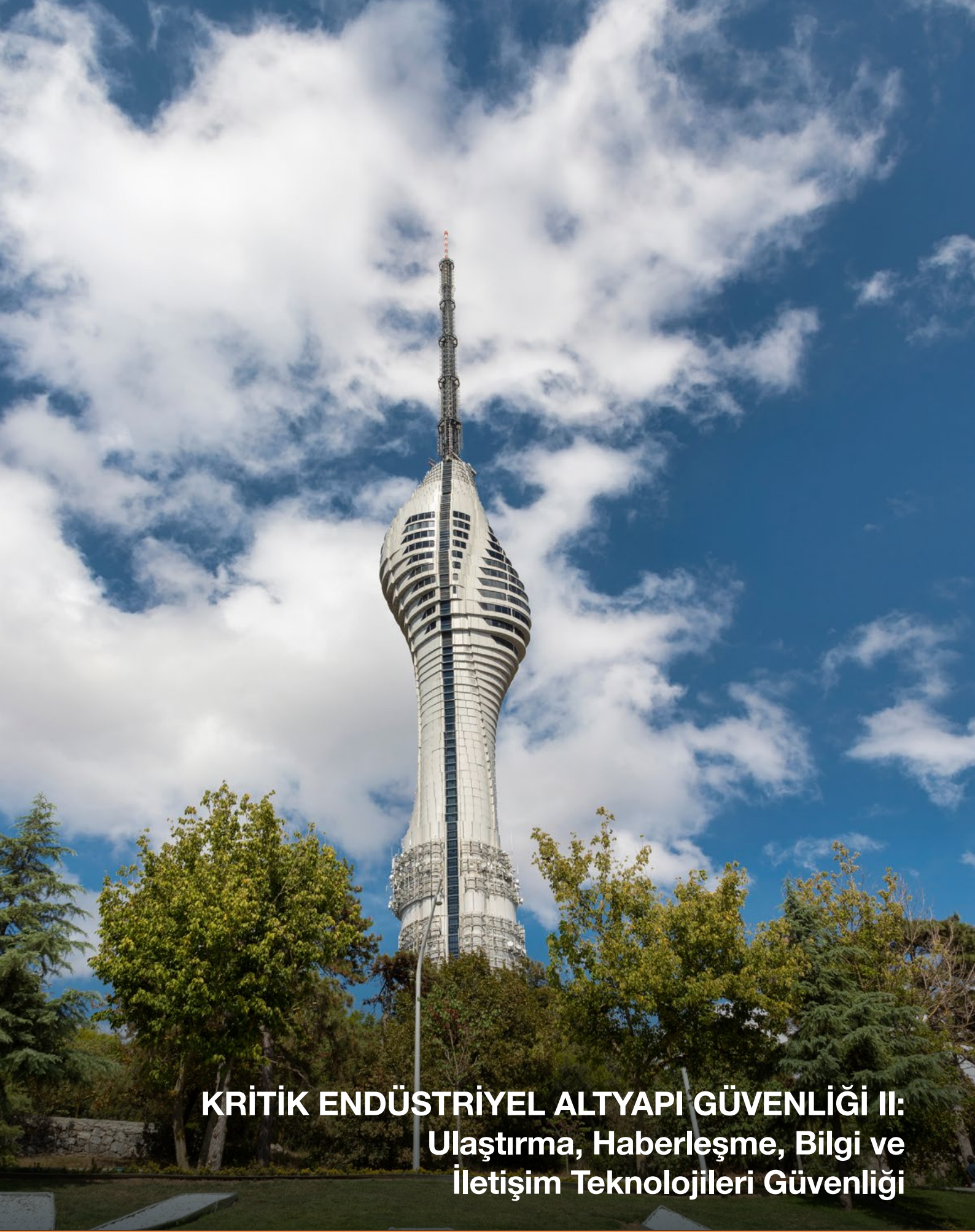


KRİTİK ENDÜSTRİYEL ALTYAPI GÜVENLİĞİ II: Ulaştırma, Haberleşme, Bilgi ve İletişim Teknolojileri Güvenliği

ARAŞTIRMA RAPORU TEMMUZ 2022

thinktech
STM Teknolojik Düşünce Merkezi

STM ThinkTech

1. GİRİŞ

Dünya genelinde, güvenlik anlayışının yeniden gözden geçirilmek zorunda kalındığı zamanlardan geçilmektedir. Küresel iklim değişikliği, COVID-19 pandemisi ve Rusya-Ukrayna savaşı küresel güvenlik kaygılarını bir kat daha artırmıştır. 2020'li yılların ilk bölümüne gıda güvenliği, enerji güvenliği, su güvenliği, sağlık güvenliği, tedarik güvenliği ve siber güvenlik endişeleri hakim olmuştur. Pandemi sırasında yaşanmaya başlayan ve Şubat 2022'de patlak veren Rusya-Ukrayna Savaşı ile daha da ağırlaşan uluslararası tedarik zincirindeki aksamalar, ülkeleri, stratejik ihtiyaçlarının karşılanmasında dışa bağımlılıklarını hızla azaltma arayışlarına teşvik etmektedir.

Birçok ülke kritik altyapılarını ve endüstrilerini güçlendirmek ve var olan sektörlerini daha sıkı korumak için harekete geçmiştir. Örneğin, pek çok ülke, yurtdışında üretim yapan şirketlerini yatırımlarını ülke içine kaydırmaya teşvik ederken, ülke içinde sanayi ve hizmetlerin verimini artırabilmek için dijitalleşmeye de ağırlık vermeye başlamıştır. Pandemi süreci uzaktan çalışma, e-eğitim ve e-sağlık gibi pratiklerin artması, eskisinden daha karmaşık ve daha yoğun siber saldırıları da beraberinde getirmektedir. Bu karmaşık ve sert güvenlik ortamında kritik altyapıların güvenliği daha büyük önem arz etmektedir.

Dünyada ve Türkiye'de kritik altyapıların mevcut durumunu ve temel eğilimlerini aktarmak; söz konusu altyapılara yönelik tehditleri irdelemek ve bunları bertaraf etmek maksadıyla geliştirilen çözüm önerilerini sunmak için başlattığımız Araştırma Raporu yazı dizimizin ikinci bölümünde; ulaştırma, haberleşme ve bilişim teknolojileri sektörlerinin kritik altyapıları ele alınacaktır.

2. KRİTİK ALTYAPI PERSPEKTİFİYLE TÜRKİYE'NİN ULAŞTIRMA ALTYAPISI

Güvenlik, tarih boyunca insanların en önemli ihtiyaçlarından biri olmuştur. Güvenliğin sağlanması gereken alanlardan biri ulaşım ağları ve altyapılarının güvenliğidir. İnsanlar tarih boyunca ihtiyaçlarını daha uygun koşullarda sağlayabilmek ve kendileri ile eşyalarını bir yerden başka bir yere daha kısa sürede, düşük maliyette ve her şeyden önce güvenli bir biçimde ulaştırmayı amaçlamışlardır. Bu nedenle ulaşım sektörü birçok ülkede kritik altyapılar kapsamında ele alınmaktadır. Türkiye'de kritik altyapılar; Siber Güvenlik Kurulu'nun 20 Haziran 2013 tarih ve 2 sayılı kararına göre elektronik haberleşme, enerji, bankacılık ve finans, kritik kamu hizmetleri, ulaştırma ve su yönetimi olarak belirlenmiştir[1].

Kritik altyapıların artan iletişim ihtiyacını ağ ve internet bağlantıları ile karşılaması, bu kurumları siber saldırılara her geçen gün daha açık hâle getirmektedir.

Bu bölümde ulaşım güvenliğinin kavramsal çerçevesi, günümüzde ve gelecekte ulaşım alanında ortaya çıkabilecek tehditler, Türkiye'nin kritik ulaşım altyapısının bileşenlerinin mevcut durumu incelenecek, Türkiye'de ulaşım ağının güvenliğinin artırılması için atılması gereken adımlara ilişkin öneriler değerlendirilecektir.

2.1 Ulaşım Altyapısı ve Ağlarının Güvenliğine Yönelik Tehditler

Ulaşım sistemlerinin güvenliği ilk çağlardan beri güvenliğin başlıca meselelerinden biri olmuştur. Doğal afetler, kazalar, korsanlar ve eşkıyalar ulusal ve uluslararası

ticaretin en büyük düşmanları olmuşlardır. Modern devletlerin ortaya çıkışı, modern ulaşım ağları ve ulaşım araçlarının yaygınlaşmasıyla ulaşımda geleneksel tehditler önemli ölçüde bertaraf edilse de yeni tehditler ortaya çıkmıştır.

Ulaşımda, taşıma türlerine (karayolu, demiryolu, denizyolu ve havayolu) göre tehditler farklılıklar göstermekle birlikte tehditleri, kasıtsız ve kasıtlı olarak tasnif etmek mümkündür.

2.1.1 Kasıtsız Tehditler

- **Doğal Felaketler ve Şiddetli Hava Olayları:** Depremler, seller, toprak kaymaları ulaşım altyapılarına zarar verirken aşırı yağışlar, şiddetli fırtınalar, kar ve kum fırtınaları ulaşımda aksamalara yol açmanın yanı sıra ulaşım yapı ve araçlarına ciddi maddi hasar verebilmektedir. Küresel iklim değişikliğiyle birlikte aşırı iklim olaylarında artış yaşanacağı, bunun taşımacılık altyapısı ve operasyonlarına olumsuz etkilerinin olacağı belirtilmektedir[2]. Sadece 2021 yılında aşırı iklim olaylarının 1,5 milyar dolar zarara yol açtığı tahmin edilmektedir.
- **Pandemiler**: Pandemiler, salgının yayılmasını ve sağlık sistemlerinin aşırı iş yükü altında ezilmesini önlenmek için alınan tedbirler (sınırların kapatılması, seyahat yasakları, karantinalar, sokağa çıkma yasakları vb.) nedeniyle ekonominin her alanında olduğu gibi taşımacılık sistemlerinin faaliyetlerinde de sert düşüşlere neden olmaktadır. Nitekim COVID-19 pandemisi sırasında hareketlilikte azalmanın ulaşım sektörü üzerinde olumsuz etkileri olmuştur. Küresel olarak, doğrudan havacılık işleri potansiyel olarak yüzde 43 ve toplam havacılık destekli işler, COVID öncesi seviyelere göre yüzde 52,5 oranında düşmüştür[3]. Pandemide, denizyolu taşımacılığında konteyner kiralama fiyatları en az beş kat artarken[4], karayolu yük ve yolcu taşımacılığının pandeminin etkili olduğu iki yılda kaybı iki trilyon doları bulmuştur[5]. İstanbul'da Mart 2020'de pandemi nedeniyle toplu taşımacılığın şehir içi yolculuğundaki payı yüzde 42'den yüzde 20'ye kadar düşmüştür[6]. COVID-19 pandemisi sürerken bilim insanları pandemilerin sıklığının artacağı[7] ve hatta aynı anda birden fazla pandemi görülebileceği uyarısında bulunmaktadır[8].
- **Protesto Eylemleri ve Grevler:** Çevresel, sosyal ve ekonomik nedenlerden kaynaklanan protesto gösterileri, eylemler ve grevler ulaştırma faaliyetlerini kesintiye uğratma veya geciktirme potansiyeline sahiptirler ve sürecin kötü yönetilmesi aksamaların uzamasına ve eylemlerin daha da pahalıya mal olmasına neden olabilir. Nitekim Fransa'da Kasım 2018'de başlayan ve ulaşım ağında sık sık kesintilere neden olan "Sarı Yelekliler" eylemlerinin 2018 yılı sonunda ülkenin ekonomik büyümesini 0,2 puan düşürdüğü tahmin edilmektedir[9].
- **Kazalar:** Hava, deniz ve demiryolunda kazalar alınan katı önlemler sayesinde önemli ölçüde azalmakla birlikte, karayolu kazaları dünyada önemli bir sorun olmaya devam etmektedir. Birleşmiş Milletler (BM) tahminlerine göre karayolu kazalarında yılda ortalama 1,3 milyon kişi yaşamını yitirmektedir[10].
- **Navigasyon Sistemlerinde Doğal Nedenli Kesintiler:** Güneş patlamaları ve güneş fırtınaları küresel konumlandırma uydu sistemleriyle (GNSS) bağlantılarda kesintiye yol açabilir. Bu da hassas konum bilgilerinin kaybolmasına, süre kaybına ve teslimat gecikmelerine yol açabilir.

