payı**	**Piyasa Değeri / GSYH**
1	New York Borsası	ABD	27,687	%21,6	%120,7
2	Nasdaq OMX	ABD	24,557	%19,2	%107,1
3	Şanghay Borsası	Çin	8,155	%6,4	%48,4
4	Euronext (Avrupa)	Hollanda, Belçika, Fransa, Portekiz, Norveç, İtalya	7,334	%5,7	%153,4
5	Japonya Borsası	Japonya	6,544	%5,1	%128,2
6	Şenzhen Borsası	Çin	6,220	%4,9	%36,9
7	Hong Kong Borsası	Hong Kong	5,434	%4,2	%1.469,8
8	Londra Borsası	İngiltere	3,799	%3	%72,7
9	Ulusal Hindistan Borsası	Hindistan	3,548	%2,8	%120,4
10	TMX Grubu	Kanada	3,264	%2,6	%161,9
38	**Borsa İstanbul**	**Türkiye**	**138**	**%0,1**	**%17,2**
	Toplam		**124,392**	**1%00**	**%122,8**

Tablo 2: Seçili borsaların değerleri ve bu değerin ilgili GSYH'ye oranları (2021)[75].

piyasa değerinin dünya GSYH'sinin yüzde 129'u seviyesinde olduğu görülmektedir. Söz konusu oran ABD'nde yüzde 120'nin, Euronext Borsası'nda yüzde 153'ün üzerindedir. Borsa İstanbul'da ise bu oran yüzde 17,2'dir (Tablo 2). Bu durum Türkiye'de halka açık sermayeli şirket sayısının oldukça kısıtlı olmasından kaynaklanmaktadır. Dünya'da halka açık şirket sayısı 52.000 civarındadır. Hindistan ulusal borsasında 5.000'den fazla şirketin hissesi işlem görürken Türkiye'de bu sayı 380'dir[75].

3.3 Kritik Altyapı Olarak Finans Piyasalarının Karşılaştığı Riskler

Günümüzde finans piyasaları, diğer kritik altyapılar gibi karmaşıklaşmış, dünya ile eklemlenmiş ve ileri düzeyde dijitalleşmiştir. Bu nedenle diğer kritik altyapı unsurlarının karşı karşıya olduğu risk ve tehditlerle karşı karşıya kalmaktadır.

3.3.1 Savaş, Terör ve Sabotaj Riskleri

Finans piyasaları, barış ve güven ortamında sağlıklı faaliyet gösterebilmektedir. Savaşlar, iç karışıklıklar ve terör olayları söz konusu piyasaların faaliyetlerinin geçici veya kalıcı olarak durmasına, paniğe ve yüksek değer kayıplarına yol açabilmektedir. Nitekim Rusya'nın Ukrayna'yı işgali üzerine Kiev Borsası 24 Şubat 2022'de geçici olarak kapatılmış[81], aynı sıralarda Moskova Borsası'nda da işlemler durdurulmuş ve ancak bir ay sonra aşamalı olarak faaliyete geçebilmiştir[82]. Savaş durumu sadece ilgili ülkelerin mali piyasalarını değil, tüm dünyadaki mali piyasaları etkilemektedir. Rusya-Ukrayna Savaşı sırasında taraflar arasında görüşmelerin bir turunun tıkanması dahil olmak üzere tüm gelişmeler dünya mali piyasalarında dalgalanmalara yol açmıştır[83].

Finansal piyasaları olumsuz yönde etkileyen en temel unsurlar arasında belirsizlik yer almaktadır. Terörizm ve terörist faaliyetler ise, bu belirsizliği tetikleyen faktörlerdendir. Yapılan bilimsel araştırmalar terör faaliyetlerinin yarattığı huzursuzluk ve belirsizlikler ile finans piyasalarındaki dalgalanmalar arasında doğrudan bağlantı bulunduğunu göstermektedir[84]. Ancak terör olaylarının finansal piyasalar üzerindeki etkisinin derecesi ülkeden ülkeye, saldırının türüne, saldırganların hedefine ve kayıpların büyüklüğüne göre değişiklik göstermektedir[85]. Örneğin 11 Eylül terör saldırılarının ardından gelişmiş bir mali piyasaya sahip ABD'de borsalarda yaşanan kayıpların ardından, saldırı öncesi seviyeye 40 günde ulaşılırken, Norveç borsalarındaki kayıpların telafisi 104 gün sürmüştür[84].

Finansal piyasalar ileri düzeyde dijitalleşmiş piyasalar olmalarından dolayı, fiziksel sabotaj riski düşük olmakla birlikte, dijital olarak sabotaja uğrayabilmektedir. Londra Borsası 2010 yılında sistem programlarında yapılan bir sabotaj nedeniyle uzun süre işlem yapamamıştır. Yapılan soruşturmada bunun bir sabotaj olduğu sonucuna varılmıştır[86]. Borsa İstanbul dahil olmak üzere[87] dünya genelinde borsa ve aracı kuruluş çalışanlarının, yazılımları çalışmaz hâle getirmek, manipülasyona yol açacak alım satımlar gerçekleştirmek gibi sabotajları da sık sık gündeme gelmektedir.

3.3.2 Küresel İklim Değişikliği Riski

Küresel iklim değişikliği ile finansal piyasalar arasında doğrudan bir bağlantı görünmemekle birlikte[88], dünya genelinde iklim değişikliği ile mücadele konusunda artan farkındalık, hükümetleri bu alanda adımlar atmaya zorunlu kılmıştır. Bugün 120'den fazla ülke iklim değişikliğine yol açan sera gazlarının salımını azaltacak tedbirlere başvurmaktadır. Ayrıca pek çok ülke ve ülke grubu ekonomik ve sosyal alanda yeşil dönüşümü hızlandırmak için kapsamlı programlar başlatmıştır[89]. ABD, Japonya, Güney Kore ve Çin gibi ülkeler, Birleşmiş Milletlere verdikleri taahhütler uyarınca milyarlarca dolar tutarında yeşil dönüşüm programları yürütmektedir. Avrupa Birliği ise bazı tahminlere göre bir trilyon avroya mal olabilecek Avrupa Yeşil Mutabakatını (AYM) benimsemiştir. 27 üyeli birlik, birtakım yapısal zafiyetlere rağmen, gerek diplomatik gerekse ekonomik gücüyle dünyada yeni iklim rejiminin tesisinin sağlanmasına öncülük edecek potansiyele sahiptir. AB'nin üye adayı ve en önemli ticari ortaklarından biri olarak Türkiye, AYM programı çerçevesinde atılacak hemen her adımdan doğrudan etkilenecek gibi görünmektedir. Söz konusu düzenlemeler dış ticaretinin yarısına yakınını AB ile yapan Türkiye için tehdit oluşturmakla birlikte, iklim alanında harekete geçmenin aciliyeti ve bu konuda atılan adımların dünya genelinde yaygınlaştığı göz önüne alındığında yeni fırsatlara da kapı aralamaktadır[89].

Söz konusu dönüşüm programları, bazı sektörlerde üretim ve iş süreçlerini yeniden yapılandırdığı veya yeni teknolojilerin kullanımını zorunlu kıldığı için ekonomilerde derin etkiler yaratacak niteliktedir. Dolayısıyla finansal piyasalar da bu dönüşümden önemli ölçüde etkilenecektir. Ancak bu dönüşüm finansal piyasalar için sadece bir risk değil, aynı zamanda bir fırsattır. Zira yeşil dönüşüm programlarının hayata geçmesi için dünya genelinde bir trilyon doların üzerinde finansmana ihtiyaç vardır[90].

3.3.3 Riskli Yatırımcı Davranışları ve Manipülasyon

Finansal piyasalar, 2008'de ABD'den başlayarak tüm dünyada yaşanan finansal krizin gösterdiği gibi, piyasa dışı aktörlerin dışarıdan bir etki olmaksızın, kendi içinde, özellikle düşük riskli dönemlerde yaşanan yüksek riskli finansal yatırım girişimleri nedeniyle krize girebilmektedir. Bu nedenle, Bölüm 2.1 ve 2.2'de aktarıldığı üzere, tüm dünyada bu tür girişimlerin önünü kesecek yasal düzenlemeler yürürlüğe konmuş ve mekanizmalar oluşturulmuştur.

Menkul kıymetler piyasalarında bir diğer risk manipülasyondur. Manipülasyon, işlem gören hisse senetleri ile ilgili olarak bilinçli bir şekilde yönlendirmek, yanlış bir intiba vermek veya yanıltıcı bir hisse senedi piyasası oluşturmak amacıyla yapılan işlemleri[91] tanımlamaktadır. Manipülasyon, finansal piyasalar üzerinde etkisi sınırlı olmakla birlikte sıkça başvurulan bir yöntem olduğu için risk teşkil etmektedir. Örneğin Borsa İstanbul'da 2020 yılının ilk dokuz ayında tespit elden manipülasyon olayları hakkında 104 gerçek ve tüzel kişiye 80 milyon TL'den fazla para cezası kesilmiş ve buna başvuran kişiler işlem yapmaktan men edilmişlerdir[92]. Manipülasyonun sıklığı borsalara güveni törpülemektedir.

3.3.4 Siber Saldırılar

Dünya finansal piyasalarında işlemlerin neredeyse yüzde 100'e yakını dijital ortamda yapılmaktadır. Dijitalleşme, mali piyasaların temel amaç ve işlevlerinden biri olan sermayeyi tabana yaymanın en etkili yolu olmuştur. Nitekim pandemi dönemi boyunca dijitalleşme ve gelişen mobil uygulamalar sayesinde Borsa İstanbul'da işlem yapan küçük yatırımcı sayısında büyük artış olduğu ve bunların yüzde 80'inin 50 yaş altı, yüzde 26'sının ise 20-29 yaş aralığında olduğu ifade edilmektedir[93].

Dijitalleşmenin ileri seviyeye taşındığı tüm sektörlerde olduğu gibi finansal piyasalar da siber saldırı riski altında bulunmaktadır. Siber saldırganlar, veri akışlarına sızarak yanlış fiyat teklifleri ekleyebilir, güvenilir bir haber kuruluşu aracılığıyla sahte haberler yayınlayabilir veya bir hisseyi hedef alarak farklı kaynaklardan geliyormuş gibi görünen senkronize satış emri oluşturabilir. Bu da hisse senedi fiyatlarını düşürebilir ve borsaları uçuruma sürükleyebilir[94]. Finansal aracı kuruluşların, yatırımcıların belirli koşullar altında otomatik olarak alım-satım yapması için yapay zekâ algoritmalarına başvurması da riski artırmaktadır[95].

Uluslararası Menkul Kıymetler Komisyonları Örgütünün (The International Organization of Securities Commissions- IOSCO) 2014'te yayınladığı raporuna göre, siber tehditler menkul kıymetler piyasaları için potansiyel bir sistemik risk oluşturmaktadır. Araştırma, dünya borsalarının yüzde 53'ünün 2013 yılında en az bir siber saldırıya uğradığını ortaya koymuştur[96]. Sonraki yıllarda mali piyasaların güvenliğinin sağlanması için kapsamlı adımlar atılmakla birlikte saldırılar devam etmiştir. Örneğin 2021 yılında Yeni Zelanda Borsası, internet sayfasına yayılan bir DDoS saldırısı nedeniyle bir süre işlem görememiştir[97]. Ancak söz konusu saldırıların çoğunluğunun fidye gibi mali kazanç amacı taşımadığı, piyasa güvenini sarsmayı ve panik yaratmayı hedeflediği belirtilmektedir. Nitekim sadece mali piyasalara yönelik saldırıların değil, halka açık şirketlere yönelik siber saldırıların da finansal piyasalarda dalgalanma yarattığı gözlemlenmektedir[94].