2.1.2 Kasıtlı Tehditler

- **Savaşlar ve İç Çatışmalar:** Bir ülkenin taraf olduğu savaşlar, iç savaşlar ve büyük toplumsal kargaşalıkların yanı sıra, yakın çevresindeki çatışmalar ulusal ve uluslararası ulaşım bağlantılarını doğrudan olumsuz etkilemektedir. Çatışan taraflardan birine veya hepsine uygulanan yaptırımlar da ulaşımı olumsuz etkilemektedir. Çatışan tarafların liman, havalimanı ve transit karayollarının kapanması, bunlardan yararlanan üçüncü tarafları alternatif çözümlere yönlendirmektedir. Örneğin Bosna Hersek ve Kosova savaşları 90'lı yıllarda Türkiye'nin Avrupa'ya yönelik ihracat taşımalarında büyük aksamalara yol açmış, kamyonlar Ro-Ro gemileriyle İtalya üzerinden Batı Avrupa'ya ulaşmak zorunda kalmıştır. Daha sonra Suriye iç savaşı ve yakın zamanda Ukrayna-Rusya Savaşı karayolu taşıma şirketlerini, Ortadoğu, Kuzey Afrika ve Rusya'ya taşımalarda Ro-Ro taşımacılığına yönlendirmiştir[11].
- **Terörizm**: Ulaşım araçları ve ulaşım sistemlerine yönelik terör saldırıları, uluslararası barış ve güvenlik için ciddi bir tehdit oluşturmaktadır. Terörist gruplar, savunmasız hedefler olarak uçakları, gemileri ve diğer ulaşım araçlarını hedef almaktadır. Terörist gruplar, uçakları ve gemileri kaçırmakta, karayolu ve köprüleri bombalamakta, demiryolu terminallerini hedef almaktadır. Küresel Terörizm Veritabanı'na göre[12], 1970'li yılların başından bu yana terör grupları 1.447 kez havaalanları ve hava taşıtlarını, 410 kez limanları ve ticari gemileri, 7.245 kez de diğer taşımacılık altyapı ve araçlarını hedef alan terör saldırıları düzenlemişlerdir. Ayrıca, ABD'de 11 Eylül 2001 tarihinde düzenlenen büyük terör saldırısında olduğu gibi bu tür saldırıları gerçekleştirmek için ulaşım araçlarını da silah olarak kullanabilmektedirler.
- **Hırsızlık**: Taşımacılık altyapısı suçlular ve suç örgütlerinin hedefindedir. Söz konusu kişi ve gruplar, ulaşım ağlarının takibi için büyük önem taşıyan kameralar, kablolar, sensörler ve diğer hassas ekipmanları çalmakta veya zarar vermekte, yük kamyonları ve vagonlarla taşınan yüklerini gasp etmektedirler. Avrupa Birliği (AB) tarafından yapılan bir araştırmaya göre, yük ve kamyon hırsızlıkları milyonlarca avro zarara yol açmaktadır. Sadece 2020 yılının ilk yarısında 85 milyon avro tutarında hırsızlık yapılmıştır[13].
- **Kötücül Saldırılar ve Siber Suçlar**: Suç şebekelerinin fidye elde etmek amacıyla gerçekleştirdiği siber saldırılar hayatın her alanında olduğu gibi ulaştırma

alanını da etkilemektedir. Saldırılar tüm ulaşım türlerinde aksamalara yol açmakta, işletmelerin hassas bilgileri ele geçirilmekte, ulaşımın bilişim altyapısında milyonlarca dolarlık hasara yol açmaktadır. Örneğin, 2017 yılında Danimarka merkezli uluslararası denizcilik ve lojistik şirketi Maersk'e yapılan siber saldırıda, şirket yaklaşık 17 saat süreyle sistemlerini kullanamamış ve saldırı 300 milyon dolara yakın zarara yol açmıştır[14]. Yine 2021'in Temmuz ayında İran'da bir demiryoluna yapılan siber saldırıda insanların demiryolu seyahatleri etkilenmiştir[15]. Şubat 2022'de patlak veren Rusya-Ukrayna Savaşı'nda geri planda büyük bir siber savaş yürütüldüğü ve bundan ulaştırma sektörünün de etkilendiği belirtilmektedir[16]. Türkiye'de de ulaşım güvenliğine yönelik siber sadırılar olmaktadır. 2009 yılında Atatürk Havalimanı'nda bilet ve bagaj işlemleri Conficker solucanı tarafından bir süre engellenmiştir. 25 Temmuz 2013'te Emniyet Genel Müdürlüğü bilgisayarlarına yapılan siber saldırı sonucu Atatürk Havalimanı ve Sabiha Gökçen Havalimanı'nda, 6 Mart 2018'de ise yine Emniyet Genel Müdürlüğü bilgisayarlarına yapılan siber saldırı sonucu Atatürk Havalimanı'nda pasaport kontrolleri yapılamamıştır[17]. Dünya genelinde akıllı ulaşım sistemlerinin artışıyla siber saldırıların daha büyük bir tehdit oluşturacağını tahmin etmek mümkündür.

2.2 Ulaşım Güvenliğinde Temel Yaklaşımlar

Ulaştırma, "İnsan, mal ve hizmetin bir mekândan başka bir mekâna ulaştırılmasının, arzu edilen şartlara göre ayarlanarak, gereği gibi yerine getirilmesi gayesiyle bir araya getirilerek, fonksiyonları ve etkileşimleri organize edilen ilgili tüm iktisadi, sosyal, fiziksel ve kurumsal bileşenler kümesi" olarak tanımlanmaktadır[18]. Ekonomik açıdan ulaştırma, insan ve eşyanın, ihtiyaçları karşılamak bakımından, zaman ve yer avantajı sağlayacak biçimde yer değiştirmesi olarak tanımlanabilir[18]. Ulaştırma sektörü ülkelerin kalkınabilmesi ve ekonomik olarak büyüyebilmesi için büyük önem arz etmektedir. Zira ekonomik sistem, ilgili toplumdaki mal ve hizmetlerin üretimini, bu üretimin dağıtımını ve kaynakların üretime tekrar dahil edilmesini kapsar. Ekonomik sistem içerisinde bu gibi faaliyetlerin yürütülmesi ancak ulaşım sektörü yardımıyla gerçekleşebilmektedir. Ekonomik faaliyetlerin yanında ulaşım sektörü; haberleşme, kültürel ve sosyal nedenlerle de ihtiyaç hâline gelmiştir. Bu kapsamda seyahat etme hakkı anayasal bir hak olarak demokratik ülkeler tarafından vatandaşlarına tanınmıştır.

Ulaşım ağı, toplumların refahı ve büyümesi için çok önemlidir. Bir ulaşım ağı kesintiye uğradığında, toplumlar birçok zorlukla karşılaşır. Bu nedenle, siyasi karar alıcılar ulaşım ağının işlevselliğinin aksamamasını sağlamak için güvenlik önlemlerine başvurmaktadır. Kritik altyapı olarak ulaşım ağlarında güvenliğin sağlanması için her şeyden önce stratejik bir öngörüye sahip olabilmek gerekmektedir. Güvenlik yönetiminin asli görevi, güvenliğe yönelik tehdit unsurlarını etkisiz hâle getirmek veya riskleri en aza indirmektir[19].

Gerek Birleşmiş Milletlerin (BM) ilgili kuruluşları[20] gerekse AB[21] ulaşımın insani gelişmişlikteki öneminden ötürü, geleceğin ulaşım sistemlerine ilişkin strateji ve yol haritalarında aşağıdaki bazı temel hedefleri belirlemişlerdir:

- Sürdürülebilirlik,
- Erişilebilirlik,
- Güvenlik,
- Çevre güvenliği,
- Elastikiyet (Resilience)

Söz konusu hedeflerin hepsine birden ulaşmak için bir yandan ulaştırma altyapısının geliştirilmesine yönelik yatırım yapılırken, pek çok ülkede olduğu gibi Türkiye'de de "Akıllı Ulaşım Sistemleri" (AUS) kavramı çerçevesinde temel bir strateji geliştirilmiştir.

AUS hâlen çeşitli alanlarda uygulama bulmakta ve uygulamaların gelecekte daha da yaygınlaşacağı beklenmektedir (Tablo 1). Gelecekte ulaşımda otonomi (sürücüsüz otomobil, otobüs, tren, gemi ve insansız hava araçları), yeşil araçlar (yenilenebilir kaynaklardan elde edilen elektrikle hareket eden araçlar), kombine taşımacılık, daha fazla demiryolu taşımacılığı ve ulaşımın tüm alanlarında dijitalleşmenin hâkim olacağını tahmin etmek mümkündür. Dolayısıyla gelecekte yıkıcı ve yenilikçi teknolojilerin etkisiyle ulaşım sektörünün, dolayısıyla insanların ulaşım anlayışının ve tarzının köklü bir dönüşüme uğraması beklenmektedir. Yapay zekâ, makine öğrenmesi ve otonom araçların etkisiyle ulaşıma ait tüm bileşenlerin tamamen kullanıcı bağımsız hâle gelmesi kaçınılmaz görülmektedir[22].

Akıllı Araçlar	Akıllı Yollar	Akıllı Şehirler
• Akıllı Navigasyon, 360 Derece Çevre Görüşü • Otomatik Park • Otonom Araçlar	• Akıllı Kavşaklar • Yolcu Bilgilendirme Sistemleri • EDS, HGS • Yeşil Dalga Kameralar • Algılayıcılar	• Akıllı Şehir Yönetim Merkezleri • Kaza ve Acil Durum Yönetimi • Toplu Taşıma ve Filo Yönetimi • Akıllı Otoparklar • Güvenli Ulaşım Uygulamaları
Ekonomi ve Çevre	**Entegrasyon ve Sistemler**	**Bilişim ve Güvenlik**
• Akıllı Enerji Sistemleri • Elektrikli Araçlar • Çevreye Duyarlı Ulaşım Altyapısı	• Tüm Ulaşım Türlerinin Entegrasyonu • Ulaşım Kontrol Merkezi • Kooperatif AUS • Tüm Ulaşım İçin Tek Ödeme	• Tüm Ulaşım Verisi Büyük Veri • Veri Güvenliği ve Paylaşımı • Siber Güvenlik • Haberleşme Sistemleri

Tablo 1: Akıllı ulaşım sistemleri uygulamalarından bazıları[22].

2.2.1 Ulaşım Sistemlerinin Elastikiyetinin Artırılması

Ulaşım ağlarına yönelik tehditlerin önemli bir bölümü klasik güvenlik kavramının dışında kalan felaketler ve öngörülmesi güç kazalar veya ihmallerden kaynaklanmaktadır. Bu nedenle ulaşım ağlarında güven göz önüne alındığında, bu kritik altyapıların güvenliğinin sağlanmasında, elastikiyet sağlayacak tedbirler ön plana çıkmaktadır. Elastikiyet, bir sistemin işlevini sürdürme yeteneğini ve büyük bir kesintiden sonra normal duruma dönme hızını ifade eder.

Ulaşım sistemlerinde de fiziksel elastikiyet, ulaşım altyapısının doğal felaketlerden, aşırı iklim olaylarından, pandemi gibi olağanüstü çalkantılı dönemlerden en az hasarla çıkmasını, cana ve mala gelen zararın en aza indirilmesini ve geçim kaynaklarının en kısa sürede eski hâline dönmesinin sağlanmasını ifade etmektedir[23].

Günümüzde ülkelerin ulaşım yatırımları, giderek daha fazla doğal afete ve iklim değişikliği sonucu aşırı iklim olaylarına maruz kalmaktadır. Heyelanlar, sel ve depremler taşımacılık altyapısına büyük zarar vermektedir. Dünyada ulaşım altyapılarının önemli bir bölümü afetler ve iklim olaylarının yarattığı tehditler altındadır. Dünya Bankası tahminlerine göre, küresel karayolu ve demiryolu varlıklarının yaklaşık yüzde 27'si her yıl en az bir afet veya iklim olayı tehlikesine maruz kalmaktadır[24]. Bu nedenle ulaşım altyapısının elastikiyetinin artırılması tüm hükümetler ve yerel yönetimler için önem taşımaktadır.

Ulaşım altyapısının afetler ve iklim olaylarına karşı elastikiyetinin artırılması ek maliyet gerektirmektedir. Örneğin su baskınlarına karşı demiryollarının elastikiyetini artırmak inşaat maliyetini yüzde 50 artırmaktadır[24]. Karayollarına ek drenaj sistemi veya bariyer kazandırmak sermaye yatırımlarını yüzde iki artırabilir. Dünya Bankası'nın 2019 yılı hesaplamalarına göre, dünyada ulaştırma sektörünü elastik hâle getirmek için 2030 yılına kadar her yıl 157 milyar dolar ila 1,1 trilyon dolar harcanması gerekecektir[24].

Buna karşılık, doğal afetler ve aşırı iklim olaylarının taşımacılık sistemlerine maliyeti her geçen gün artmaktadır. Dünya Bankasının tahminine göre afetler ve iklim olayları dünyada yılda 3,1 milyar dolar ila 22 milyar dolar hasara ve ekonomik kayba yol açmaktadır[24]. AB'de yapılan bir araştırmaya göre, aşırı iklim olaylarının taşımacılık sistemlerinde yarattığı zarar (altyapı hasarları, ulaşımda kesintilerin ekonomik maliyeti vb.) yılda 2,5 milyar doları bulmaktadır[24]. Dünyada şehirlerde belediyelerin bakım bütçelerinin yüzde 30-50'si hava olaylarının yarattığı hasarların giderilmesine harcanmaktadır[25].

Ulaştırma sistemlerine elastikiyet sağlanması için harcanması gereken kaynak, tarihsel verilere göre hesaplanan zararlardan yüksek görünmekle birlikte, tüm ulaşım varlıklarının tüm tehlike ve tehditlere karşı dirençli hâle getirilmesi gerektiği unutulmamalıdır. Ülkeler kritik ulaşım varlıklarını belirleyerek sınırlı maliyetlerle bunları dirençli hâle getirebilirler. Yapılacak analizle en önemli taşımacılık altyapısı ve bunların zayıf yönleri ve söz konusu altyapının kesintiye uğramasının diğer sistemler üzerindeki etkisi ve sistemler arası karşılıklı bağımlılık etkisi ortaya konulabilir.

Türkiye gibi gelişmekte olan ülkeler bu afetleri yönetmek, ulaşım sistemlerini planlamak, tasarlamak, inşa etmek, işletmek ve sürdürmek için yeni yaklaşımlar aramaktadır. Dünya Bankası öncülüğünde beş ülkede (Kenya, Laos, Paraguay, Peru ve Sırbistan) yapılan "Taşımacılık sisteminin iklim değişikliği karşısında elastikiyetini artırma" amaçlı proje, bu konuda bir yol haritası sunmaktadır. Proje bağlamında ulaşımda elastikiyeti artırmak için alınacak tedbirler üç başlıkta toplanabilir[26]:

- **Analiz, teknik rapor ve yönerge safhası:** Ulaştırma altyapısında afetler ve iklim değişikliğinden en çok etkilenecek varlıklar belirlenir, felaketlerin yol açabileceği zararlar hesaplanır. Zararların azaltılması veya bertaraf edilmesi için atılması gereken adımlara ilişkin yönergeler oluşturulur.
- **Kapasite artırımı, paydaşlar ve ortaklıkların güçlendirilmesi:** Ulaşım altyapısının güçlendirilmesi sorumluluğuna sahip kurum ve kuruluşlar arasında işbirliği artırılır. Uluslararası işbirliği olanakları araştırılır.
- **Politikalar ve planlar tasarlanması ve hayata geçirilmesi:** Ulaşım ağlarının güçlendirilmesi, bakımı ve yönetimine ilişkin siyasi belgeler ve planlar hazırlanır ve uygulanır.

Dünya Bankasının yol haritasında da altı çizildiği üzere, kritik ulaşım altyapısının elastikiyetinin ve güvenliğinin sağlanması için öncelikle ulaşım varlıklarına ilişkin analizlerin yapılması gereklidir. Analiz için de uzaktan, insan müdahalesi en aza indirgenerek elde edilmiş güncel verilerin toplanması sağlanmalıdır. Söz konusu amaç için son yıllarda gelişmiş teknolojilerden yararlanılarak "Akıllı Ulaşım Sistemleri" ön plana çıkmıştır.

2.2.2 Akıllı Ulaşım Sistemlerinin Tesisi ve Güvenliğinin Sağlanması

Akıllı Ulaşım Sistemleri (AUS); seyahat sürelerinin azaltılması, trafik güvenliğinin artırılması, mevcut yol kapasitelerinin etkin ve verimli kullanılması, hareketliliğin artırılması, enerji verimliliği sağlanarak ülke ekonomisine katkı sağlanması ve çevreye verilen zararın azaltılması gibi amaçlar doğrultusunda geliştirilen kullanıcı-araç-altyapı-merkez arasında çok yönlü veri alışverişi ile izleme, ölçme, analiz ve kontrol mekanizmaları içeren sistemlerdir[22].

Temelinde nesnelerin interneti, gelişmiş sensörler, hassas kameralar, yeryüzü gözlem uyduları, bulut bilişim, bilişim teknolojileri bulunan AUS, toplumun ulaşım ihtiyaçlarını daha güvenli, hızlı, etkin ve verimli şekilde karşılamak için sürekli gelişim ve değişim göstermektedir. Bununla birlikte, farklı alanlardaki teknolojik gelişmeler de ulaşım sektöründe geniş uygulama alanı bulabilmektedir.

Akıllı Ulaşım Sistemleri genellikle karayolu ve demiryolu ulaşım sistemlerinde hayat bulmakla birlikte (Tablo 1), denizyolu ve havayolu taşımacılığında da giderek yaygınlaşmaktadır. Denizyolu taşımacılığında yeni teknolojiler yaygın kullanım alanı bulmaktadır[27]. Otonom veya yarı otonom konteyner terminalleri giderek

yaygınlaşmaktadır. 2025 yılına kadar dünya genelinde 55 tam otonom veya yarı otonom konteyner terminalinin faaliyet göstermesi beklenmektedir. Ayrıca, liman operatörlerinin limanın tüm unsurları hakkında anlık bilgi sahibi olmasını ve öngörüsel analiz yapmalarını sağlarken, operasyonel verimliliği artıran ve güvenliği en üst seviyeye çıkaran "dijital ikiz" teknolojisi de yaygınlaşmaya başlamıştır[28]. Yakın gelecekte insansız kargo gemileri de uluslararası sularda olacaktır. Japonya'da bu tür bir geminin test seferleri sürmektedir[29].

ABD'de 11 Eylül 2001'deki terör saldırılarının ardından zaten en üst seviyeye çıkarılan sıkı güvenlik önlemleri altındaki havayolu taşımacılığında dijital teknolojiler yoğunlukla kullanılmaktadır. Havayolu şirketleri ve havalimanı terminal işletmeleri, yükselen enerji fiyatları ve ek güvenlik tedbirleri nedeniyle artan maliyetlerini hafifletirken, yolcuların havayoluyla seyahat konforunu artırmak için ileri teknolojilerden yararlanmaktadır. Havalimanları, deniz limanları gibi dijital ikiz teknolojisinden yararlanarak işletme maliyetlerini azaltmakta ve güvenlik açıklarını en aza indirmektedir[30].

Ulaşım alanındaki dijitalleşme, kritik ulaşım altyapıları ve varlıklarının daha yüksek farkındalıkla yönetilmesini, operasyon verimliliğini artırılmasını, sera gazı emisyonunun düşürülmesini ve güvenliğin en üst düzeye çıkarılmasını sağlarken, aynı zamanda yeni risklere de yol açmaktadır. Her sektörde olduğu gibi, ulaşımda da daha fazla dijital dönüşüm, daha fazla risk anlamına gelmektedir. Ulaşımda, genellikle geniş coğrafi alanları kapsayan hem fiziksel hem de dijital ağları izleyen, ağ bağlantılı ulaşım sistemleri arasında iletişim kuran geniş bir veri yelpazesi bulunmaktadır. Daha fazla kontrol sistemi ve nesnelerin interneti cihazı çevrimiçi hâle getirildikçe, fiziksel varlıklara zarar verme potansiyelini artıran daha fazla güvenlik açığı ortaya çıkacaktır. Nitekim havayolları ve havaalanı altyapısı, demiryolu altyapısı sahipleri ve operatörleri, lojistik şirketleri ve otomotiv endüstrisi, fiziksel ağları kesintiye uğratma ve büyük kesintilere neden olma potansiyeline sahip siber saldırılara müsaittir.

2020 yılında EasyJet havayolu şirketine yapılan siber saldırıda binlerce şirket müşterisinin kişisel verileri çalınmıştır[31]. Mart 2022'de İtalyan demiryolu şirketleri Trenitalia ve RFI'ye yapılan siber saldırı demiryolu ulaşımının bir gün boyunca tümüyle durmasına neden olmuştur[32]. Şubat 2022'deki büyük siber saldırı Almanya, Belçika ve Hollanda'daki limanlarda petrol terminallerinin operasyonlarını kesintiye uğratmıştır[33]. ABD'li karayolu taşımacılığı şirketi Bay & Bay Transportation, Şubat 2022'de 2018'deki büyük siber saldırıdan sonra ikinci kez fidye amaçlı saldırıya uğramıştır[34].

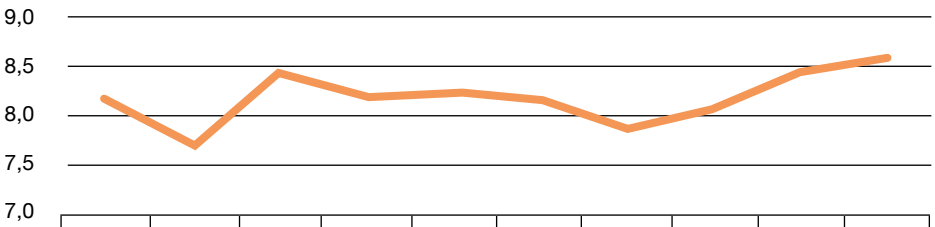
Ulaşımda siber saldırılar daha büyük maliyetler de yaratabilir. İngiltere'nin Cambridge Üniversitesinin Risk Araştırmaları Merkezi tarafından yayınlanan, "Asya Pasifik Limanlarında Siber Risk" başlıklı bir rapora göre, Asya'nın büyük limanlarında kargo veritabanı kayıtlarına bulaşan varsayımsal bir virüs, konteyner trafiğinin durdurulmasına, küresel denizcilik tedarik zincirinin ve yolcu gemisi endüstrisinin durma noktasına gelmesine ve önemli limanların kapatılmasına yol açabilir. Böylesi bir siber saldırının maliyeti 110 milyar doları bulabilir[35]. Daha da kötüsü ulaşım sistemlerine yönelik siber saldırılar büyük can kayıplarına yol açabilir. ABD'li tüketici hakları örgütü Consumer Watchdog'a göre sürücüsüz ve internet bağlantılı araçların sayısının hızla arttığı ABD'de yoğun trafik saatlerinde yapılacak bir siber saldırı yaklaşık 3.000 kişinin yaşamını kazalarda yitirmesine neden olabilir[36]. Bu nedenle akıllı ulaşım sistemlerinin siber güvenliğinin sağlanması büyük önem taşımaktadır.