4. SİGORTA SEKTÖRÜNÜN GÜVENLİĞİ

Sigorta sektörü piyasa ekonomisinin hâkim olduğu ülkelerde bankalar ve mali piyasalarla birlikte finansal sistemin en önemli üç temel aktöründen biridir.

Türk Ticaret Kanunu'nda sigorta; "bireylerin değeri para ile ölçülebilir kıymet, menfaat veya emtialarını zarara uğratan tehlike ve kayıpların meydana gelmesi hâlinde, bu zararların telafi edilebilmesi amacıyla, karşılıklı olarak kararlaştırılan koşullar ve limitler doğrultusunda, sigortacı tarafından sigorta ettirene tazminat ödenmesini öngören bir yazılı akit" olarak tanımlanmıştır (Türk Ticaret Kanunu, Madde 1263)[98].

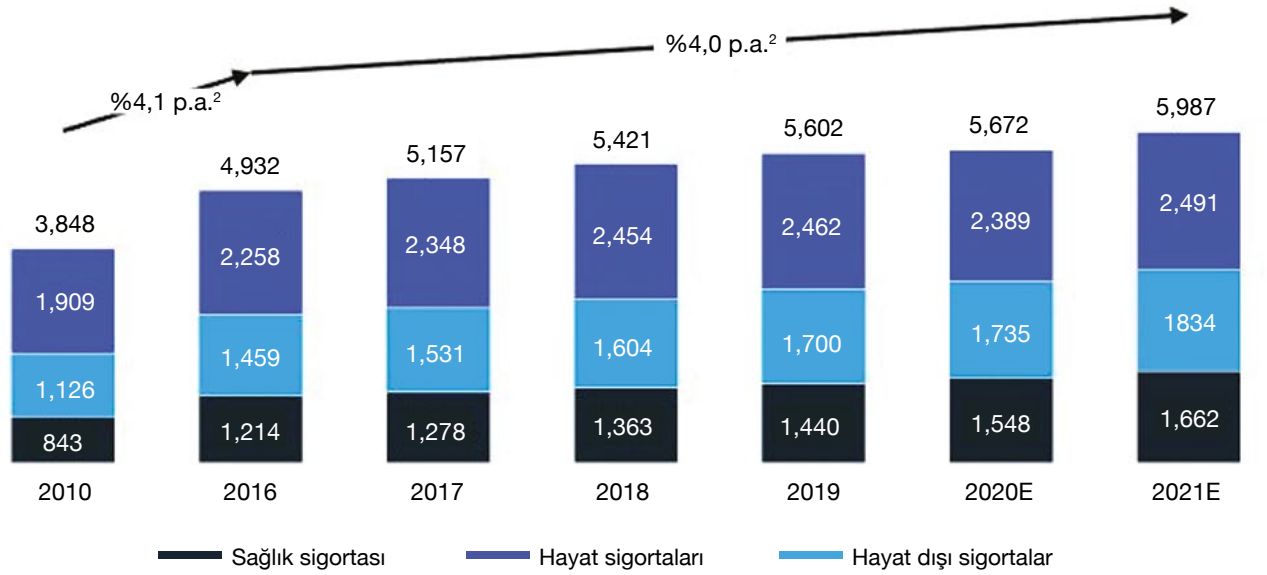
Sigorta, sosyal, ekonomik ve siyasi alanlarla birlikte altyapısı sağlam, istikrarı sağlamış olan gelişmiş ülkelerde özellikle ekonomik faaliyetlerin yürütülmesinde hiç şüphesiz büyük öneme sahiptir.

Sigortacılık; topluma ve ekonomiye, ekonomik kalkınma ve ekonomik büyümeye katkıda bulunmak, firmaların finansal açıdan sağlam yapıda olmalarını, asıl işlevlerine yoğunlaşmalarını sağlamak ve önemli bir risk transfer aracı olmak gibi çeşitli yararlar sağlamaktadır[99].

Kritik altyapı olarak sigorta sektörü toplumsal risklerin azaltılmasında önemli rol oynamaktadır. Sigorta sosyo-ekonomik çöküntüleri önler veya azaltır. Sigortalanmamış riskler gerçekleştiklerinde bireyleri, aileleri ve işletmeleri sarsar, zor duruma düşürür. Bu zor durumlardan kaynaklanan sıkıntılar yayılarak başkalarını da etkiler. Bunların toplam etkisi büyük toplumsal çöküşlerdir. Sigorta bu tür çöküşleri ya tamamen önler veya etkilerini azaltır[100]. Bu açıdan sigorta sisteminin sağlık ve istikrarının korunması büyük önem taşımaktadır.

4.1 Dünyada Sigorta Sektörünün Durumu ve Gelecek Öngörüleri

Dünyada sigortacılık faaliyetleri yaklaşık 5.000 yıl önce uluslararası ticaretin ortaya çıktığı günden bu yana



Şekil 5: Küresel sigortacılık sektörünün prim gelirleri (2010-2021)[104].

yapılmaktadır. Modern anlamda sigorta şirketlerinin ortaya çıkışı ise 17'nci yüzyılın başına kadar gitmektedir. Sigortacılık bugün dünyada en yaygın işkollarından biridir ve 2022 yılı sonu itibarıyla 7 trilyon dolar büyüklüğe ulaşması beklenmektedir[101]. Dünyanın en büyük 2.000 şirketinden 105'i sigorta sektöründe faaliyet göstermektedir[102]. Ana şirketleri ve acenteleri ile birlikte milyonlarca kişiye istihdam sağlayan sigorta şirketleri, tüm ekonomik faaliyetlerin yanındadır. Modern hayatın tüm risklerine çözümler üretebilen sigorta sektörü kalkınma, inovasyon ve girişimciliğin en büyük güvencelerinden biri olmuştur. Ancak sigortacılık sektöründe gelişmiş ve gelişmekte olan ülkeler arasında ciddi bir fark bulunmaktadır. Gelişmekte olan ülkelerde "sigorta penetrasyonu", yani sigorta primlerinin toplamının ülkenin GSYH'sine oranı yüzde 20'leri bulurken, bu oran gelişmekte olan ülkelerde yüzde 5'in altındadır. Dünya ortalaması ise yüzde 7 civarındadır[103].

Ülke	Pazar payı
ABD	%39,1
Çin	%9,8
Japonya	%7,3
Birleşik Krallık	%5,8
Fransa	%4,2
Almanya	%3,9
Güney Kore	%2,8
İtalya	%2,7
Kanada	%2,1
Tayvan	%1,9
Türkiye	%0,2

Tablo 3: Seçilmiş bazı ülkelerin küresel sigorta pazarındaki payları[101].

Dünya genelinde sigortacılık, hayat sigortası ve hayat dışı sigortalar (mal ve sorumluk sigortaları) olarak iki branşta ele alınmaktadır. Hayat sigortaları, insan hayatına ve sağlığına yönelik tehdit oluşturan rizikoları teminat altına alan genellikle uzun vadeli sigortalardır. Hayat dışı sigortalar ise bireylerin sigortalanabilir emtia, kıymet ve menfaatlerini poliçede belirtilen çeşitli rizikolara karşı güvence altına almakta; yangın, doğal afetler, kaza, mühendislik, tarım ve nakliyat sigortaları başlıkları altında çeşitlere ayrılmaktadır.

Dünyada prim üretimi 2021 yılında bir önceki yıla kıyasla yüzde 3,4 artışla 6,9 trilyon dolar olarak gerçekleşmiş; bunun 3 trilyon doları hayat, 3,9 trilyon doları ise hayat dışı branşlarda gerçekleşmiştir. 2021 yılı prim üretimi hayat branşında yüzde 4,5 oranında, hayat dışı branşlarda ise yüzde 2,6 oranında yükselmiştir[105].

Sigortacılık, dönemsel olarak toplumda risk algılarının ve teknolojilerin değişmesinden etkilenmektedir. Örneğin COVID-19 pandemisi, dünya genelinde hayat sigortaları primlerinde 2020-2022 arasında ortalama yüzde 3,8'lik artış yaşanmasının en önemli nedeni olarak görülmektedir[101], [106]. Küresel iklim değişikliğinin şiddetini artırdığı doğal felaketler nedeniyle 2020 yılında sigorta şirketlerinin hasar ödemeleri, tarihin en yüksek seviyesine çıkmıştır[107]. Bu eğilimin gelecek 20 yılda da devam etmesi ve doğal felaketlere karşı yaptırılan sigortalara ödenen primlerin 2040 yılına kadar yüzde 40 artışla 183 milyar dolara ulaşması beklenmektedir[108]. Buna karşılık teknolojik değişimler bazı alanlarda sigorta talebinde düşüşe neden olabilir. Örneğin ulaşım araçlarının daha akıllı ve güvenli olmasıyla 2030 yılına kadar motorlu araç sigortalarının hayat dışı sigortalar alanındaki payının yüzde 43'ten yüzde 34'e düşmesi beklenmektedir[108].

Yakın gelecekte sigorta sektöründe sadece teknoloji ve risk algılarında değil, iş süreçlerinin de kapsamlı şekilde değişmesi beklenmektedir:

- **Dijitalleşme ve yalınlaşma:** Küresel sigorta sektörü son yıllarda teknolojiye önemli ölçüde yatırım yapmıştır. Bir araştırmaya göre, küresel sigorta şirketleri dijitalleşme yatırımlarını 2021 yılında yüzde 59 artırmıştır[109]. Dijitalleşme sigortacılık sektörünün, müşterilerine ulaşmasını kolaylaştıran yeni dağıtım kanallarının ortaya çıkmasına neden olurken, var olan kanalların gelişiminde de rol oynamaktadır. Dijitalleşme; aynı zamanda müşteriler açısından bilinirliğin artmasında ve müşterilerin bilinçli tercihler yapmalarında fayda sağlamaktadır. Uzun yıllar boyunca yasal düzenlemeler nedeniyle önemli bir bölümü ağır bürokratik yük altında olan sigorta sektörü, dijitalleşme ile yalınlaşmaya ağırlık vermiştir.

  Sigorta şirketleri, yapay zekâ uygulamaları ile daha isabetli risk analizleri yapabilmektedir. Blok zincir uygulamaları daha hızlı ödeme sistemleri sağlarken dolandırıcılık ve kara para aklama olaylarıyla mücadelede etkin rol oynamaktadır. Bazı sigorta şirketleri kripto paralarla ödeme almaya başlamıştır[110].
- **Insurtech:** Bankacılık alanında FinTech eğilimi sigortacılık sektörüne aksetmektedir. Son dönemde sigortacılık alanında faaliyet iznine sahip ancak sadece dijital ortamda hizmet veren "Insurtech" start-up'ları ortaya çıkmıştır. İngilizce "Insurance" (Sigorta) ve "Technology" kelimelerinin birleşimi olan "Insurtech" henüz küresel sigortacılık sektöründe küçük bir paya sahiptir. 2021 sonunda küresel sigortacılık sektörünün büyüklüğü 7 trilyon dolara dayanmışken, insurtech firmaları 3,85 milyar dolar büyüklüğe ulaşabilmiştir[109]. Buna karşılık bu yeni sektör 2021 yılında 14,6 milyar dolar yatırım çekmiştir[104]. Sektörün gelecek 10 yılda hızla pazar payını artırması, 2030 yılına kadar ortalama yüzde 51,7 büyüme kaydetmesi beklenmektedir[109].
- **Talebe Dayalı (on-Demand) Sigortacılık:** Sigorta şirketleri nesnelerin interneti, yapay zekâ, büyük veri ile öngörüsel bakım gibi teknolojiler sayesinde, müşterilerine çevrimiçi olarak talep ettikleri teminatlara göre poliçeler hazırlayabilmektedir[111]. ABD'de Trov, Cuvva ve Slice gibi Insurtech firmaları, müşterilerin ihtiyaç duyduklarında kişisel eşya sigortası, ev ve seyahat sigortası ve araba sigortası satın almak için bir mobil uygulama kullanmalarına olanak tanımaktadır. Müşteriler, yalnızca varlık gerçekten kullanımda ve "risk altında" olduğunda prim ödemesi yapmaktadır. Talebe dayalı sigortanın bir türü yıllardır var olsa da, isteğe bağlı sigorta hâlâ küresel sigorta pazarının yalnızca yüzde 1'ini temsil etmektedir[111]. Ancak bu tür sigorta hizmetlerinin 2025 yılına kadar hızla büyüyeceği tahmin edilmektedir[112].

Gerek Insurtech firmaları gerekse talebe dayalı sigortalar, geleneksel olarak acente ağırlıklı olan sigortacılık sektöründe yapısal bir değişikliğe doğru gidildiğinin işaretini vermektedir. Bu durum yüz binlerce kişiye istihdam sağlayan sektörde bir daralmayı beraberinde getirebilir.

4.2 Türkiye'de Sigorta Sektörünün Durumu ve Gelecek Öngörüleri

Türkiye'de 2021 yılı sonunda 65 sigorta, reasürans ve emeklilik şirketi faaliyet göstermekte ve acenteleri ile birlikte 200 binden fazla kişiye istihdam sağlamaktadır. Sektörün aktif büyüklüğü 429,2 milyon TL'ye ulaşmıştır[105]. Sigorta potansiyelinin yüksek olması nedeniyle Türk sigortacılık piyasası uluslararası yatırımcıların ilgisini çekmeye devam etmektedir. Tarihsel olarak sigortacılık sektörü yabancı şirketlerin faaliyetleriyle gelişen Türkiye'de, günümüzde sigorta şirketlerinin üçte ikisi yabancı sermayelidir. Ülkemizde uluslararası sermayeye sahip şirket sayısı 2021 sonu itibarıyla 41'dir.

Türkiye'deki sigortacılık sektörü, son yıllarda pandemi koşullarından sınırlı şekilde etkilenmiş, Türk lirası cinsinden prim üretimini artırmayı sürdürmüştür. 2021 yılında hayat dışı sigorta branşlarında 87,6 milyar TL, hayat grubu sigorta dallarında ise 17,8 milyar TL olmak üzere toplam 105,4 milyar TL prim üretimi gerçekleştirilmiştir. Buna karşılık 233,6 trilyon TL teminata imza atılmış, gerçekleşen teminat ise 63,6 milyon TL olarak gerçekleşmiştir. Toplam prim üretimi 2020 yılına göre yüzde 28 oranında artmıştır[105].

Türkiye'de sigortacılık sektörü dinamiktir ve hızla büyümektedir. Ancak dünya ile karşılaştığında Türkiye'de sigorta pazarının son derece sınırlı olduğu görülmektedir. Tablo 3'te de görüleceği üzere Türkiye sigorta sektörünün küresel pazardaki payı binde iki seviyesindedir. Bu durum için çeşitli nedenler ileri sürülmektedir. Nedenlerden bazıları şunlardır[113]:

- Toplumda sigorta bilinci ve kültürünün tam olarak yerleşmemesi,
- Türkiye'de gelir seviyesi ve alım gücünün gelişmiş ülkelere kıyasla düşük olması,
- Sigorta şirketlerindeki yetersizlikler ve pazarlama sorunları,
- Sektörde yoğun rekabet ve düşük kârlılık.

Türkiye'de sigortacılık sektöründe dijitalleşmenin pazarın büyümesine etkisi de sınırlı kalmıştır. Ülkemizde sigorta şirketleri çevrimiçi hizmetler vermekte, cep telefonu uygulamalarıyla müşterilerinin hasar tazmin taleplerine en kısa sürede yanıt vermeye çalışmaktadır. Ancak Insurtech ve talebe dayalı sigortacılık örnekleri çok sınırlıdır.

Hayat branşında e-ticaret satışlarının toplam satış içindeki payı son beş yılda, yıllık yüzde 0,7'den yüzde 12,1'e ulaşmıştır[114]. Bu artışın en önemli nedenlerinden biri hayat branşının dağıtım kanalı yapısıdır. 2020 yılında hayat sigortalarının yüzde 84'ü bankalar aracılığıyla satılmıştır. Geleneksel acentelerle kıyaslandıklarında çok daha ileri teknolojik imkânlara sahip olan bankalar, hayat sigortalarının önemli bir kısmını kendilerinin sağladığı kredilere istinaden satmaktadır[114].

Türkiye'de hayat dışı sigorta satışlarında acentelerin payı yüzde 57 gibi çok yüksek orandadır. Bunda acentelerin müşterileri için kolay erişilebilir olmaları ve müşterilerine danışmanlık hizmeti vermelerinin etkisi büyüktür. Dolayısıyla Türkiye sigortacılık sektöründe

GÜÇLÜ YÖNLER	ZAYIF YÖNLER
• Devletin bireysel emeklilik sistemi, tarım ve doğal afet sigortaları gibi stratejik alanlardaki desteği, • Sektörün sermayedar yapısını banka ve yabancı yatırımcıların oluşturması sayesinde kurumsal yapının sağlamlığı, • Çalışan genç nüfus oranının yüksekliği, • Türkiye'nin uzun vadeli yüksek büyüme potansiyeli.	• Sigorta kavramının önündeki geleneksellik temeline dayanan sosyokültürel engeller, • Sigorta şirketlerinin sundukları hizmetlerdeki derinliğin yeterince tanıtılamaması, • Satış kanallarının görece etkisizliği.
FIRSATLAR	**TEHDİTLER**
• Düşük penetrasyon oranları, • Dijitalleşmenin yaratacağı verimlilik artışları, • Artan risk bilinci, • Kredi, alacak ve kefaret sigortası sisteminin yarattığı farkındalık.	• Kârlılığa etki eden çetin rekabet koşulları, • Makroekonomik görünüm, • Başta inşaat olmak üzere ana sektörlerdeki talep daralması, • Salgın hastalık ve pandemi riski, • Jeopolitik riskler, • Büyük doğal felaket riskleri.

Tablo 4: Türkiye'de sigortacılık sektörünün SWOT analizi[103].

dijitalleşmenin dünyadaki genel gelişimin gerisinde olduğunu ileri sürmek mümkündür.

Türkiye'de sigortacılık sektörünün güçlü ve zayıf yönlerini Tablo 4'te olduğu gibi özetlemek mümkündür:

4.3 Sigorta Sektörüne Yönelik Riskler ve Tehditler

Belirsizlerin hâkim olduğu bir dönemde güvence arayanların başvurduğu sigorta sektörü, diğer altyapılar gibi çeşitli risklerle karşı karşıyadır.

4.3.1 Siber Güvenlik Riskleri

Küresel sigortacılık sektörünün risk algısına ilişkin yapılan araştırmalar, siber güvenliğin sektördeki en çok kaygılandıran konu hâline geldiğini göstermektedir[115].

Sigorta sektörü, birçok siber saldırı türü için yoğun bir şekilde hedef olmaktadır. Bu tehditler arasında poliçe sahibi verilerinin ele geçirilmesi ve satışı, COVID-19 ile ilgili açıklardan yararlanma, yabancı devlet destekli saldırılar ve fidye yazılımları ön sıralarda yer almaktadır[116]. ABD'de bir sigorta firmasının siber saldırıda bulunan Rusya kökenli bir hacker grubuna 40 milyon dolar fidye ödemek zorunda kaldığı ileri sürülmüştür[117].

Şirketlerin genişleyen tedarik zincirlerine yeni teknolojileri, bulut bilişimi ve üçüncü parti hizmetleri dahil etmesiyle birlikte sigorta sektörü için zorluklar eskisinden çok daha karmaşık hâle gelmiştir. Şirketler teknolojiye erişimlerini, özellikle de uzaktan teknoloji kullanımlarını artırarak siber riske daha fazla maruz kalmaktadır. Pandemiden sonra uzaktan çalışmanın yaygınlaşması ve kişisel cihazların iş için kullanılması kurumsal ağları saldırılara açık hâle getirmiştir. Örneğin, 2021 yılında ABD'de sigorta şirketlerine yönelik siber saldırılar, 2020'ye kıyasla yüzde 50 artmış, haftada ortalama 925 saldırı gerçekleşmiştir. Bunların büyük çoğunluğunu da oltalama saldırıları ve ardından gelen fidye talepleri oluşturmuştur. Sigorta şirketlerinden talep edilen fidye miktarı ise 2021 yılında bir önceki yıla kıyasla yüzde 900 artmıştır[118].

Öte yandan tüm sektörlerde artan siber güvenlik endişesi, sigorta şirketlerinin prim üretimini de artırmaktadır. Munich RE tarafından yapılan bir araştırmaya göre, 2022 yılı başı itibarıyla küresel sigortacılık sektörü, siber suçlara karşı sağladığı güvencelerden 9,2 milyar dolar prim elde etmiştir ve bu miktarın 2025 yılına kadar 22 milyar dolara yükselmesi beklenmektedir[119].

4.3.2 Savaşlar, Terör ve Siyasi Riskler

Savaşlar ve iç karışıklıklar, yarattıkları doğrudan zararların yanı sıra yurtiçi ve yurtdışı ticaretteki aksamalarla sigorta sektörüne büyük darbe vurmaktadır. Sigorta yaptıranlar, söz konusu riskler ortaya çıktığında can kayıpları ve yaralanmalar; taşıma araçları, üretim ve hizmet merkezlerinin gördüğü maddi zararlar; tedarik zincirlerinin kesintiye uğramasının yol açtığı üretim aksamaları; ulaşımda aksamalar, ticaret kaybı ve diğer nedenlerle sigorta şirketlerine tazminat taleplerinde bulunmaktadır. Neredeyse eşzamanlı yapılan bu başvurular sigorta şirketlerini mali olarak güç durumda bırakabilmektedir. Nitekim Rusya-Ukrayna Savaşı nedeniyle sigorta şirketlerinin 16-35 milyar dolar zarara uğrayacağı tahmin

edilmektedir[120]. Sadece havacılık şirketlerinin savaştan dolayı yaşadığı operasyonel kayıplardan ötürü sigorta şirketlerinden tazminat taleplerinin 4 milyar doları bulabileceği belirtilmektedir[121].