2.3 Türkiye'de Ulaştırma Sektörünün Genel Görünümü

Ulaştırma sektörü, Türkiye'nin ekonomik büyümesinin temel bileşenlerinden biridir ve bölgeler arası gelişmişlik farkının kapanmasında önemli rol oynamaktadır[18]. Tarihsel veriler Türkiye'de ulaştırma-depolama sektörünün GSYH'de yüzde 8-9 bandında pay aldığını göstermektedir (Şekil 1)[37].

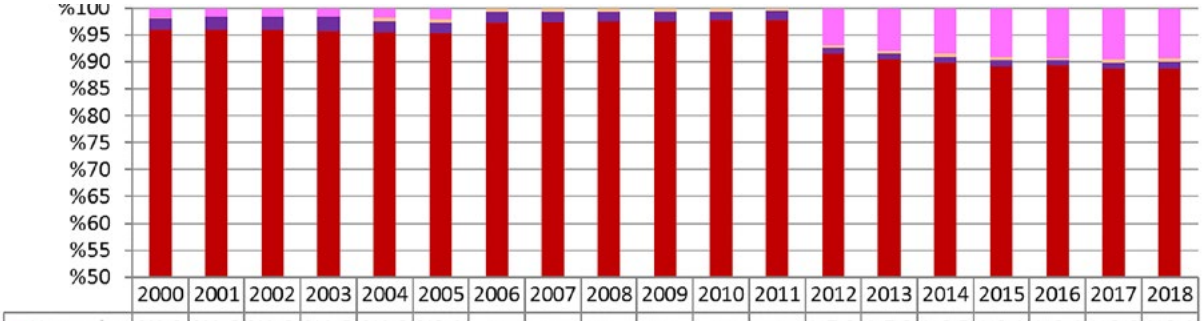
Artan dünya nüfusu, büyüyen küresel ekonomi ve ulaştırma ile ilgili altyapı projelerinin tamamlanması gibi gelişmeler sonucunda sektörün Türk ekonomisindeki payının daha da artacağı beklenmektedir.

Bir ülkenin ulaştırma altyapısı ulaşım ağları, taşıt filoları ve ulaşım işletmeleri bileşenlerinden oluşmaktadır. Ulaştırma sektöründe yer alan bileşenlerin her biri kendi içerisinde karayolu, denizyolu, havayolu, demiryolu, iç suyolları ve boru hattı alt sektörlerinden meydana gelmektedir. Türkiye'de akarsuların debilerinin yüksek olması ve engebeli arazi nedeniyle iç suyolu taşımacılığı ihmal edilebilecek ölçüde yapılmaktadır. Boru hatlarının güvenliği konusu ise enerji güvenliği altında incelenmektedir. Diğer taşıma türlerinin yük ve yolcu taşımacılığındaki payları ise Şekil 2 ve 3 ile Tablo 2'de verilmiştir.



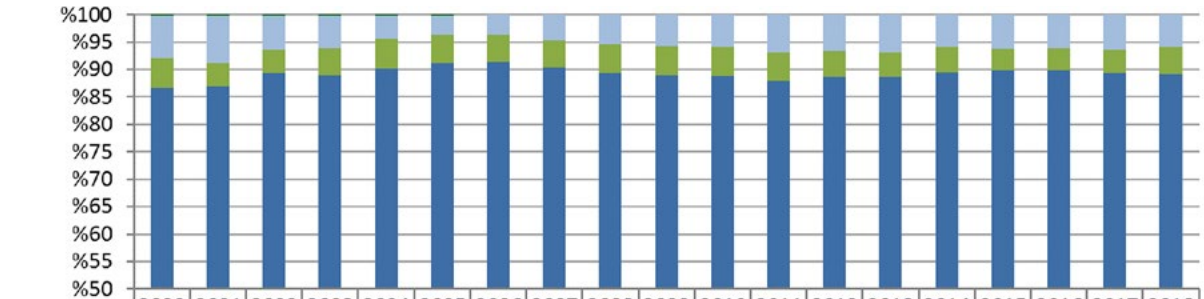
	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
— Ulaştırma ve Depolama'nın GSYH içindeki payı	8,1	7,7	8,4	8,2	8,2	8,2	7,9	8,1	8,4	8,6

Şekil 1: Türkiye'de ulaştırma ve depolamanın GSYH içindeki payı[37].



	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Havayolu	%1,8	%1,6	%1,6	%1,6	%1,8	%2,1	-	-	-	-	-	-	%7,0	%7,9	%8,5	%9,1	%9,4	%9,6	%9,4
Denizyolu	0,03	0,03	0,02	0,02	0,63	0,65	0,72	0,73	0,74	0,75	0,68	0,63	0,52	0,56	0,59	0,56	0,33	0,59	0,56
Demiryolu	%2,2	%2,4	%2,3	%2,7	%2,1	%1,9	%2,0	%1,9	%1,7	%1,6	%1,6	%1,6	%1,1	%1,0	%1,1	%1,1	%1,0	%1,0	%1,2
Karayolu	95,9	95,9	96,1	95,7	95,5	95,3	97,3	97,4	97,5	97,6	97,8	97,8	91,5	90,5	89,8	89,2	89,3	88,8	88,8

Şekil 2: Türkiye'de yurtiçi yolcu taşımalarında taşıma türlerinin aldığı payların 2000-2018 arası seyri[38].



	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Havayolu	%0,2	%0,2	%0,2	%0,2	%0,2	%0,2													%0,0
Denizyolu	%7,8	%8,6	%6,3	%5,8	%4,2	%3,5	%3,6	%4,8	%5,5	%5,8	%5,9	%6,9	%6,6	%6,9	%5,9	%6,3	%6,1	%6,4	%6,0
Demiryolu	%5,3	%4,3	%4,3	%5,1	%5,4	%5,0	%5,0	%4,9	%5,3	%5,2	%5,3	%5,1	%4,8	%4,4	%4,6	%3,9	%4,1	%4,3	%4,8
Karayolu	86,7	86,9	89,3	88,9	90,2	91,3	91,4	90,3	89,3	89,0	88,8	88,0	88,6	88,7	89,5	89,8	89,7	89,2	89,2

Şekil 3: Türkiye'de yurtiçi yük taşımalarında taşıma türlerinin aldığı payların 2000-2018 arası seyri[38].

Şekil 2'de görüldüğü üzere Türkiye'de yurtiçi yolcu taşımacılığında karayolu yolcu taşımacılığı sektörünün payı 2011 yılına kadar yüzde 95'in üzerinde seyretmiştir. Bu tarihten sonra iç hat havayolu taşımacılığına verilen teşviklerin yanı sıra, altyapı ve araçlara yapılan yatırımlar sayesinde havayolu taşımacılığı büyük aşama kaydetmiş ve yolcu taşımacılığında karayolunun payı yüzde 90'ın altına gerilemiştir. Türkiye'de kabotaj yolcu taşımacılığı hizmeti sınırlı olduğu için denizyolu taşımacılığının yolcu taşımacılığındaki payı son derece düşük kalmaya devam ederken, yüksek hızlı tren hatlarının devreye girmesine rağmen demiryolunda yolcu taşımacılığının payı yüzde 1 seviyesine kadar gerilemiştir.

Yurtiçi yük taşımacılığına bakıldığında ise (Şekil 3), karayolu taşımacılığının yüzde 85-90 oranında pay aldığı ve bu dağılımın yıllar içinde çok az değişim gösterdiği görülmektedir.

	Karayolu		Havayolu		Denizyolu		Demiryolu	
Yıl	**İthalat**	**İhracat**	**İthalat**	**İhracat**	**İthalat**	**İhracat**	**İthalat**	**İhracat**
2010	5,10	24,32	0,09	0,74	94,07	74,01	0,74	0,93
2011	4,47	24,22	0,07	0,97	94,75	73,84	0,70	0,97
2012	3,98	22,54	0,06	0,99	94,38	75,83	0,59	0,63
2013	4,11	24,25	0,07	1,03	94,27	74,38	0,55	0,35
2014	3,89	24,04	0,07	1,12	94,60	74,41	0,45	0,42
2015	3,73	24,68	0,07	1,15	94,76	73,69	0,45	0,49
2016	3,72	24,49	0,06	0,81	94,78	74,19	0,43	0,52
2017	4,00	22,12	0,06	0,81	94,56	76,49	0,37	0,58
2018	4,05	20,44	0,05	0,83	94,48	78,25	0,42	0,48
2019	4,34	17,59	0,06	0,87	94,12	81,09	0,49	0,45
2020 (3 Çeyrek)	4,04	16,19	0,04	0,35	94,35	82,84	0,56	0,62

Tablo 2: Türkiye'nin dış ticaret taşımalarının taşıma türlerine göre dağılımı (2010-2020)[39].

Uluslararası yük taşımacılığına bakıldığında ise denizyolu nakliyesinin ağırlığı göze çarpmaktadır. Türkiye'nin ithalatının yüzde 95'ine yakını, ihracatının ise yaklaşık yüzde 75-80'i denizyoluyla yapılmaktadır (Tablo 2). Karayolu taşımacılığı sektörü ise ithalatta önemsiz bir paya sahipken ihracat yükünün yaklaşık beşte birini taşımaktadır. Türkiye'nin ithalat ve ihracatında demiryolu ve havayolu taşımacılığı ise son derece sınırlı bir pay almaktadır.

Bu verilerden yola çıkarak, Türkiye'de yolcu taşımacılığında karayolu ve havayolu, yük taşımacılığında ise karayolu ve denizyolu altyapılarının kritik önem arz ettiği söylenebilir.

2.3.1 Türkiye'de Karayolları Sektöründe Mevcut Durum

Karayolu taşımacılığı, başlangıç ve varış noktaları arasında aktarmasız bir taşımaya olanak sağlaması, öteki taşıma türlerine kıyasla daha hızlı olması ve özellikle kısa mesafeli taşımalarda nispeten ucuz olması nedeniyle bazı avantajlara sahiptir. Buna karşılık, karayolu taşımacılığının birim taşımada gerek yolcu/km gerek ton/km maliyeti, tükettiği enerji miktarı, kullandığı enerji türü, yol açtığı çevre kirliliği, yüksek kaza riski ve özellikle uluslararası siyasi ve ekonomik konjonktürde meydana gelen gelişmeler karşısında göreceli olarak hassas ve kırılgan bir yapı arz etmesi nedeniyle, bazı dezavantajları da bulunmaktadır. Ayrıca sektör, başta yoğun rekabet ve yükselen petrol fiyatları nedeniyle artan maliyet giderleri olmak üzere, kendi içinde bazı zorluklarla karşı karşıya bulunmaktadır.

Türkiye'de karayolu ağırlıklı bir ulaşım ağı bulunmaktadır. Bunun nedeni 1950'li yıllardan bu yana Türkiye'de karayollarının gelişiminin, ulaşım politikalarının ana eksenini oluşturmasıdır. 2000'li yıllara kadar karayolu ağının genişletilmesine odaklanırken, bu tarihten sonra, karayolları üzerindeki yük ve yolcu trafiğinin baskısının trafik kazalarını artırması nedeniyle "bölünmüş yol" yapımı ulusal bir politikaya dönüşmüş ve mevcut karayollarında iyileştirmeler yapılmıştır.

Bu çalışmalar sonucu 2003 yılında 6.000 km olan bölünmüş yol uzunluğu Ocak 2022 itibariyle 27.000 km'nin[41] üzerine çıkmıştır. Türkiye karayolu ağı üzerinde toplam uzunluğu 651 km'ye ulaşan karayolu tüneli[42], ve toplamda 500.000 m uzunluğunda köprü[43] bulunmaktadır. Söz konusu kritik karayolu yapıları arasında İstanbul Boğazı üzerinde üç, İzmit Körfezi'nde bir ve Çanakkale Boğazı'nda bir olmak üzere beş adet asma köprünün yanı sıra, 14,6 km'lik Avrasya Tüneli de bulunmaktadır. Toplam 14,3 km uzunluğu ile Avrupa'nın en uzun çift tüplü tüneli, dünyanın en uzun altıncı karayolu tüneli olan Ovit Tüneli, Türkiye'nin kuzey- güney karayolu koridorunda stratejik öneme sahiptir. Ovit Tüneli'nden biraz daha uzun olan Yeni Zigana Tüneli'nin ise 2022 yılında kaba inşaatının bitmesi hedeflenmektedir[44]. Devreye giren ve girecek projelerle Türkiye'nin Çin'den Avrupa'ya uzanan Orta Koridor'un yanı sıra TEM, TEN-T, TRACECA ve ESCAP gibi uluslararası karayolu ağlarındaki[45] önemi bir kat daha artacaktır.