Terör ve sabotaj, ABD'deki 11 Eylül 2011 terör saldırılarının ardından pek çok ülkede sigortacılık sektörünün teminat sunduğu bir alan hâline gelmiştir. Sigorta şirketleri terör saldırıları nedeniyle zarar görenlere çeşitli teminatlar sunmaktadır. Terör de savaş gibi doğrudan veya dolaylı sigorta maliyetleri yaratmaktadır. Dönem dönem ortaya çıkan ve çoğu zaman öngörülmeyen karışıklıklar, sigorta sektörüne mali yük getirmektedir. Ayrıca devletlerin, terörün finansmanının önüne geçilmesi (kara para aklama, uluslararası terör finansmanı) için aldığı önlemler sigortacıların iş yükünü artırmaktadır. Türkiye'de 2021 yılında yayınlanan "Aklama, Terörizmin ve Kitle İmha Silahlarının Finansmanı İle Mücadelede Sigorta ve Bireysel Emeklilik Sektör Rehberi"nde[122] sıralandığı üzere sigorta şirketleri, sigorta yaptıranlarının terörle bağlantılı kişiler olmadığını belirleme konusunda son derece titiz bir çalışma yürütmek zorundadır.

Protestolar, ayaklanmalar, genel grevler, yağma, vandalizm gibi toplumsal olaylar, sigorta sektörü üzerinde giderek daha fazla baskı oluşturmaktadır. Son yıllarda, Fransa'da "Sarı Yelekliler" protestoları yaklaşık 225 milyon avro[123], Şili'deki yağma ve vandalizm olayları yaklaşık üç milyar dolar[124], Hong Kong protestoları yaklaşık iki milyar dolar[125], Bolivya protestoları 100 milyon dolar[126] ve Ekvador'daki eylemler 110 milyon dolar[127] hasara yol açmıştır. Bu rakama ofis, mağaza ve dükkânların açılamamasının yol açtığı iş kayıpları dahil değildir. ABD'de 2020 yılında George Floyd'un ölümünün ardından 20 eyalet ve 40 şehirde yaşanan olaylar iki milyar dolar zarara neden olmuştur[128]. Daha yakın tarihte, Temmuz 2022'de Sri Lanka'da patlak veren olaylar iki milyon dolardan fazla zarara yol açmıştır[129]. Dünya ekonomisi daha pandeminin etkisinden kurtulamamışken patlak veren Rusya-Ukrayna Savaşı, beraberinde getirdiği enerji ve gıda güvenliği krizleriyle, dünya genelinde onlarca ülkede Sri Lanka'da olduğu gibi toplumsal olaylara neden olabileceği kaygısını artırmıştır[130].

Doğal felaketlerde olduğu gibi savaş, terör ve siyasi risklerdeki artış sigortacıların bir bölümünü, bu tür riskleri çoğu üründe teminat dışında bırakmaya yöneltmektedir ve bu dünya genelinde bir tartışma konusudur. Toplumsal yararlarından ötürü sigorta şirketlerinin bu tür riskleri teminat kapsamında tutan modeller geliştirmesi gerektiği ifade edilmektedir[131].

4.3.3 İklim Değişikliği ve Doğal Afet Riskleri

Her yıl dünya çapında, doğal afetler milyarlarca dolara ulaşan varlıkları yok etmektedir. Ancak çoğu zaman, bu hasarın sadece küçük bir kısmı sigortalıdır. Munich RE'ye göre 2021 yılında seller, tayfunlar, toprak kaymaları, depremler, orman yangınları ve aşırı kuraklık gibi doğal afetler yaklaşık 280 milyar dolar zarara yol açmış, ancak bunun yüzde 60'ından fazlası sigorta edilmemiştir. Son yıllarda sanayileşmiş ülkelerde doğal afetlere karşı sigorta açığı azalırken, gelişmekte olan ülkelerde hâlâ önemli bir uçurum bulunmaktadır. Bir felaketten etkilenen bireylerin ve şirketlerin, ne olursa olsun devam etmek zorunda kaldıkları ve kendi ülkelerinden veya yurtdışından gelen bağışlara güvenmek zorunda kaldıkları sıklıkla görülen bir durumdur.

İklim değişikliği bağlantılı felaketlerin sıklığının ve şiddetinin artması özellikle mal ve kaza sigortalarında önemli ölçüde artışa neden olmaktadır. Bugün, mal ve kaza sigortalarında teminat miktarı yaklaşık 1,8 trilyon dolardır. 2040'a kadar bu, iki katından fazla artarak 4,3 trilyon dolara ulaşacaktır[108]. Bu son derece yüksek risk düzeyini azaltmak, yeni bir yaklaşım gerektirecektir. Bu yaklaşımın odağında ise risk azaltma ve adaptasyon hedefi yer alacaktır. Sigortacılar doğal felaket risklerini iyi analiz edebilmek için daha yeni teknolojilerden yararlanmak ve devletlerle işbirliği yoluna gitmek zorunda kalacaklardır.

5. FİNANS SEKTÖRÜ İÇİN SİBER GÜVENLİK ÖNERİLERİ

Türk savunma sanayiinin önde gelen kuruluşlarından STM'nin teknoloji odaklı düşünce merkezi STM ThinkTech'in 3 Kasım 2021'de düzenlediği "Bütünleşik Güvenlik Bağlamında Siber" başlıklı odak toplantısına[132] katılan Yapı Kredi Teknoloji Bilgi Sistemleri Güvenlik Yönetimi Genel Müdür Yardımcısı Ahmet Gökhan Yalçın, finans sektöründe en önemli tehdidin siber saldırılar olduğuna dikkat çekmiştir. Siber saldırıların etkisinin artık dijital ortamda kalmadığını ve hayatın her alanını etkileyip, can ve mal kayıplarına yol açtığını belirten Ahmet Gökhan Yalçın, güç birliği yapıldığı takdirde siber saldırıların önüne geçmenin mümkün olduğunu savunmuştur. Yalçın'ın altını çizdiği önlemler ve yaklaşımlardan bazıları şunlardır:

5.1 Ön İstihbarat Mümkündür

Siber saldırgan grupları daha önceki saldırılarda işe yaramış teknik ve araçları tekrar kullanma eğilimindedir. Dolayısıyla daha önce yaşanmış vakalar, belirli saldırı araçları ya da saldırı göstergeleri incelenerek bir saldırının hangi gruplardan ya da hangi ülkeden geldiği tahmin edilebilir. Bütün bu açık kaynak kodlu istihbarat verisinden faydalanarak, geçmiş vakalar da taranarak hâlihazırda güncel olan vakaların kimler tarafından yapıldığı kısmen eşleştirilebilir.

5.2 Finans Sektörü Siber Saldırı Önleme Kurulu Oluşturmalı

Yurtdışı kaynaklı saldırılarda Türkiye'de faaliyet gösteren bankaların birkaçı birden hedef alınmaktadır. Bir finans kuruluşu saldırıyı savuştursa bile diğer finans kurumlarıyla istihbarat paylaşabileceği bir platform olmadığı için diğerleri saldırıdan olumsuz etkilenebilmektedir.

5.3 Aktif Veri Merkezlerinin İşlerliği Sağlanmalı

Siber olaylar sadece siber saldırılardan ibaret değildir. Sistem sorunları veya kurum içi kullanıcıların hataları

siber olayların önemli bir bölümünü teşkil etmektedir. Bu nedenle özellikle finans kuruluşlarının Olağanüstü Durum Merkezleri (ODM) kurmaları ve bunların gerektiği gibi çalıştığından emin olmaları büyük önem taşımaktadır. Ancak bunlar yüksek maliyetli yatırımlardır. Bu nedenle ODM'lerin test merkezlerinin ötesine geçip aktif veri merkezleri olarak işlerlik kazanması gereklidir.

5.4 Ulusal Çapta Bilgi Güvenliği Farkındalığı Sağlanmalı

Finans sektörü özellikle yoğun oltalama saldırıları altındadır. Bir çalışanın bir linke tıklaması bütün sistemi çökertebilir. Sadece çalışanların değil, tüm ulusun siber güvenlik farkındalığının artırılması için girişimde bulunulmalıdır.

5.5 Doğru Veri Yönetişim Stratejisi Oluşturulmalı

Türkiye'de finans sektörü katı düzenlemelere tabidir. 2020 yılında yayınlanan Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Yönetmeliği ve 2016 tarihli Kişisel Verilerin Korunması Kanunu nedeniyle veri güvenliği çok önemli bir noktaya gelmiştir. Veri ve veri güvenliği ihlallerinde artık maddi cezalar dahil olmak üzere çok ciddi yaptırımlar söz konusudur. Artık veri güvenliği siber güvenlik ile aynı anlama gelmektedir. Farklı tipte verileri farklı şekilde korumak gereklidir. Bir kurumun doğru bir veri yönetişim stratejisi yoksa üstüne bir veri güvenliği programı inşa etmek mümkün değildir. Önce veri analizi ve sınıflandırılması yapılmalı, sonra bu sınıfların gerekliliklerine uygun olarak farklı güvenlik aksiyonları alınmalıdır.

5.6 Kurum İçi Suistimaller ve Veri Çıkışı Kontrol Altına Alınmalı

Finans kuruluşları dışarıdan gelecek saldırılara önem verdiği kadar kurum içi suistimalleri yakından takip etmelidir. Veri güvenliğinde çalışanların, yetkisi dışındaki verilere erişimi ve aynı zamanda yetkisi dahilinde anormal erişim yapmaları engellenmelidir. Yetki dahilindeki hareketlerde anomali tespiti için izleme ve alarm sistemi kurulmalıdır. Kurum içinde bu tip anormal davranışlar yapan kişiler hakkında kınamadan işten çıkarmaya kadar tedbirler uygulanabilir.

Kurum dışına çıkan veri konusu da kritiktir. Gerçekten hassas verilerin kurum dışına çıkmaması, çıkıyorsa da son derece sınırlı olması sağlanmalı ve kontrol edilmelidir. Bu kontroller arasında veri sızıntısı önleme kontrolleri, Veri Kaybı Önleme (Data Loss Prevention -DLP) kontrolleri ve etiketleme, e-postaların etiketlenmesi, ofis dokümanlarının etiketlenmesi, hem sistem kurallarıyla otomatik olarak hem de kullanıcının kararına bırakılarak etiketlenmesi gibi uygulamalara başvurulabilir.

5.7 Üçüncü Taraflarla Veri Paylaşımı Denetlenmelidir

FinTech ve Insurtech hızla yaygınlaşmaktadır. Söz konusu üçüncü taraf firmaların devreye girmesi riskleri daha da artacaktır. Bu artış günümüzde en kritik konular arasında yer almaktadır. Üçüncü taraflarla entegrasyonlarda ne tip veriler paylaşıldığına ve bunlar için ne gibi önlemler alındığına dikkat edilmelidir.

6. SONUÇ

Dünyada ve Türkiye'de kritik altyapıların mevcut durumunu ve temel eğilimlerini aktarmak; kritik altyapılara yönelik tehditleri irdelemek ve bunları bertaraf etmek maksadıyla geliştirilen çözüm önerilerini sunmak için başlattığımız Araştırma Raporu yazı dizimizin son bölümünü de tamamlamış bulunmaktayız.

Yazı dizimizde enerji, ulaştırma, haberleşme, bilişim ve finans alanlarındaki kritik altyapıların önemine, bu tür altyapıların gelecekte hangi yöne evrileceğine, hangi risk ve tehditlerle karşı karşıya olunduğuna ve söz konusu risklerin bertaraf edilebilmesi için alınan tedbirlere göz atılmış, öneriler irdelenmiştir.

Vatandaşların yaşam kalitesi ve güvenliklerinin yanı sıra iç pazarın doğru ve verimli işleyişi, çok çeşitli sektörlerde farklı kritik altyapılar aracılığıyla temel hizmetlerin sağlanmasına bağlıdır. Bu nedenle, kritik altyapıların hem doğal hem de insan kaynaklı, kasıtsız ve kötü niyetli geniş bir tehdit yelpazesine karşı yeterince korunması zorunludur.

Güvenliği üzerinde titizlikle durulması gereken sektörlerden biri de finans sektörüdür. Bankacılık, sermaye piyasaları ve diğer finansman kuruluşlarının yanı sıra sigortacılık ve bireysel emekliliği içeren birçok alt sektörü ve kurumu kapsayan finans sektörü ekonominin hayat damarıdır. Finans sektörü, ekonomik aktörlerin kaynak ihtiyacını karşılamak için birikimlere yön vermekte, maruz kalınan risklere karşı koruma sağlamaktadır. Bu işlev, toplumsal servetin korunması, sermayenin tabana yayılması, refahın artması, yatırım ve inovasyonun teşviki açısından büyük önem taşımaktadır.

Vazgeçilmez öneme sahip finans sektörü diğer kritik altyapılar gibi savaşlar, terör, sabotaj, iklim değişikliği, doğal afetler ve büyük ekonomik buhranlar gibi risklerle karşı karşıyadır. Ancak sektörün en önemli sorunu siber güvenliktir. Teknolojiye yatırım yaparak hizmetlerini iyileştiren ve bu sayede inovasyona da öncülük eden finans sektörü, siber saldırıların öncelikli hedefi konumundadır.

Türkiye'de bankacılık ağırlıklı olan finans sektörü, teknoloji kullanımı açısından ileri bir noktadadır. Siber güvenlik mevzuatı açısından da ülkemiz dünyada örnek gösterilebilecek bir konumdadır. Ancak finans sektöründe bazı alanlarda bazı zafiyetler sürmekte, pandemi döneminde artan uzaktan çalışma ve üçüncü parti hizmet kullanımı gibi pratikler siber güvenliğin sağlanmasını güçleştirmektedir.

Bu nedenle STM ThinkTech'in 3 Kasım 2021'de düzenlediği "Bütünleşik Güvenlik Bağlamında Siber" başlıklı odak toplantısına katılan sektör temsilcilerinin altını çizdiği üzere, hassas verilere erişimin kısıtlanması, çalışanlara siber güvenlik bilincinin aşılanması ve sektör paydaşları arasında siber istihbarat paylaşımını sağlayacak mekanizmaların kurulması büyük önem taşımaktadır.

KAYNAKÇA

[1] Ross, Sean; (2021), "Financial Services: Sizing the Sector in the Global Economy", *Investopedia*, (30 Eylül 2021), https://www.investopedia.com/ask/answers/030515/what-percentage-global-economy-comprised-financial-services-sector.asp. (Erişim Tarihi: 12 Ağustos 2022)

[2] *Businesswire*, (2021), "Global Financial Services Market Outlook 2021-2030; Expected to Reach $28.52 Trillion by 2025 - ResearchAndMarkets.com", (10 Mart 2021), https://www.businesswire.com/news/home/20210310005386/en/Global-Financial-Services-Market-Outlook-2021-2030-Expected-to-Reach-28.52-Trillion-by-2025---ResearchAndMarkets .com. (Erişim Tarihi: 12 Ağustos 2022)

[3] *BDDK*, "2021 Faaliyet Raporu", https://www.bddk.org.tr/KurumHakkinda/EkGetir/5?ekId=86. (Erişim Tarihi: 12 Ağustos 2022)

[4] Yetiz, Filiz; (2016), "BANKACILIĞIN DOĞUŞU VE TÜRK BANKACILIK SİSTEMİ", *Niğde Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, (Nisan 2016), https://bit.ly/3PjrcX6. (Erişim Tarihi: 12 Ağustos 2022)

[5] Gülençer, Sinan; (2020), "TÜRKİYE'DEKİ MEVDUAT BANKALARININ TOPSIS VE VIKOR YÖNTEMLERİYLE ANALİZİ", *Kırklareli Üniversitesi Sosyal Bilimler Meslek Yüksekokulu Dergisi*, (Haziran 2020), https://dergipark.org.tr/en/download/article-file/1179657. (Erişim Tarihi: 12 Ağustos 2022)

[6] *Statista*, "Market capitalization of banking market worldwide from 1st quarter 2016 to 3rd quarter 2021", https://www.statista.com/statistics/265135/market-capitalization-of-the-banking-sector-worldwide/. (Erişim Tarihi: 12 Ağustos 2022)

[7] *knoema*, "Market capitalization of listed companies in current prices", https://knoema.com/atlas/topics/Economy/Financial-Sector-Capital-markets/Market-capitalization. (Erişim Tarihi: 12 Ağustos 2022)

[8] Heredia, Lubasha; (2021), "The $100 Trillion Machine", (Temmuz 2021), *Boston Consulting Group*, https://web-assets.bcg.com/79/bf/d1d361854084a9624a0cbce3bf07/bcg-global-asset-management-2021-jul-2021.pdf. (Erişim Tarihi: 12 Ağustos 2022)

[9] A Williams, Ollie; (2021), "World's Wealth Hits Half A Quadrillion Dollars", *Forbes*, (10 Haziran 2021), https://www.forbes.com/sites/oliverwilliams1/2021/06/10/worlds-wealth-hits-half-a-quadrillion-dollars/?sh=4b323a9e309d. (Erişim Tarihi: 12 Ağustos 2022)

[10] *World Bank*, "Financial Sector", https://www.worldbank.org/en/topic/financialsector/overview#:~:text=The%20World%20Bank%20Group%20works,most%20pressing%20financial%20sector%20challenges. (Erişim Tarihi: 12 Ağustos 2022)

[11] Vittorio, Andrea; (2014), "Critical Facilities Would Be Protected From Power Outages by New Jersey Bank", *Clane Group*, (5 Eylül 2014), https://www.cleanegroup.org/wp-content/uploads/Critical-Facilities-Would-Be-Protected-From-Power-Outages-by-New-Jersey-Bank.pdf. (Erişim Tarihi: 12 Ağustos 2022)

[12] Ceylan, Fatih; Erem CEYLAN, Işıl; (2020), "DOES BANK PROFITABILITY PROMOTE ECONOMIC GROWTH AND VICE VERSA? PANEL CAUSALITY EVIDENCE FROM THE SELECTED COUNTRIES", *Journal of Economics, Business & Organization Research*, (2020), https://dergipark.org.tr/tr/download/article-file/1468727#:~:text=The%20banking%20sector%20enables%20the,creation%20through%20the%20credit%20mechanism. (Erişim Tarihi: 12 Ağustos 2022)

[13] *McKinsey*, (2021), "McKinsey's Global Banking Annual Review", (1 Aralık 2021), https://www.mckinsey.com/industries/financial-services/our-insights/global-banking-annual-review. (Erişim Tarihi: 12 Ağustos 2022)

[14] *European Central Bank*, (2022), "Russia-Ukraine war increases financial stability risks, ECB Financial Stability Review finds", (25 Mayıs 2022), https://www.ecb.europa.eu/press/pr/date/2022/html/ecb.pr220525~fa1be4764d.en.html. (Erişim Tarihi: 12 Ağustos 2022)

[15] *BDDK*, (2022), "Türk Bankacılık Sektörü Temel Göstergeleri", (Mart 2022), https://www.bddk.org.tr/Veri/EkGetir/8?ekId=86. (Erişim Tarihi: 12 Ağustos 2022)

[16] *KPMG*, (2022), "Bankacılık Sektörel Bakış", https://assets.kpmg/content/dam/kpmg/tr/pdf/2022/05/bankacilik-sektorel-bakis.pdf. (Erişim Tarihi: 12 Ağustos 2022)

[17] *TBB*, 2022), "Dijital, İnternet ve Mobil Bankacılık İstatistikleri", (Mart 2022), https://www.tbb.org.tr/Content/Upload/istatistiki-raporlar/ekler/3805/Dijital-Internet-Mobil_Bankacilik_Istatistikleri-Mart_2022.pdf. (Erişim Tarihi: 12 Ağustos 2022)

[18] *QNB*, "Yeni normalde büyümek – Faaliyet Raporu 2021", https://www.qnbfinansbank.com/medium/document-file-3455.vsf. (Erişim Tarihi: 12 Ağustos 2022)

[19] *BKM*, "SEÇİLEN AYA AİT GENEL İSTATİSTİK", https://bkm.com.tr/secilen-aya-ait-istatistikler/?filter_year=2022&filter_month=3&List=Listele. (Erişim Tarihi: 12 Ağustos 2022)

[20] *Antalya Ticaret ve Sanayi Odası*, (2022), "KREDİ VE BANKA KARTI HARCAMALARINDAKİ ARTIŞ HIZLA DEVAM EDİYOR", (21 Nisan 2022), https://www.atsovizyon.org.tr/kredi-ve-banka-karti-harcamalarindaki-artis-hizla-devam-ediyor/. (Erişim Tarihi: 12 Ağustos 2022)

[21] Arslan Coşkun, Özge; Eken, Mehmet Hasan; (2015), "2001 ve 2008 Krizlerinin Türk Bankacılık Sektörüne Etkilerinin Karşılaştırılması", *Dergipark*, https://dergipark.org.tr/tr/download/article-file/412417. (Erişim Tarihi: 12 Ağustos 2022)

[22] Şanlı, Orhan; (2021), "TÜRKİYE'DE 1994, 2001 VE 2018-2021 KUR KRİZLERİNİN YENİ NESİL KRİZ TEORİLERİ ÇERÇEVESİNDE İNCELENMESİ (EXAMINING OF THE 1994, 2001 AND 2018-2021 CURRENCY CRISES IN TURKEY WITHIN THE FRAMEWORK OF THE NEW GENERATION CRISIS THEORIES)", *Research Gate*, (Aralık 2021), https://bit.ly/3bNrnMD. (Erişim Tarihi: 12 Ağustos 2022)

[23] *IMF*, "Financial Access Survey", https://data.imf.org/?sk=E5DCAB7E-A5CA-4892-A6EA-598B5463A34C&sId=1390030109571. (Erişim Tarihi: 12 Ağustos 2022)

[24] *Deloitte*, (2022), "E-ticaretin öne çıkan başarısı, tüketici davranışlarında değişim ve dijitalleşme", (Şubat 2022), https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/consulting/E-ticaretin-one-cikan-basarisi-2022.pdf. (Erişim Tarihi: 12 Ağustos 2022)

[25] *Accenture*, (2021), "Banking as usual", https://images.info.accenture.com/Web/ACCENTURE/%7B23aa3f91-cda-c-4119-8e63-506e4e36b34e%7D_Accenture-Banking-Global-Industry-Outlook.pdf?elqcst=272&elqcsid=1168. (Erişim Tarihi: 12 Ağustos 2022)