Yıllar	Devlet Yolu	Otoyol	İl Yolu	Toplam
2003	31,358	1,753	30,133	63,244
2008	31,311	1,922	30,712	63,945
2013	31,341	2,127	32,155	65,623
2018	31,021	2,842	34,153	68,376
2019	31,006	3,060	34,165	68,231
2020	30,974	3,523	34,136	68,633

Tablo 3: Türkiye Otoyol, Devlet Yolu, İl Yolu Toplam Uzunlukları (Km)[40]

Karayolu üstyapısına bakıldığında ise Türkiye'de yetki belgesine sahip 500.000'e yakın kişi veya şirketin, kayıtlı yaklaşık 1,4 milyon araçla karayolunda yük ve yolcu taşımacılığı yaptığı görülmektedir[46]. Söz konusu araçların 1,3 milyonu yük araçları (kamyon, kamyonet, TIR vb.), yaklaşık 86.000'i ise karayolu yolcu araçlarıdır (otobüs, midibüs, minibüs vb.). Türkiye'deki tüm karayolu taşıtların sayısı ise 24,3 milyona yakındır[46]. Türkiye'de kayıtlı 310 yük ve yolcu terminali işletmesi[47], 10 lojistik merkez[48], yaklaşık 1.200 gümrüklü antrepo[49] ve toplamda yaklaşık 15 milyon m^2 depolama kapasitesi[50] bulunmaktadır.

2.3.2 Türkiye'de Demiryolu Taşımacılığının Mevcut Durumu

Demiryolu taşımacılığı; konfor, hız, çevre ve emniyet açılarından güvenilir, sürdürülebilir ve verimli bir seçenek olarak ön plana çıkmaktadır. Demiryolu, ulaşımda toplu taşıma sağlamasının yanında, kullandığı yolda sürtünmenin az olması nedeniyle de diğer sistemlere göre daha düşük enerji tüketimi sağlamaktadır. Dolayısıyla uzun mesafelerde karayolu araçlarına göre yüzde 10 ila 40 oranında daha ekonomiktir[51]. Demiryolu taşımacılığında karayolu taşımacılığına göre yüzde 75 daha az sera gazı emisyonu[52] gerçekleşmektedir. Bunun yanı sıra uygun şekilde güvenilir ve konforlu seyahat imkânı sağlar. Demiryolu ile ulaşım, ölüm ve ağır yaralanma riski açısından karayolunda otomobil ile seyahat etmekten 24 kat daha güvenlidir[53].

İlk yatırım maliyeti diğer taşıma türlerine göre daha yüksek olmasına rağmen dünya genelinde demiryolu yatırımları, artan bir şekilde devam etmektedir. Avrupa Demiryolları Endüstrileri Birliğinin (UNIFE) çalışmasına göre, dünya demiryolu pazarının ortalama yüzde 2,3 yıllık büyüme ile 2016-2021 yılları arasında ortalama yıllık 185 milyar avro değerine ulaşacağı tahmin edilmiştir[53]. Söz konusu eğilimde demiryolu taşımacılığının diğer faydalarının yanı sıra bölgeler arası gelişmişlik farklarını azaltıcı etkisi de rol oynamaktadır.

Dünyada demiryolu yatırımlarına en çok pay ayıran ülke Çin'dir. Çin'de hızlı demiryolu ağı 2021 yılı sonu itibarıyla 40.000 km'yi aşmıştır[54]. Çin'in sahip olduğu hızlı demiryolu ağı, AB ülkelerindeki toplam hızlı demiryolu ağının dört katından daha fazladır[55]. Çin ayrıca

Avrupa'ya yönelik yük taşımalarında denizyolundan sonra en çok yük trenleri kullanmaktadır. 2016'da başlayan düzenli Çin-Avrupa yük treni seferleri, 15.000'i 2021 yılında olmak üzere[56] 50.000'den fazla sefer yapmıştır[57]. Ancak söz konusu seferlerin büyük çoğunluğu Rusya üzerinden yapılmakta olup Rusya-Ukrayna Savaşı'ndan büyük ölçüde etkilenmiştir. Çin'in yük trenleri için Orta Asya ülkeleri ve Türkiye üzerinden geçen "Orta Koridoru" daha fazla kullanmayı planladığı kaydedilmektedir[58]. Daha önce yapılan deneme seferleri, Çin trenlerinin Rusya rotasına kıyasla 12 gün gibi kısa bir sürede İstanbul'a ulaşabildiğini göstermiştir[59]. Bu nedenle Türkiye'nin bu yoğun yük treni hareketinden yararlanma olasılığı artmaktadır. Bakü-Tiflis-Kars demiryolu ve Marmaray'ın ardından Yavuz Sultan Selim Köprüsü'nde planlanan demiryolu hattının devreye girmesi, Türkiye'nin demiryolu koridoru niteliğini pekiştirecektir.

Türkiye'nin uluslararası kritik demiryolu koridoru olma potansiyeli artarken ülke içinde demiryolu, yük ve yolcu taşımacılığı ulaşımda oldukça düşük oranlarda pay almaktadır. Bunda en önemli etken demiryolu ağının yeterince geniş olmaması ve demiryolu altyapısındaki çeşitli yetersizliklerdir. Hâlen Trabzon ve Antalya gibi önemli liman kentlerinin demiryolu erişimi bulunmamaktadır. Demiryollarının yarıya yakını sinyalsiz (yüzde 49) ve elektriksizdir (yüzde 55)[60].

Türkiye'de demiryolu yatırımları İkinci Dünya Savaşı sonrasında önemli ölçüde azalmıştır. Türkiye'de 1923-1950 yılları arasında ortalama 3.764 km demiryolu hattı yapılıp işletmeye açılmışken, karayolu ağırlıklı politikaların izlenmeye başlandığı 1950-2002 yılları arasında sadece 945 km demiryolu hattı yapılabilmiştir[61]. 2002 yılında yaklaşık 11.000 km olan demiryolu uzunluğu 2021 yılında 12.803 km'ye[46] ulaşırken, söz konusu artışta yeni inşa edilen yüksek hızlı ve hızlı hatların devreye girmesi etkili olmuştur. 2002-2021 döneminde sadece yaklaşık 600 km konvansiyonel hat inşa edilirken, 1.213 km yüksek hızlı ve hızlı hat inşa edilmiştir[46]. Buna karşılık 11.022 km hattın komple bakım ve yenilemesi yapılmıştır. Bu durum Türkiye'nin 2000'li yıllarda demiryolu altyapısında yeni hat inşasından çok, mevcut hatların modernizasyonuna ve yüksek teknolojili hat inşasına yöneldiğine işaret etmektedir. Söz konusu dönemde elektrikli hat uzunluğu yüzde 175, sinyalli hat uzunluğu ise yüzde 173 artırılırken, demiryolu seyahat sürelerini uzatan hemzemin geçit sayısı yüzde 44 azaltılmıştır. Demiryolu ağındaki tünel sayısı 2002'ye kıyasla yüzde 10 artışla 837'ye, demiryolu tünellerin toplam uzunluğu ise yüzde 56 artışla 281 kilometreye çıkarılmıştır[46]. Türkiye'de 200 kadar gar ve istasyon[62], 12 adet demiryolu lojistik merkezi ve üç adet raylı sistemler fabrikası[63] faaliyet göstermektedir.

Yapılan iyileştirmelerin ardından demiryolu ile yük ve yolcu taşımacılığında önemli ölçüde ilerleme kaydedilmiş, 2002-2020 döneminde demiryoluyla seyahat eden yolcu sayısı yüzde 103, taşınan yük miktarı ise yüzde 136 artmıştır[46]. Söz konusu dönemde Marmaray devreye girmiş ve Avrupa'dan Asya'ya kesintisiz demiryolu seyahati sağlanmıştır. Marmaray'ın projesine paralel olarak Bakü-Tiflis-Kars Demiryolu projesi 2017'de hayata geçirilmiş, Avrupa'dan Çin'e demiryoluyla kesintisiz yük taşınması mümkün hâle gelmiştir[60].

Türkiye'de 2000'li yıllarda şehir içi raylı sistemler (metro, tramvay ve füniküler sistemler) alanında da aşama kaydedilmiş, 14 kentte toplam uzunluğu 500 km'yi aşan raylı sistemlerle yolcu taşımacılığı yapılmaya başlanmıştır[60]. Ulaştırma ve Altyapı Bakanlığının 2018 yılında yayınladığı, "Ulaşan ve Erişen Türkiye 2018 - Demiryolu" belgesinde 2023-2035 yılları arasında 6.000 km ilave hızlı demiryolu yapılması ve demiryolu ağının 31.000 km'ye çıkartılması ve demiryolu taşımacılığının tüm taşıma türleri arasında yüzde 20, yolcu taşımacılığında ise yüzde 15 paya ulaştırılmasının hedeflendiği belirtilmektedir[64].

2.3.3 Türkiye'de Denizyolu Taşımacılığının Mevcut Durumu

Denizyolu taşımacılığı tarihin ilk çağlarından beri en etkili taşımacılık türlerinden biri olmuştur. Denizyolu; sınır aşımı olmaksızın ulaşım kolaylığı, en güvenli taşıma şekli olması, bir defada en büyük miktardaki yükü en çabuk şekilde ulaştırması ve bunların avantajlarının oluşturduğu ucuzluk nedeniyle en çok tercih edilen ulaşım şeklidir. Günümüzde yolcu taşımacılığındaki önemi azalmış olmakla birlikte özellikle uluslararası yük taşımacılığında önemli bir paya sahiptir. Uluslararası denizcilik, küresel ticaretin yüzde 80'inden fazlasını taşımaktadır[65]. Denizyolu taşımacılığı, çoğu mal için uluslararası nakliyenin en verimli ve uygun maliyetli yöntemidir. Demiryoluna göre 3,5, karayoluna göre 7 ve havayoluna göre 22 kat daha ucuz olması denizyolu taşımacılığının en önemli avantajıdır[66].

Günümüzde küresel anlamda denizcilik sadece bir taşıma türü olmaktan çıkmış, dünya ticaret hacmindeki artış ve hızla gelişen teknolojilere paralel olarak yük ve yolcu taşımacılığı başta olmak üzere, gemi inşa sektörü, liman hizmetleri, turizm, canlı ve cansız doğal kaynakların yönetimini kapsayan birendüstri, ticaret ve hizmet dalına dönüşmüştür.

2020'nin başında, toplam dünya filosu, toplam kapasitesi 2,06 milyar dedveyt tonu* bulan 98.140 adet ticari gemiye ulaşmıştır. 2019 yılında, küresel ticari denizcilik filosu yüzde 4,1 oranında büyüyerek 2014'ten sonra ulaşılan en yüksek büyüme oranını yakalamıştır[67]. 8.400 km'den fazla olan doğal kıyı uzunluğu ile Avrupa ile Asya arasında bir köprü konumunda olan, İstanbul ve Çanakkale gibi stratejik noktaların kontrolünü elinde tutan Türkiye, denizcilik açısından yüksek potansiyele sahiptir. Ancak Türkiye, denizcilik sektörünün potansiyelini tam anlamıyla kullanmamaktadır. Yine de Türkiye'de denizyolu taşımacılığı, ithalat ve ihracatta yük taşımacılığında en çok kullanılan (Tablo 2) yöntemdir.