[26] Dixit, Nimayi; (2021), "Pandemic pushes customers out of branches, banks ramp up closures", *S&P Global*, (13 Temmuz 2021), https://www.spglobal.com/marketintelligence/en/news-insights/reseaaarch/pandemic-pushes-customers-out-of-branches-banks-ramp-up-closures. (Erişim Tarihi: 12 Ağustos 2022)

[27] Peru, Georgie; (2022), "Mobile Banking Statistics (2022)", *Web Hosting Professional*, (13 Mart 2022), https://webhostingprof.com/blog/mobile-banking-statistics/

[28] *CBINSIGHTS*, "The Complete List Of Unicorn Companies", https://www.cbinsights.com/research-unicorn-companies. (Erişim Tarihi: 12 Ağustos 2022)

[29] *CBINSIGHTS*, (2021), "The Big Tech In Fintech Report: How Facebook, Apple, Google, & Amazon Are Battling For The $28.2T

Market", (17 Haziran 2021), https://www.cbinsights.com/research/report/famga-big-tech-fintech/. (Erişim Tarihi: 12 Ağustos 2022)

[30] *Resmi Gazete*, (2021), "DİJİTAL BANKALARIN FAALİYET ESASLARI İLE SERVİS MODELİ BANKACILIĞI HAKKINDA YÖNETMELİK", (29 Aralık 2021), https://www.resmigazete.gov.tr/eskiler/2021/12/20211229-6.htm. (Erişim Tarihi: 12 Ağustos 2022)

[31] *IBM*, "2022 Global Outlook for Banking and Financial Markets", https://www.ibm.com/downloads/cas/5DEMLZBL

[32] *STM ThinkTech*, (2022), "Metaverse Ekonomisi", (14 Haziran 2022), https://thinktech.stm.com.tr/tr/metaverse-ekonomisi. (Erişim Tarihi: 12 Ağustos 2022)

[33] Sen, Meghna; (2022), "Crypto market can slumps under $1 trillion for first time since Jan 2021", *mint*, (14 Haziran 2022), https://www.livemint.com/market/cryptocurrency/crypto-market-cap-slumps-under-1-trillion-for-first-time-since-jan-2021-11655112702885.html. (Erişim Tarihi: 12 Ağustos 2022)

[34] *STM ThinkTech*, (2022), "Metaverse: Fırsatlar ve Tehditler", (14 Şubat 2022), https://thinktech.stm.com.tr/tr/metaverse-firsatlar-ve-tehditler. (Erişim Tarihi: 12 Ağustos 2022)

[35] *Atlantic Council*, "Central Bank Digital Currency Tracker", https://www.atlanticcouncil.org/cbdctracker/#:~:text=105%20countries%2C%20representing%20over%2095,GDP%2C%20are%20exploring%20a%20CBDC. (Erişim Tarihi: 12 Ağustos 2022)

[36] *TCMB*, (2021), "Merkez Bankası Dijital Türk Lirası Ar-Ge Projesi Hakkında Basın Duyurusu", (15 Eylül 2021), https://www.tcmb.gov.tr/wps/wcm/connect/TR/TCMB+TR/Main+Menu/Duyurular/Basin/2021/DUY2021-40. (Erişim Tarihi: 12 Ağustos 2022)

[37] Weiss, N. Eric; (2009), "Banking and Financial Infrastructure Continuity: Pandemic Flu, Terrorism, and Other Challenges", *Congressional Research Service*, (4 Mayıs 2009), https://sgp.fas.org/crs/misc/RL31873.pdf. (Erişim Tarihi: 12 Ağustos 2022)

[38] *BBC*, (2020), "Dünyadaki ekonomik krizler: 150 yılda yaşanan 14 resesyon nasıl başladı, maliyeti ne oldu?", (8 Temmuz 2020), https://www.bbc.com/turkce/haberler-dunya-53327594. (Erişim Tarihi: 12 Ağustos 2022)

[39] Tarakçı, Ceyhun Cem; (2019), "TÜRKİYE'DE YAŞANAN EKONOMİK KRİZLER, MALİ ETKİLERİ VE KAMUSAL TEDBİRLER: 2001 VE 2008 KRİZLERİ", *İstanbul Üniversitesi*, http://nek.istanbul.edu.tr:4444/ekos/TEZ/ET000842.pdf. (Erişim Tarihi: 12 Ağustos 2022)

[40] CHACHAK, ELIAS; "Financial Cyber-Attacks in 2021", *CyberDB*, https://www.cyberdb.co/financial-cyber-attacks-in-2021/. (Erişim Tarihi: 12 Ağustos 2022)

[41] *IBM*, (2022), "X-Force Threat Intelligence Index 2022", (Şubat 2022), https://www.ibm.com/downloads/cas/ADLMYLAZ. (Erişim Tarihi: 12 Ağustos 2022)

[42] *Akamai*, (2019), "Akamai Threat Research: Phishing and Credential Stuffing Attacks Remain Top Threat to Financial Services Organizations and Customers", (30 Temmuz 2019), https://www.akamai.com/newsroom/press-release/state-of-the-internet-security-financial-services-attack-economy. (Erişim Tarihi: 12 Ağustos 2022)

[43] *U.S. Department of the Treasury*, (2021), "Treasury Continues to Counter Ransomware as Part of Whole-of-Government Effort; Sanctions Ransomware Operators and Virtual Currency Exchange", (8 Kasım 2021), https://home.treasury.gov/news/press-releases/jy0471. (Erişim Tarihi: 12 Ağustos 2022)

[44] Osborne, Charlie; (2022), "1.5 million customers impacted by Flagstar Bank data breach", *ZDNet*, (21 Haziran 2022), https://www.zdnet.com/article/1-5-million-customers-impacted-in-flagstar-data-breach/. (Erişim Tarihi: 12 Ağustos 2022)

[45] *CySecurity*, (2021), "Banco Pichincha: Ecuador's Largest Bank Hit by a Cyber Attack", (15 Kasım 2021), https://www.cysecurity.news/2021/10/banco-pichincha-ecuadors-largest-bank.html. (Erişim Tarihi: 12 Ağustos 2022)

[46] *Akamai*, (2021), "Phishing for Finance", https://www.akamai.com/site/en/documents/state-of-the-internet/soti-security-phishing-for-finance-report-2021.pdf. (Erişim Tarihi: 12 Ağustos 2022)

[47] *Turk Internet*, (2015), "DDOS Saldırısı Banka İşlemlerini de Etkiledi", (27 Aralık 2015), https://turk-internet.com/ddos-saldirisi-banka-islemlerini-de-etkiledi/. (Erişim Tarihi: 12 Ağustos 2022)

[48] Baş, Hanife; (2019), "Türkiye büyük siber saldırı atlattı", *Milliyet*, (29 Ekim 2019), https://www.milliyet.com.tr/ekonomi/turkiye-buyuk-siber-saldiri-atlatti-6067044. (Erişim Tarihi: 12 Ağustos 2022)

[49] *Reuters*, (2021), "German cooperative banks hit by DDoS hack attack on IT provider", (4 Haziran 2021), https://www.reuters.com/technology/german-it-company-that-serves-banks-experiences-ddos-hack-attack-2021-06-04/. (Erişim Tarihi: 12 Ağustos 2022)

[50] *Deloitte*, (2019), "SWIFT Systems and the SWIFT Customer Security Program", (Ekim 2019), https://www2.deloitte.com/content/dam/Deloitte/be/Documents/risk/be-ra-swift-customer-security-programme.pdf. (Erişim Tarihi: 12 Ağustos 2022)

[51] Banka, Neha; (2021), "Explained: The story of how North Korea hackers stole $81 million from Bangladesh Bank", *Indian Express*, (30 Haziran 2021), https://indianexpress.com/article/explained/bangladesh-bank-robbery-north-korea-lazarus-heist-7375441/. (Erişim Tarihi: 12 Ağustos 2022)

[52] *Reuters*, (2017), "Taiwan's Far Eastern International fined T$8 million over SWIFT hacking incident", (12 Aralık 2017), https://www.reuters.com/article/us-far-eastern-fine-idUSKBN1E60Y3. (Erişim Tarihi: 12 Ağustos 2022)

[53] *Reuters*, (2017), "Hackers tried to steal 55 mln roubles from Russia's Globex bank - Kommersant", (21 Aralık 2017), https://www.reuters.com/article/russia-cyber-globex-idINL8N1OL4DP. (Erişim Tarihi: 12 Ağustos 2022)

[54] *IBM*, (2021), "IBM Report: Cost of a Data Breach Hits Record High During Pandemic", (28 Temmuz 2021), https://newsroom.ibm.com/2021-07-28-IBM-Report-Cost-of-a-Data-Breach-Hits-Record-High-During-Pandemic. (Erişim Tarihi: 12 Ağustos 2022)

[55] *Trend Micro*, (2021), "Attacks Surge in 1H 2021 as Trend Micro Blocks 41 Billion Cyber Threats", (14 Eylül 2021), https://newsroom.trendmicro.com/2021-09-14-Attacks-Surge-in-1H-2021-as-Trend-Micro-Blocks-41-Billion-Cyber-Threats. (Erişim Tarihi: 12 Ağustos 2022)

[56] M. Eisenbach, Thomas; (2020), "Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis", *Federal Reserve Bank of New York*, (Ocak 2020), https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr909.pdf. (Erişim Tarihi: 12 Ağustos 2022)

[57] *Cybersecurity INSIDER*, (2020), "Insider Threat Report", https://www.cybersecurity-insiders.com/wp-content/uploads/2019/11/2020-Insider-Threat-Report-Gurucul.pdf. (Erişim Tarihi: 12 Ağustos 2022)

[58] *Paloalto Networks*, "Financial Services Cybersecurity", https://www.paloaltonetworks.com/industry/unit42-financial-services. (Erişim Tarihi: 12 Ağustos 2022)

[59] Gatlan, Sergiu; (2021), "Fired NY credit union employee nukes 21GB of data in revenge", *Bleeping Computer*, (1 Eylül 2021), https://www.bleepingcomputer.com/news/security/fired-ny-credit-union-employee-nukes-21gb-of-data-in-revenge/. (Erişim Tarihi: 12 Ağustos 2022)

[60] *Infoblox*, (2022), "2022 Global State of Security Report", https://files.scmagazine.com/wp-content/uploads/2022/05/Infoblox-Main-Report.pdf. (Erişim Tarihi: 12 Ağustos 2022)

[61] Picus Labs Blue Team; Özarslan, Süleyman; (2021), "Six Stages of Dealing with a Global Security Incident", *Picus*, (5 Ocak 2021), https://www.picussecurity.com/resource/blog/six-stages-of-dealing-with-a-global-security-incident. (Erişim Tarihi: 12 Ağustos 2022)

[62] *Deloitte*, "Cloud banking: More than just a CIO conversation", https://www2.deloitte.com/be/en/pages/financial-services/articles/bank-2030-financial-services-cloud.html. (Erişim Tarihi: 12 Ağustos 2022)

[63] *Financial Stability Board*, (2019), "Third-party dependencies in cloud services: Considerations on financial stability implications", (9 Aralık 2019), https://www.fsb.org/2019/12/third-party-dependencies-in-cloud-services-considerations-on-financial-stability-implications/. (Erişim Tarihi: 12 Ağustos 2022)

[64] Wilson, Christopher; (2019), "Cybersecurity Risk Supervision", *IMF*, https://www.imf.org/-/media/Files/Publications/DP/2019/English/CRSEA.ashx. (Erişim Tarihi: 12 Ağustos 2022)