Türkiye'nin denizcilik altyapısında son 20 yılda önemli gelişmeler yaşanmıştır. Türk sahipli 1.000 groston ve üzeri ticari gemi sayısı yüzde 16 artışla 568'den 1.484'e, filonun toplam tonajı ise yüzde 216 artışla 9,3 milyon dedveyt tondan, 29,35 milyon dedveyt tona çıkmıştır[46].

***Dedveyt Ton:** Uluslararası deniz ticaretinde kullanılan bir ağırlık ölçü birimidir (dwt). Kökeni, ölü ağırlık anlamına gelen (deadweight long tons/metric tons) İngilizce terimden gelmektedir.

Türkiye dünyanın 15'inci en büyük deniz filosuna sahiptir. Türkiye'de çeşitli kapasitelerde ve donanımda 50 kadar büyük limanda elleçlenen* yük miktarı 2004'te 57,34 milyon ton iken, 2020 yılında bu miktar 138,9 milyon tona çıkmıştır. Aynı dönemde ithalat elleçlemeleri yüzde 88 artışla 226,54 milyon tona yükselmiştir. Liman faaliyetlerindeki çarpıcı gelişmelerden biri yüzde 496 artışla konteyner elleçlemelerinde yaşanmıştır[46].

Son 20 yılda Türkiye'nin gemi inşa sektöründe de çarpıcı bir büyüme olduğu görülmektedir. Tersane sayısı 37'den 84'e çıkarken, toplam tersane kapasitesi 550 bin dedveyt tondan 4,65 milyon dedveyt tona yükselmiştir[46]. Yaklaşık 30.000'i tersanelerde olmak üzere Türk denizcilik sektöründe istihdam edilenlerin sayısı 200.000'in üzerindedir. Buna karşılık denizyolu ile kabotaj yük ve yolcu taşımacılığı Türkiye'de istenilen seviyede değildir.

2.3.4 Türkiye'de Havayolu Taşımacılığının Mevcut Durumu

Dünya'da en son ortaya çıkmasına rağmen en hızlı gelişme kaydeden taşımacılık türü havayolu taşımacılığıdır. Özellikle yolcu taşımacılığında ulaşım süresi ve konfor açısından rekabetsiz bir konuma sahip havayolu taşımacılığında 2018 yılı itibariyle tüm dünyada 1.397 havayolu, 25.000 ticari uçak, 3.864 havalimanı, 173 hava trafik kontrol hizmet ünitesi ile 4 milyar yolcu, 60 milyon ton kargo taşınmış ve 63 milyon kişilik istihdam yaratılmıştır[68].

Diğer taşıma türlerine kıyasla katbekat pahalı olmasına rağmen havayolu taşımacılığı, hız ve konfor açısından diğerlerinden üstündür. Ne var ki havacılık sektörü, ekonomik, siyasi ve çevresel etmenlere; diğer taşıma türlerine kıyasla daha duyarlıdır. Dolayısıyla havayolları ulaşım ağı ve güvenliği diğer ulaşım türlerine göre daha hassastır.

Dünyadaki gelişmelere paralel olarak Türkiye'de de havacılık sektörü son 20 yılda büyük aşama kaydetmiştir. 2002-2022 döneminde sivil hava trafiğine açık havaalanı sayısı iki kattan fazla artarak 26'dan 56'ya, Türkiye merkezli havayollarının uçak sayısı iki buçuk kattan fazla artarak 150'den 552'ye; havayolu kargo kapasitesi üç kattan fazla artarak yaklaşık 25.000'den yaklaşık 105.000'e, hava kargo kapasitesi ise yedi kattan fazla artarak 303 tondan yaklaşık 2.450 tona çıkmıştır[46]. Türkiye'nin havayolu şirketleri yurtdışında uçtukları nokta sayısını yaklaşık dört buçuk kat artırmış, 2018 yılı son çeyreğinde hizmete açılan 150 milyon yolcu kapasiteli İstanbul Havalimanı ile İstanbul, dünyanın sayılı transit merkezlerinden biri hâline gelmiştir. Türkiye'nin havayolu sektörünün cirosunu 44 kattan daha fazla, istihdamını ise dört kattan fazla artırmıştır. Türkiye'de COVID-19 pandemisi öncesi havayolu taşımacılığı sektöründe çalışanların sayısı 300.000'e yaklaşmıştır.

Bu büyük canlanma taşınan yolcu sayısında patlamaya yol açmıştır. İç hatlarda taşınan yolcu sayısı 8,73 milyondan yaklaşık 50 milyona, dış hatlarda taşınan yolcu sayısı ise 25 milyondan 32 milyona çıkmıştır. Türkiye taşınan yolcu sayısı itibarıyla Avrupa'da dördüncü, dünyada ise 10'uncu sıraya yükselmiştir[46]. Bu hızlı gelişmenin yanında ülkemizin stratejik konumu, altyapı yatırımları ve havacılık teknolojilerindeki gelişmeler Türk sivil havacılığının sahip olduğu büyüme potansiyelini artırmaktadır.

2.4 Türkiye'de Kritik Ulaştırma Altyapısının Güvenliğine İlişkin Düzenlemeler

Türkiye'nin ulaşımda kritik altyapılara ilişkin özel bir stratejik planı bulunmasa da farklı belgeler ve düzenlemelerde bu konu ele alınmıştır. Örneğin 2020 yılında açıklanan "Türkiye Ulaştırma Politika Belgesi"nde[69] ulaşım güvenliğinin sağlanması için bazı temel politikaların altı çizilmiştir:

- Emniyet ve güvenlik amacıyla kamu ve özel kurumların taşımacılık verilerine erişimi kurallara bağlanarak sağlanır.
- Tüm taşımacılık türlerinde emniyet ve güvenliği artırma konusunda yapılan çalışmalar desteklenir.
- Serbest ticaret akışını engellemeden güvenli tedarik zincirleri oluşturmak amacıyla "uçtan uca" güvenlik sertifikaları geliştirilir.
- Hareketlilik planlarının hazırlanmasında potansiyel dış saldırıların etkileri dikkate alınır.
- Terörizm ve korsanlık gibi diğer suç faaliyetlerine karşı mücadelede uluslararası işbirlikleri artırılarak sürdürülür.
- Farklı taşıma türleri arasında birlikte çalışabilirliği sağlamak için tehlikeli malların çok modlu (en iyi verimin alınabilmesi için varış noktasına kadar birden fazla taşıma türünün kullanıldığı yük ve yolcu seyahatleri) taşımacılığına yönelik kurallar sürekli iyileştirilir.

Yine Ulaştırma Bakanlığı tarafından hazırlanıp 5 Nisan 2022'de yayınlanan "2053 Ulaştırma ve Lojistik Ana Planı"nda[70] ise kritik ulaşım varlıklarının güvenliğine ilişkin şu hususlar yer almıştır:

- Raylı sistemlerde sinyalizasyon ve elektrifikasyon çalışmalarını önceliklendirmek suretiyle insan, altyapı, ekipman kaynaklı kazaları sıfıra indirmek hedeflenmeli ve veriler şeffaf bir şekilde halkla paylaşılmalıdır.
- Teknolojik çözümleri kullanarak otonom sürücü, akıllı yollar, esnek, enerji sönümleyen oto korkuluklar vb. seyahat emniyetini artıracak çalışmaların sürekliliği sağlanmalıdır.
- Ulusal toplu taşıma güvenlik master planının geliştirilmesine dönük çalışmalar yürütülmelidir.
- Terörizme ve korsanlık gibi diğer suç faaliyetlerine karşı mücadelede uluslararası işbirlikleri artırılarak sürdürülmelidir.
- Farklı modlar arasında birlikte çalışabilirliği sağlamak için tehlikeli maddelerin çok modlu taşımacılığına yönelik kurallar sürekli iyileştirilmelidir.
- Bilgi teknolojileri ile ilgili sağlanan her türlü hizmet, işlem ve bilgi ile bunların işlenmesi, depolanması ve sunumunda kullanılan sistemlerin gizliliğinin,

* Elleçleme (İngilizcesi Handling): Yükleme-Boşaltma

bütünlüğünün ve erişilebilirliğinin sağlanmasına yönelik çalışmalar yürütülmeli ve gerekli önlemler alınmalıdır.

- Siber güvenliğin sağlanması konusunda bireylerin kurumların, kuruluşların ve tüm paydaşların üzerine düşen sorumlulukları anlayarak bu sorumlulukları yerine getirecek şekilde hareket etmeleri beklenmektedir.

Her iki belgede de ulaşım sistemleri altyapısının geliştirilmesi ve birbirine entegre edilmesi vurgulanmakta, ulaşım altyapısının trafiğin güvenliğinin sağlanmasında dijitalleşmenin ve bilgi güvenliğini sağlamanın öneminin vurgulandığı görülmektedir.

Türkiye'de kritik ulaşım varlıklarının güvenliğinden farklı kurumlar sorumludur. Dijital felaketler dahil olmak üzere doğal afetlerde kritik altyapının korunması ile görevli kurumlar arasında koordinasyon görevi AFAD'a verilmiştir. 1988'de çıkarılan "Sabotajlara Karşı Koruma Yönetmeliği" savaş, terör ve casusluk olaylarında kritik altyapının korunmasında Türk Silahlı Kuvvetlerinin yanı sıra, bakanlıklar ve ilgili kamu ve özel kuruluşlara da görevler vermektedir[71].

Bunların dışında taşıma türüne göre kritik altyapıların güvenliğine ilişkin özel düzenlemeler mevcuttur.

2.4.1 Karayolları Ulaşım Ağı ve Altyapı Güvenliği

Karayollarında, özellikle Trans Avrupa Ağlarına dahil olan karayollarının güvenliğinin, proje aşamasından itibaren denetlenmesi görevi Karayolları Genel Müdürlüğüne verilmiştir[72]. Karayolu taşımacılık altyapısı ve üstyapısının kontrol altına alınması için dijitalleşmenin getirdiği olanaklardan giderek daha fazla yararlanılmaktadır. Karayollarının güvenliğinin sağlanması ve yönetiminin kolaylaştırılması amacıyla yaklaşık 1.000 km'lik karayolunda optik haberleşme kurulumu tamamlanmıştır[73]. Karayollarının sensörler ve kameralarla izlenmesi için çalışmalar sürmektedir. Yük ve yolcu taşımacılığı faaliyeti yürüten şirketler; depo, tesis ve araç parklarının takibi, yük ve yolcu sevkiyatlarının sorunsuz yapılması, pazarlama ve tedarik zinciri takibi gibi faaliyetler için ileri teknolojiden giderek daha fazla yararlanırken, teknoloji firmaları da çeşitli platformlar aracılığıyla yük ve yolcu taşımacılığı yapan şirketlere araç takibi, yük ve yolcu rezervasyonu, anlık haberleşme ve ödeme takibi dahil olmak üzere çeşitli hizmetler sunmaktadır. Gelecekte Ankara-Niğde Otoyolu gibi "akıllı karayolu"[74] altyapısının yaygınlaşmasıyla karayolu güvenliğinin siber güvenliği daha fazla önem kazanacaktır.

2.4.2 Denizyolları Ulaşım Ağı ve Altyapı Güvenliği

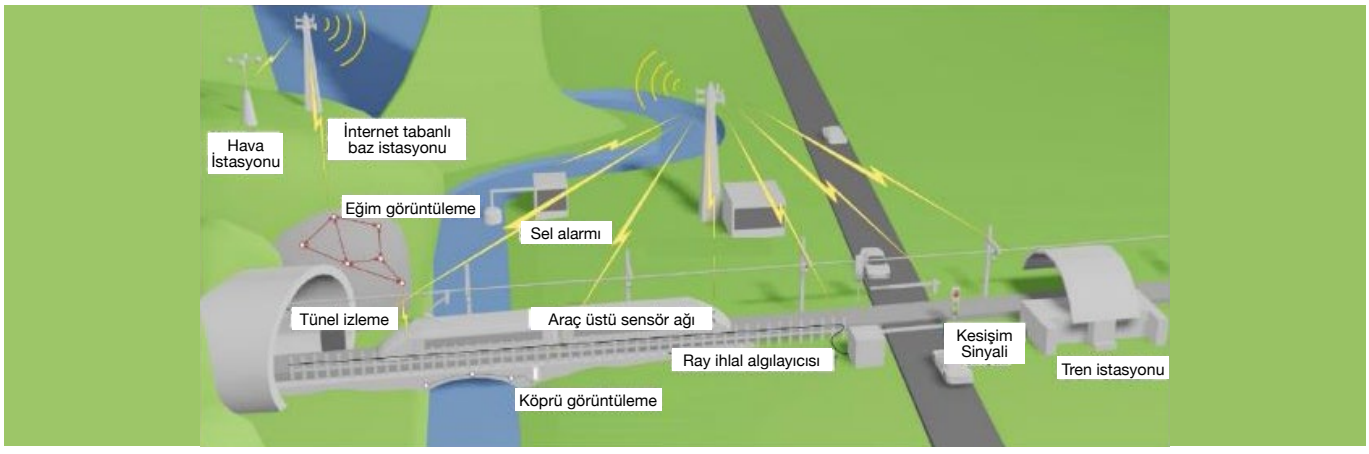
Denizyolu taşımacılığı sektöründe en önemli kritik altyapılar ticari limanlardır. Denizcilik özünde uluslararası bir sektör olduğu için, bu alanda Uluslararası Denizcilik Örgütünün (IMO) belirlediği kurallar büyük önem taşımaktadır. IMO, uluslararası taşımacılık yapan gemiler ve ticari limanların güvenliğinin sağlanması için Gemi ve Liman Tesisi Güvenlik Kuralları (ISPS)[75] kapsamında ayrıntılı kriterler belirlenmiştir. Bunun dışında bazı ülkeler tarafından ISPS'ye ek kriterler de istenmektedir. Örneğin ABD, 2006'da denizyoluyla teröristlerin veya bunların kullanabileceği silahların ülkeye sızmasına engel olmak için ABD'ye yük taşıyan gemilerin ABD'nin belirlediği kurallar çerçevesinde daha çıkış limanında iken güvenlik taramasından geçirilmesi uygulamasına geçilmiştir[76].

Türkiye'de ISPS kurallarına tabi uluslararası deniz liman tesisleri, faaliyetlerini "Özel Güvenlik Kanunu ve Kanunun Uygulanmasına İlişkin Yönetmelik"[77] kapsamında yürütmektedir. Yönetmeliğe göre limanlar, koruma ve güvenlik planları hazırlamak ve valiliğe sunmakla yükümlüdür. Yangın, hırsızlık, deprem ve doğal afetler, sabotajlar ve toplu eylemlere karşı alınacak tedbirler söz konusu planda ayrıntılı biçimde yer almalıdır.

2.4.3 Demiryolları Ulaşım Ağı ve Altyapı Güvenliği

Demiryolu taşımacılığı en güvenli taşımacılık türlerinden biri olmasına karşın çeşitli riskler taşımaktadır. Elektriksiz ve sinyalsiz hatların yanı sıra çok sayıda hemzemin geçit demiryolları güvenliğinin kontrol altında tutulmasını güçleştirdiği gibi kaza riskini de artırmaktadır.

Dünyadaki genel eğilime paralel olarak Türkiye'de demiryolu altyapısının güvenliğinin artırılması için elektrikli ve sinyalli hat uzunluğu artırılırken, hemzemin geçitlerin sayısının mümkün olduğunca azaltılmasına çalışılmaktadır. Bu tedbirlerin yanı sıra 5G ve nesnelerin interneti



Şekil 4: Demiryolunda akıllı yönetim sistemi örneği[79].

uygulamaları destekli demiryolu yönetim sistemlerinin geliştirilmesi ve demiryolu ağının anlık takibinin sağlanması yönünde genel bir eğilim söz konusudur. Ulaştırma ve Lojistik Ana Planı'na göre ülkemizde 2053 yılına kadar 6.196 km hızlı tren hattı, 1.474 km konvansiyonel hat, 622 km yüksek hızlı tren ve 262 km çok yüksek hızlı tren hattı olmak üzere toplam 8.554 km'lik demiryolu hattı yapımı planlanmaktadır[70]. Bir başka deyişle gelecek 30 yılda Türkiye'nin demiryolu taşımacılığında ana rotası yüksek ve çok yüksek hızlı hatlar olacaktır. Söz konusu yatırımlarla "Akılı Demiryolu Sistemi" kurulacağı belirtilmektedir[78].

Diğer ulaştırma alanlarında olduğu gibi raylı sistemlerde de akıllı sistemler kullanıma devam etmekte ve gelişimini hızla sürdürmektedir. Raylı sistemlerde tren istasyonu, demiryolu hattı, araç üstü ekipman ve merkezi yönetim alt sistemlerinde akıllı ulaştırma sistemleri uygulama alanı bulmaktadır. Tren kontrol ve sevkiyat, müşteri servis, acil kurtarma ve yönetimde akıllı sistemler mevcut altyapının ve üstyapının güvenli, verimli ve etkin bir şekilde kullanılmasına olanak sağlamaktadır.

Demiryolu taşımacılığında dijitalleşme durumsal farkındalığı artırarak kritik altyapıların güvenliğine önemli ölçüde katkı sağlamaktadır. Ancak dijitalleşme aynı zamanda siber saldırıya maruz kalma riskini de artırmaktadır.

Öte yandan demiryolları, özellikle kentiçi raylı sistemler, yoğun yolcu trafiği nedeniyle terör ve sabotaj eylemlerinin hedefi olabilmektedir. İspanya'da 2004 yılında üç tren istasyonuna düzenlenen saldırıda 186 kişi yaşamını yitirmiştir[80]. Rusya'nın başkenti Moskova'da 2010 yılında iki istasyondaki patlamalarda 37 can kaybı yaşanmıştır[81]. O nedenle özellikle raylı sistemlerle yolcu taşımacılığında çok yönlü güvenlik önlemlerinin alınması büyük önem taşımaktadır.

Demiryolu taşımacılığında ise 19 Kasım 2015'te yürürlüğe giren "Demiryolu Emniyet Yönetmeliği"[82], Türkiye'de demiryolu işletmeciliği tekeli ortadan kalktıktan sonra bu alanda faaliyet gösterecek firmaların altyapının korunması dahil demiryolu emniyeti için alması gereken önlemlere ilişkin esasları düzenlemektedir. Aynı yönetmelik, Türkiye'de giderek genişleyen şehir içi raylı taşıma operatörlerini de kapsamaktadır.

2.4.4 Havayolları Ulaşım Ağı ve Altyapı Güvenliği

Havacılık sektörü dünyada küreselleşmeyi sağlayan faktörlerden biri ve belki de en önemlisidir. Havayolu taşımacılığı halklar arasında ekonomik ve kültürel köprüler kurulmasını sağladığı gibi mal ve hizmetlerde uluslararası üretim ve tedarik zincirlerinin ulaşmasına imkân tanımaktadır.

Havayolu taşımacılığı, çağın dinamizmini en iyi şekilde yansıtması, uluslararası niteliği ve taşıdığı diğer sembolik değerler nedeniyle ekonomik kazanç veya sansasyon peşinde olan suç ve terör gruplarının fiziki ve siber saldırılarının başlıca hedefleri arasında yer almaktadır. ABD'de 11 Eylül terör saldırıları, 2016 yılında İstanbul Atatürk Havalimanı[83] ve aynı yıl Belçika'nın başkenti Brüksel'in Zaventem Havalimanı'na yönelik can kayıplarının yaşandığı terör saldırıları havayolu taşımacılığına yönelik fiziki tehditlere birkaç örnektir. Ticari uçaklara yönelik saldırılar da son yıllarda azalmakla birlikte sık sık yaşanmaktadır. Örneğin dünya genelinde 1990-2021 yılları arasında 300'e yakın uçak kaçırma girişimi yaşanmıştır[84]. Havayolu taşımacılığına yönelik siber saldırılar ise derin kaygı yaratacak boyutlara ulaşmıştır. Avrupa Havacılık Güvenliği İdaresine (EASA) göre, havacılık sistemine yönelik her ay yaklaşık 1.000 kadar siber saldırı yaşanmaktadır[85]. Türkiye'de havaalanları[86] ve havayolu şirketlerinin[87], [88] uğradığı siber saldırılar zaman zaman kamuoyuna yansımaktadır.

Havacılıkta kritik altyapılarının fiziki korunmasında önemli bir mesafe katedilmiştir. Uluslararası Sivil Havacılık Örgütü (ICAO), Avrupa Sivil Havacılık Konferansı (ECAC) Avrupa Seyrüsefer Güvenliği Teşkilatı (EUROCONTROL) ve Avrupa Havacılık Otoriteleri Birliği gibi kuruluşlar, havaalanlarının tüm noktaları, hava araçları ve sivil uçuş rotalarının güvenliğinin sağlanması için katı kurallar oluşturmuş ve uygulamaya almışlardır. Türkiye'de sivil havacılık sektörünün düzenleyici kuruluşu olan Sivil Havacılık Genel Müdürlüğü (SHGM) de söz konusu uluslararası kuruluşlarla işbirliği içindedir.

Sivil havacılık sektörünün fiziki güvenliğinin sağlanması için başvurulan güvenlik sistemleri insan ve makinelerin bir kombinasyonudur ve bunlar giderek karmaşık hâle gelmektedir. Dünyada havacılık sektörüne ağır darbe vuran COVID-19 pandemisi havacılıkta dijitalleşmeyi hızlandırmıştır. İnsan etkileşimini azaltan uygulamalar, örneğin geleneksel check-in masalarının yerini alan otomatik kiosklar, gelişmiş nesne ve vücut tarama teknolojileri, kâğıtsız biniş kartları ve otomatik biniş süreci gibi pek çok uygulama nesnelerin interneti uygulamalarıyla birbirine bağlanmaktadır. Bunlara ek olarak yolcu taramasına olanak sağlayan biyometrik uygulamalar, pandemiyle daha da öne çıkan sosyal mesafe koruyucu sistemler, kamerayla etkinleştirilen kalabalık yoğunluklu monitörler, fiziksel mesafeyi korumak ve terminaller arasındaki insan akışını yönetmek için radar ve üç boyutlu sensörler de bu dijital dönüşümün unsurlarıdır[89].

Ulaştırma sektörünün önemli bir parçası olan havacılık sektörü ilk uçuşun yapıldığı günden bu yana büyük değişime uğramıştır. Özellikle artan teknoloji kullanımı hava araçlarını, havalimanlarını ve kontrol sistemlerini daha karmaşık hâle getirmiştir. Uçuş emniyetinin artırılması ve kullanım kolaylığı sağlanması kapsamında yapılan bu yenilikler aynı zamanda hava araçlarını, havalimanlarını ve uçuş kontrol sistemlerini iletişim ve bilişim sistemlerine bağlı hâle getirmiştir. Bu bağlılık aynı zamanda hava aracı operasyonlarını siber saldırıların hedefi hâline getirmiştir. Bu sebeple havacılık faaliyetlerinin yürütüldüğü iletişim sistemlerinin ve ağ bağlantı altyapılarının siber güvenliğinin gözden geçirilmesi zorunluluğunu ortaya çıkarmıştır.

Hava taşımacılığı kapsamında ele alındığında mevcut havaalanlarının siber güvenliği ön plana çıkmaktadır. Havaalanlarına yönelik mevcut siber güvenlik önlemlerinin sadece uçuş kontrol sistemlerine odaklanmış olması konunun öneminin artmasına neden olmaktadır. Yolcu, bagaj ve kargo taşımacılığı gibi birçok faaliyetin eşzamanlı olarak yürütüldüğü havaalanlarının bütün bu faaliyetleri kapsayacak şekilde daha genel siber güvenlik politikalarına ihtiyacı vardır[90].