[65] Gaidosch, Tamas; (2019), "Cybersecurity Risk Supervision", (24 Eylül 2019), https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2019/09/23/Cybersecurity-Risk-Supervision-46238. (Erişim Tarihi: 12 Ağustos 2022)

[66] *World Bank*, (2022), "Cybersecurity and the Financial Sector: The Third-Party Risk Challenge", (10 Mayıs 2022), https://www.worldbank.org/en/events/2022/04/28/cybersecurity-and-the-financial-sector-the-third-party-risk-challenge. (Erişim Tarihi: 12 Ağustos 2022)

[67] *European Union Agency For Cybersecurity*, "Network and Information Security in Finance Sector", https://resilience.enisa.europa.eu/EGFI. (Erişim Tarihi: 12 Ağustos 2022)

[68] *Resmi Gazete*, (2020), "BANKALARIN BİLGİ SİSTEMLERİ VE ELEKTRONİK BANKACILIK HİZMETLERİ HAKKINDA YÖNETMELİK", (15 Mart 2020), https://www.resmigazete.gov.tr/eskiler/2020/03/20200315-10.htm. (Erişim Tarihi: 12 Ağustos 2022)

[69] *Bilgi Teknolojileri Kurumu*, (2013), "T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı", (Ocak 2013), https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-plani-2013-2014-5a3412cf8f45a.pdf. (Erişim Tarihi: 12 Ağustos 2022)

[70] *T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi*, (2020), "Bilgi ve İletişim Güvenliği Rehberi", (24 Temmuz 2020), https://cbddo.gov.tr/bigrehber/. (Erişim Tarihi: 12 Ağustos 2022)

[71] Akçakanat, Özen; (2021), "İşletmelerde Siber Güvenlik Riskleri ve Bilgi Teknolojileri Denetimi: Bankaların Siber Güvenlik Uygulamalarının İncelenmesi", *Mehmet Akif Ersoy Üniversitesi Uygulamalı Bilimler Dergisi*, https://dergipark.org.tr/en/download/article-file/1906847. (Erişim Tarihi: 12 Ağustos 2022)

[72] Bora, Ali; (1997), "Finansal Piyasalar ve Türkiye Değerlendirmesi", *Dergipark*, (Ocak 1997), https://dergipark.org.tr/en/download/article-file/1071985. (Erişim Tarihi: 12 Ağustos 2022)

[73] *TCMB*, "Piyasalar", https://www.tcmb.gov.tr/wps/wcm/connect/TR/TCMB+TR/Main+Menu/Banka+Hakkinda/Sikca+Sorulan+Sorular/Piyasalar/. (Erişim Tarihi: 12 Ağustos 2022)

[74] *TAKAS İSTANBUL*, "Genel Tanım", https://www.takasbank.com.tr/tr/hizmetler/isletilen-piyasalar/takasbank-para-piyasasi-tpp/genel-tanim. (Erişim Tarihi: 12 Ağustos 2022)

[75] Fıkırkoca Asena, Ekin; Altaş, Gökben; Yalın Uzunlu, Barış; Anıl, Ceylan; Kahraman, Deniz; (2022), "Türkiye Sermaye Piyasası 2021", *TSPB*, (Mayıs 2022), https://www.tspb.org.tr/wp-content/uploads/2022/05/Turkiye-Sermaye-Piyasasi-2021.pdf

[76] Hazar, Adalet; Babuşcu, Şenol; Başcı, Esref Savaş; Ersoy, Ersan; (2021), "Sermaye Piyasası Araçları - Teori, İşleyiş ve Uygulama Örnekleri", *Research Gate*, (Eylül 2021), https://www.researchgate.net/publication/355889246_Sermaye_Piyasasi_Araclari_-_Teori_Isleyis_ve_Uygulama_Ornekleri. (Erişim Tarihi: 12 Ağustos 2022)

[77] Akbulut, Yıldız; "SERMAYE PİYASASININ GELİŞMESİNDE MUHASEBE BİLGİLERİNİN ÖNEMİ", *Mevzuat Dergisi*, https://bit.ly/3zTBvM0 . (Erişim Tarihi: 12 Ağustos 2022)

[78] *IFC*, (2017), "THE IMPORTANCE OF LOCAL CAPITAL MARKETS FOR FINANCING DEVELOPMENT", (Ocak 2017), https://www.ifc.org/wps/wcm/connect/3784b5b2-6e70-4067-87d8-3ab54cced330/EM+compass+Note+28+Capital+Markets+FINAL+1-26+FINAL2.pdf?MOD=AJPERES&CVID=lDuoHOp. (Erişim Tarihi: 12 Ağustos 2022)

[79] *sifma*, (2021), "2021 Capital Markets Fact Book", (Temmuz 2021), https://www.sifma.org/wp-content/uploads/2021/07/CM-Fact-Book-2021-SIFMA.pdf. (Erişim Tarihi: 12 Ağustos 2022)

[80] *World Bank*, "Gross domestic product 2021", https://databank.worldbank.org/data/download/GDP.pdf. (Erişim Tarihi: 12 Ağustos 2022)

[81] *Reuters*, (2022), "Gross domestic product 2021", (24 Şubat 2022), https://www.reuters.com/business/ukraines-stock-market-regulator-stops-securities-circulation-2022-02-24/. (Erişim Tarihi: 12 Ağustos 2022)

[82] *ALARABIA*, (2022), "Moscow stock exchange begins gradual reopening with bonds trading", (21 Mart 2022), https://english.alarabiya.net/business/markets/2022/03/21/Moscow-stock-exchange-begins-gradual-reopening-with-bonds-trading. (Erişim Tarihi: 12 Ağustos 2022)

[83] Semenova, Alexandra; (2022), "Stock market news live updates: Stocks fall after Russia-Ukraine ceasefire talks fail, red-hot CPI print", *Yahoo*, (11 Mart 2022), https://finance.yahoo.com/news/stock-market-news-live-updates-march-10-2022-233755035.html. (Erişim Tarihi: 12 Ağustos 2022)

[84] Ağırman, Ensar; Özcan, Muhammet; Yılmaz, Ömer; (2014), "Terörizmin Finansal Piyasalara Etkisi: Ampirik Bir Çalışma", *BDDK*, https://www.bddk.org.tr/Content/docs/bddkDergiTr/dergi_0016_06.pdf. (Erişim Tarihi: 12 Ağustos 2022)

[85] ASLAM, FAHEEM; (2018), "THE IMPACT OF TERRORISM ON FINANCIAL MARKETS: EVIDENCE FROM ASIA", *World Scientific*, https://www.worldscientific.com/doi/10.1142/S0217590815501118. (Erişim Tarihi: 12 Ağustos 2022)

[86] Treanor, Jill; (2010), "Turquoise trading shutdown may have been sabotage, LSE says", *Guardian*, (2 Kasım 2010), https://www.theguardian.com/business/2010/nov/02/turquoise-trading-shutdown-sabotage-suspicions. (Erişim Tarihi: 12 Ağustos 2022)

[87] *T24*, (2014), "'İstanbul borsasına sabotaj' iddiası", (23 Temmuz 2014), https://t24.com.tr/haber/istanbul-borsasina-sabotaj-iddiasi,265288. (Erişim Tarihi: 12 Ağustos 2022)

[88] Faccini, Renato; (2021), "Are Climate-Change Risks Reflected in Stock Prices?", *CLS Blue Sky Blog*, (3 Kasım 2021), https://clsbluesky.law.columbia.edu/2021/11/03/are-climate-change-risks-reflected-in-stock-prices/. (Erişim Tarihi: 12 Ağustos 2022)

[89] *STM ThinkTech*, (2021), "Yeni İklim Rejimine Doğru: Avrupa Yeşil Mutabakatı Ve Türkiye'ye Etkileri Üzerine Bir İnceleme", (22 Aralık 2021); https://thinktech.stm.com.tr/tr/yeni-iklim-rejimine-dogru-avrupa-yesil-mutabakati-ve-turkiyeye-etkileri-uzerine-bir-inceleme. (Erişim Tarihi: 12 Ağustos 2022)

[90] *United Nations*, (2021), "The trillion dollar climate finance challenge (and opportunity)", (27 Haziran 2021), https://news.un.org/en/story/2021/06/1094762. (Erişim Tarihi: 12 Ağustos 2022)

[91] Kutukız, Doğan; "Menkul Kıymet Piyasalarında Manipülasyon ve İstanbul Menkul Kıymet Borsası'nda Manipülasyon Önlemleri", *Dergipark*, https://dergipark.org.tr/tr/download/article-file/116542. (Erişim Tarihi: 12 Ağustos 2022)

[92] *Bloomberg*, (2020), "Borsada manipülasyon cezaları 80 milyon TL'yi aştı", (4 Kasım 2020), https://www.bloomberght.com/borsada-manipulasyon-cezalari-80-milyon-tl-yi-asti-2267880. (Erişim Tarihi: 12 Ağustos 2022)

[93] *Bloomberg*, (2020), "Dijitalleşme, borsada yatırımcı sayısındaki artışta önemli faktör", (9 Temmuz 2020), https://www.bloomberght.com/finansal-teknoloji/video/dijitallesme-borsada-yatirimci-sayisindaki-artista-onemli-faktor/63945. (Erişim Tarihi: 12 Ağustos 2022)

[94] Robinson, Justine; (2022), "How Cybersecurity Issues Affect Stock Prices", *CyberProtection Magazine*, (18 Şubat 2022), https://cyberprotection-magazine.com/how-cybersecurity-issues-affect-stock-prices. (Erişim Tarihi: 12 Ağustos 2022)

[95] Polyakov, Alex; (2021), "Could The Next Stock Market Crash Be Potentially Caused By A Cyberattack?", *Forbes*, (14 Nisan 2021), https://www.forbes.com/sites/forbestechcouncil/2021/04/14/could-the-next-stock-market-crash-be-potentially-caused-by-a-cyberattack/. (Erişim Tarihi: 12 Ağustos 2022)

[96] *IOSCO*, (2013), "Cyber-crime, securities markets and systemic risk", (16 Temmuz 2013), https://www.iosco.org/research/pdf/swp/Cyber-Crime-Securities-Markets-and-Systemic-Risk.pdf. (Erişim Tarihi: 12 Ağustos 2022)

[97] Tarabay, Jamie; (2021), "How a Dated Cyber-Attack Brought a Stock Exchange to its Knees", *Bloomberg*, (4 Şubat 2021), https://www.bloomberg.com/news/articles/2021-02-04/how-a-dated-cyber-attack-brought-a-stock-exchange-to-its-knees#xj4y7vzkg. (Erişim Tarihi: 12 Ağustos 2022)

[98] *Mevzuat.gov*, (1956), "TÜRK TİCARET KANUNU", (9 Temmuz 1956), https://www.mevzuat.gov.tr/MevzuatMetin/5.3.6762.pdf. (Erişim Tarihi: 12 Ağustos 2022)

[99] Akın, Faruk; Ece, Nalan; (2011), "Gelişmiş ve gelişmekte olan ülkelerde sigortacılık sektörü: türk sigorta sektörü üzerine bir değerlendirme", *ABMYO Dergisi*, https://dergipark.org.tr/tr/download/article-file/746890#:~:text=Sigortac%C4%B1l%C4%B1k%3B%20topluma%20ve%20ekonomiye%2C%20ekonomik,2006%2C%209%2D11. (Erişim Tarihi: 12 Ağustos 2022)

[100] Okan Yayla, Şerafettin; (2019), "Sigortacılık ve Türkiye'de Sigorta Sektörünün Durumu", *Liberal Düşünce Dergisi*, (27 Haziran 2019), https://dergipark.org.tr/tr/download/article-file/753795. (Erişim Tarihi: 12 Ağustos 2022)

[101] *Swiss Re Institute*, (2022), "sigma 4/2022 - World insurance", (13 Temmuz 2022), https://www.swissre.com/institute/research/sigma-research/sigma-2022-04.html. (Erişim Tarihi: 12 Ağustos 2022)

[102] Tucker, Hank; (2022), "Forbes Global 2000: The World's Largest Insurance Companies In 2022", *Forbes*, (12 Mayıs 2022), https://www.forbes.com/sites/hanktucker/2022/05/12/the-worlds-largest-insurance-companies-in-2022/?sh=2e70a04339a1. (Erişim Tarihi: 12 Ağustos 2022)

[103] *KPMG*, (2021), "KPMG Perspektifinden Sigortacılık Sektörüne Bakış", https://assets.kpmg/content/dam/kpmg/tr/pdf/2021/05/sigorta-sektorel-bakis-2021.pdf. (Erişim Tarihi: 12 Ağustos 2022)

[104] *McKinsey*, (2022), "Creating value, finding focus: Global Insurance Report 2022", (15 Şubat 2022), https://www.mckinsey.com/industries/financial-services/our-insights/creating-value-finding-focus-global-insurance-report-2022. (Erişim Tarihi: 12 Ağustos 2022)

[105] *T.C. SİGORTACILIK VE ÖZEL EMEKLİLİK DÜZENLEME VE DENETLEME KURUMU*, (2021), "SİGORTACILIK VE ÖZEL EMEKLİLİK FAALİYETLERİ HAKKINDA RAPOR", https://www.seddk.gov.tr/upload/doc/2021-sigortacilik-ve-BES-faaliyet-raporu.pdf. (Erişim Tarihi: 12 Ağustos 2022)

[106] Bevere, Lucia; (2022), "Natural catastrophes in 2021: the floodgates are open", *Swiss Re Institute*, (30 Mart 2022), https://www.swissre.com/institute/research/sigma-research/sigma-2022-01.html. (Erişim Tarihi: 12 Ağustos 2022)

[107] Holzheu, Thomas; (2021), "sigma 4/2021 - More risk: the changing nature of P&C insurance opportunities to 2040", *Swiss Re Institute*, (6 Eylül 2021), https://www.swissre.com/institute/research/sigma-research/sigma-2021-04.html. (Erişim Tarihi: 12 Ağustos 2022)

[108] *Swiss Re Institute*, (2021), "In a world of growing risk the insurance industry has a crucial role to play", (6 Eylül 2021), https://www.swissre.com/risk-knowledge/building-societal-resilience/growing-risk-insurance-industry-crucial-role.html. (Erişim Tarihi: 12 Ağustos 2022)

[109] *Grand View Research*, (2022), "Insurtech Market Size, Share & Trends Analysis Report By Type", https://www.grandviewresearch.com/industry-analysis/insurtech-market#:~:text=The%20global%20insurtech%20market%20is,USD%20152.43%20billion%20by%202030. (Erişim Tarihi: 12 Ağustos 2022)

[110] *Globe News Wire*, (2021), "UFCIC Becomes First U.S. Insurer to Accept Cryptocurrency for Premium Payments", (22 Haziran 2021), https://www.globenewswire.com/en/news-release/2021/06/22/2251213/0/en/UFCIC-Becomes-First-U-S-Insurer-to-Accept-Cryptocurrency-for-Premium-Payments.html. (Erişim Tarihi: 12 Ağustos 2022)

[111] *KPMG*, (2017), "Will on-demand insurance become mainstream?", (Eylül 2017), https://assets.kpmg/content/dam/kpmg/uk/pdf/2017/09/will-on-demand-insurance-become-mainstream.pdf. (Erişim Tarihi: 12 Ağustos 2022)

[112] *NAIC*, (2022), "ON-DEMAND INSURANCE", (11 Mayıs 2022), https://content.naic.org/cipr-topics/demand-insurance. (Erişim Tarihi: 12 Ağustos 2022)

[113] Atilla, İclal; Gülay, Abdulaziz; (2022), "TÜRKİYE'DE SİGORTA PRİM ÜRETİMLERİNİN DÜNYA SİGORTACILIK SEKTÖRÜNDEKİ YERİ", *Uygulamalı Sosyal Bilimler ve Güzel Sanatlar Dergisi*, https://dergipark.org.tr/en/download/article-file/2403012. (Erişim Tarihi: 12 Ağustos 2022)

[114] Meral, Hasan; (2021), ""Covid-19 Sonrası Türk Sigorta Sektörünün Genel Görünümü", *Sigorta Strateji*, (17 Kasım 2021), https://sigortastrateji.com/inceleme/covid-19-sonrasi-turk-sigorta-sektorunun-genel-gorunumu/. (Erişim Tarihi: 12 Ağustos 2022)

[115] *PriceWaterhouseCoopers*, (2021), "Insurance Banana Skins 2021", (Ekim 2021), https://www.pwc.com.tr/tr/sektorler/sigortacilik/pdf/sigortacilikta-ongorulen-riskler-2021.pdf. (Erişim Tarihi: 12 Ağustos 2022)

[116] Davies, Vikki; (2022), "5 cybersecurity threats hitting insurance companies in 2022", *InsurTech*, (20 Mart 2022), https://insurtechdigital.com/insurtech/5-cybersecurity-threats-hitting-insurance-companies-in-2022. (Erişim Tarihi: 12 Ağustos 2022)

[117] Mehrotra, Kartikay; Turton, William; (2021), "CNA Financial Paid $40 Million in Ransom After March Cyberattack", *Bloomberg*, (20 Mayıs 2021), https://www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack#xj4y7vzkg. (Erişim Tarihi: 12 Ağustos 2022)

[118] Ambrose, Lynn; (2022), "Cyber Risk and Insurance in 2022", *Insurance Thought Leadership* (9 Mart 2022), https://www.insurancethoughtleadership.com/cyber/cyber-risk-and-insurance-2022. (Erişim Tarihi: 12 Ağustos 2022)

[119] *Munich RE*, (2022), "Munich Re Global Cyber Risk and Insurance Survey 2022" https://www.munichre.com/content/dam/munichre/contentlounge/website-pieces/documents/Munich-Re-Topics-Cyber-Whitepaper-2022.pdf/_jcr_content/renditions/original./MunichRe-Topics-Cyber-Whitepaper-2022.pdf. (Erişim Tarihi: 12 Ağustos 2022)

[120] S & P Global Ratings, (2022), "Russia-Ukraine Conflict Adds To A Bumpy Start To 2022 For Global Reinsurers", (31 Mart 2022), https://www.spglobal.com/ratings/en/research/articles/220331-russia-ukraine-conflict-adds-to-a-bumpy-start-to-2022-for-global-reinsurers-12329001. (Erişim Tarihi: 12 Ağustos 2022)

[121] *Financial Times*, (2022), "Insurance industry braces for soaring payouts from war in Ukraine", https://www.ft.com/content/e62df5f9-1716-4220-b583-91ba24d4cfb2. (Erişim Tarihi: 12 Ağustos 2022)

[122] *Türkiye Sigorta Birliği*, (2021), "AKLAMA, TERÖRİZMİN ve KİTLE İMHA SİLAHLARININ FİNANSMANI İLE MÜCADELEDE SİGORTA VE BİREYSEL EMEKLİLİK SEKTÖR REHBERİ", (12 Temmuz 221), https://tsb.org.tr/media/ckeditor_uploads/2021/08/09/masak_sektor-rehberi-09082021.pdf. (Erişim Tarihi: 12 Ağustos 2022)

[123] Özcan, Yusuf; (2019), "Yellow Vest protests cause $225M in damages", Anadolu Ajansı, (26 Mart 2019), https://www.aa.com.tr/en/europe/yellow-vest-protests-cause-225m-in-damages/1430929. (Erişim Tarihi: 12 Ağustos 2022)

[124] *Business Insurance*, (2019), "Protests cause $3 billion of property damage in Chile", (27 Kasım 2019), https://www.businessinsurance.com/article/20191127/STORY/912331938/Protests-cause-$3-billion-of-property-damage-in-Chile. (Erişim Tarihi: 12 Ağustos 2022)

[125] Hui, Zhang; Qingqing, Chen; (2019), "Violent HK protests cause billions in damage", *Global Times*, (10 Eylül 2019), https://www.globaltimes.cn/content/1164212.shtml. (Erişim Tarihi: 12 Ağustos 2022)

[126] *refworld*, (2004), "Chronology for Lowland Indigenous Peoples in Bolivia", https://www.refworld.org/docid/469f386b1e.html. (Erişim Tarihi: 12 Ağustos 2022)

[127] León Cabrera, José María; Janetsky, Megan; (2022), "Ecuador Roiled by Protests Set Off by Rising Fuel and Food Prices", New York Times, (23 Haziran 2022), https://www.nytimes.com/2022/06/23/world/americas/quito-ecuador-protests-inflation.html. (Erişim Tarihi: 12 Ağustos 2022)

[128] Polumbo, Brad; (2020), "George Floyd Riots Caused Record-Setting $2 Billion in Damage, New Report Says. Here's Why the True Cost Is Even Higher", *FEE Stories*, (16 Eylül 2020), https://fee.org/articles/george-floyd-riots-caused-record-setting-2-billion-in-damage-new-report-says-here-s-why-the-true-cost-is-even-higher. (Erişim Tarihi: 12 Ağustos 2022)

[129] *Fitch Ratings*, (2022), "Losses from Sri Lanka's Riots Manageable for Insurers", (26 Mayıs 2022), https://www.fitchratings.com/research/insurance/losses-from-sri-lankas-riots-manageable-for-insurers-26-05-2022. (Erişim Tarihi: 12 Ağustos 2022)

[130] Kumar, Nikhil; (2022), "War, protest and spiking prices: How spiraling inflation is setting the world on fire", *Grid*, (6 Temmuz 2022), https://www.grid.news/story/global/2022/07/06/war-protest-and-spiking-prices-how-spiralling-inflation-is-setting-the-world-on-fire/. (Erişim Tarihi: 12 Ağustos 2022)

[131] Bateman, Jon; (2020), "War, Terrorism, and Catastrophe in Cyber Insurance: Understanding and Reforming Exclusions", *Carnegie Endowment For International Peace*, (5 Ekim 2020), https://carnegieendowment.org/2020/10/05/war-terrorism-and-catastrophe-in-cyber-insurance-understanding-and-reforming-exclusions-pub-82819. (Erişim Tarihi: 12 Ağustos 2022)

[132] *STM ThinkTech*, (2022), "Bütünleşik Güvenlik Bağlamında Siber", (18 Şubat 2022), https://thinktech.stm.com.tr/tr/butunlesik-guvenlik-baglaminda-siber. (Erişim Tarihi: 12 Ağustos 2022)

thinktech
STM Teknolojik Düşünce Merkezi
http://thinktech.stm.com.tr