3. HABERLEŞME KRİTİK ALTYAPISI GÜVENLİĞİ

Haberleşme sistemleri tarihin ilk çağlarından bu yana bilgi alışverişinin belkemiğidir. Türkiye'de 2008'de yayınlanan "Elektronik Haberleşme Kanunu"[91] Elektronik Haberleşme'yi (EH), "Elektriksel işaretlere dönüştürülebilen her türlü işaret, sembol, ses, görüntü ve verinin kablo, telsiz, optik, elektrik, manyetik, elektromanyetik, elektrokimyasal, elektromekanik ve diğer iletim sistemleri vasıtasıyla iletilmesi, gönderilmesi ve alınması" olarak tanımlamaktadır.

EH sektörü sabit ve mobil telefon şirketleri, internet hizmet sağlayıcıları, iletişim uyduları operatörleri ve kablo şirketlerinden oluşmaktadır. EH ekipmanları üreticileri, işletmeci kuruluşlar, içerik ve yazılım geliştiricileri, bakım ve diğer hizmetleri sunan şirketleriyle telekomünikasyon sektörü, küresel ekonominin en büyük bileşenlerinden biridir. Küresel EH sektörünün büyüklüğünün 2021 yılı sonunda 1,7 trilyon dolara ulaştığı tahmin edilmektedir[92]. Aynı dönemde küresel EH sektörüne yatırım miktarı 1,5 trilyon doların üzerine çıkmıştır[93]. Sektör sürekli büyümekte, dünya genelinde milyonlarca kişiyi istihdam etmektedir.

Telekomünikasyon sistemlerinin önemi, ekonomik değerini de aşmaktadır. Söz konusu teknolojilerin yaygın kullanımı her türlü bilginin iletimi, işlenmesi ve saklanmasını büyük ölçüde kolaylaştırıp ucuzlatmış ve bu tür bilginin girdi olarak kullanıldığı tüm ekonomik ve sosyal aktivitelerin yapısını değiştirmiştir, inovasyonun başlıca kaynağı olmuştur. EH teknolojileri, bilişim teknolojileri ile birlikte, eğitimden sağlığa, tarımdan iş yaşamına kadar hayatın tüm alanlarında köklü değişiklere yol açmaktadır. Uluslararası Telekomünikasyon Birliğinin altını çizdiği üzere, bilişim ve iletişim teknolojileri, "vatandaşların, tüketicilerin, endüstrinin ve hükümetlerin dünya hakkında bilgi edinme ve paylaşma şeklini dönüştürmektedir" ve "iklim değişikliği ile mücadele etmek, artan küresel rekabete yanıt vermek ve en yoksul, en az yetenekli veya başka şekilde marjinal olanlar da dahil olmak üzere toplumun tüm kesimlerinin artan beklentilerini ve ihtiyaçlarını karşılamak için çözümler geliştirmede merkezi bir rol" oynamaktadır[94].

EH sistemleri ayrıca, ulusal güvenlik ve acil durum hazırlık kaynaklarının kritik bir unsurudur. Bu nedenle iletişim ve haberleşme altyapısının korunması büyük önem taşımaktadır. Bu bölümde dünyada ve Türkiye'de EH kritik altyapısının mevcut durumu, söz konusu altyapıya yönelik tehdit ve bu tehditlerin bertaraf edilmesi, altyapının kesintiyse uğramaması veya elastikiyetinin artırılması için atılması gereken adımlar ele alınacaktır.

3.1 Dünyada ve Türkiye'de Haberleşme Altyapısı ve Pazarının Genel Durumu

Telekomünikasyon teknolojisi, mesafeler arasında ses, veri, görüntü ve/veya video bilgilerinin aktarılması için kullanılan bir dizi yöntemi kapsamaktadır. Ses iletiminde sabit hat ve mobil telefon şebekeleri kullanılmaya devam etmekle birlikte dünya genelinde sabit hat telefon kullanımı hızla düşmektedir. Uluslararası Telekomünikasyon Birliği (International Telecommunication Union -ITU) verilerine göre 2005 yılında 1,2 milyardan fazla olan sabit hat abone sayısı, 2021 yılında 884 milyona kadar düşerken, aynı dönemde mobil telefon abone sayısı 2,2 milyardan 8,6 milyarın üzerine çıkmıştır[95]. Mobil telefon şebekeleri dünya genelinde yüksek yatırım görmektedir. Mobil şebeke operatörlerinin küresel birliği olan GSMA'ya üye 750'den fazla şirket bulunmaktadır[96]. Söz konusu şirketlerin dünya genelinde yaklaşık altı milyon baz istasyonu[97] kurduğu ve yaklaşık 2.000 uydudan hizmet aldığı belirtilmektedir[98]. Bu büyük şebeke dünyada geniş kesimlere ulaşmayı başarmıştır. ITU'ya göre 2021 yılı sonu itibarıyla 7,6 milyar insan, yani dünya nüfusunun yüzde 96,7'si mobil ağların kapsama alanındadır[95]. Öte yandan mobil iletişimde pazar doygunluğuna erişildiği izlenimi yanıltıcıdır. Bu sektör yeni nesil şebekelerle ve yeni kabiliyetlerle dinamizmini korumaktadır. Örneğin 5G mobil hizmetleri henüz yeni atağa kalkmışken 6G mobil internetin araştırma ve geliştirme çalışmaları sürmektedir[99]. Dünya genelinde 5G baz istasyonu sayısı 2021 yılı sonunda 1,5 milyonun üzerine çıkarken, bunda Çin'in yaptığı büyük ölçekli yatırımların etkisi belirleyici olmuştur[100]. 2021 yılı sonu itibariyle 5G abone sayısı 521 milyona ulaşırken 5G'nin pazardaki payının 2026 yılında yüzde 40'a yaklaşması beklenmektedir[101].

Veriler ise sabit ve mobil internet hizmet sağlayıcıları yoluyla iletilmektedir ve bu alanda da hızlı bir gelişme yaşanmaktadır. ITU verilerine göre dünya genelinde 2008 yılında 411 milyon sabit genişbant internet abonesi bulunurken, bu sayı 2021 yılı sonunda 1,3 milyara ulaşmıştır. 3G, 4G ve 4,5G'nin ardından 5G mobil şebekelerinin devreye girmesiyle mobil internet kullanıcı sayısında da patlama yaşanmış, 2008 yılında 422 milyon olan küresel mobil internet kullanıcı sayısı 2021 yılında 6,5 milyarı aşmıştır[95]. Dünya genelinde internet erişimi ülkelerin gelişmişlik ve şehirleşme düzeylerinin yanı sıra, kullanıcıların yaşları ve cinsiyetlerine göre farklılık arz etmektedir. ITU verilerine göre dünyada 2,9 milyar insanın internete erişimi bulunmamaktadır ve bunların yüzde 96'sı az gelişmiş veya gelişmekte olan ülkelerde yaşamaktadır[102]. Dünya genelinde şehirlerde yaşayanlarla kırsal kesimde yaşayanların internet kullanım oranlarında da büyük farklılık bulunmaktadır. Şehirlerde yaşayanlar arasında internet kullanım orayı yüzde 76'ya çıkarken, kırsal kesimde yaşayanlar arasında bu oran yüzde 39'a düşmektedir. 15-24 yaş arası dünya gençlerinin yüzde 71'i internet erişimine sahipken bu oran diğer yaş gruplarında yüzde 57'ye gerilemektedir. Erkek ve kadınların internet kullanımı arasındaki fark ise giderek kapanmaktadır. 2021 yılı sonu itibarıyla erkeklerin yüzde 60'ının, kadınların ise yüzde 57'sinin internete erişimi bulunmaktadır[102].

Görüldüğü üzere, dünyada internet erişimi alanında pazar potansiyeli hâlâ çok yüksektir. Yeryüzünün her noktasına internet erişimi sağlamak için gerek mobil şebeke operatörleri gerekse uzay şirketleri[103] binlerce küçük uydudan oluşan takım uydu sistemleri ile yatırımlara başlamışlardır. 21'inci yüzyılın ortalarına doğru dünyanın

her bir noktasında internet erişiminin bulunacağı ve her bir dünya vatandaşının internete bağlanabileceği belirtilmektedir[104].

Mobil şebekeler görüntü ve video aktarımında da etkilidir. Ancak sabit genişbant erişiminin artmasıyla, ödemeli televizyon ve video içerik platformlarının kullanıcı sayısı da gittikçe artmaktadır. Kablolu ve şifreli yayınların ardından son yıllarda internet veya uydu üzerinden ön ödemeli içerik aktaran platformların sayısı, özellikle pandemi döneminde patlama yaratmıştır. Bir tahmine göre, bu tür video akış hizmeti sunan platformların dünya genelindeki abone sayısı 1,3 miyarı bulmuştur[105].

Türkiye'de EH sektörü, dünyadaki gelişmelere paralel bir seyir izlemektedir. Türkiye'de de son 20 yılda hem özel sektörün hem de kamu sektörünün telekomünikasyon yatırımları bu kapsamda artmış ve telekomünikasyon altyapısı hızla gelişmiştir. Türkiye'de EH sektöründe faaliyet gösteren firma sayısı, mobil abonelik ve internet veri trafiği gibi alanlarda yüksek büyüme hızları yakalanırken, sabit telefon hattı abone sayısı düşmektedir (Tablo 4). EH sektöründeki gelişme Türkiye'nin büyümesine de olumlu katkı sağlamaktadır. Yapılan bir araştırmaya göre telekomünikasyonda yüzde 1'lik bir artışın Türkiye'nin GSYH'sinde yüzde 0,06'lik bir artışa neden olduğu sonucuna ulaşılmıştır[106].

EH trafiğinin yüzde 95'i mobil şebekeler üzerinden gerçekleşmektedir[107]. Türkiye'de mobil operatörler, yaklaşık 1.700'ü yerli üretim olmak üzere 200.000'e yakın baz istasyonu üzerinden faaliyet göstermektedir[108]. Nüfusa göre mobil abonelik oranını ifade eden mobil yaygınlık oranı, Aralık 2021 sonu itibarı ile yüzde 101,9'a çıkmıştır. Makineler arası iletişim (M2M) ve 0-9 yaş nüfus hariç olmak üzere mobil yaygınlık oranı ise yüzde 109,3 olarak hesaplanmaktadır. Mobil abonelerin yaklaşık 4 milyonu 3G abonesidir ve bu sayı hızla düşmektedir. 4,5 G mobil abone sayısı ise 80 milyonun üzerine çıkmıştır.

Türkiye'de internet erişimi, gelişmiş ülkeler seviyesindedir. 2008 yılında altı milyon civarında olan genişbant internet abonesi, 2021 yılı dördüncü çeyreği itibarıyla 88,2 milyona ulaşmıştır (Şekil 5).

Türkiye'de internet erişim oranları yüksek olmakla birlikte, OECD ülkeleri ortalamasının altında kalmaktadır. Türkiye'de nüfusa göre sabit genişbant yaygınlık oranı yüzde 21,4, OECD ortalaması ise yüzde 33,2'dir. Mobil genişbant yaygınlık oranı ise Türkiye'de yüzde 82,7, OECD ortalaması ise yüzde 118,3'tür. Öte yandan

Şekil 5: Türkiye genişbant internet abone sayısındaki değişim[107].

	2021	2020	Değişim
EH Sektörü Gelirleri (TL)	92.376.308.641	77.088.009.102	19,8
EH Sektörü Yatırımları (TL)	21.790.248.248	16.683.036.908	30,6
EH Sektöründe Faaliyet Gösteren İşletme Sayısı	442	452	-2.2
Sabit Abone Sayısı	12.310.016	12.448.604	-1.1
Toplam Mobil Abone Sayısı	86.288.834	82.128.104	5.1
M2M Abone Sayısı	7.444.802	6.380.454	5.1
Toplam Genişbant İnternet Abone Sayısı	88.164.739	82.364.590	7.0
xDLS	11.373.647	11.036.313	3,2
Fiber	4.840.908	4.005.880	20,8
Kablo	1.373.647	1.298.340	5.8
Diğer	535.064	394.320	29,3
Toplam Genişbant İnternet Trafiği	50.742.29	36.137.759	40,4
Abone Başına Aylık Veri Trafiği (GB)			
Mobil	10,7	8,9	20,2
Sabit	204,5	160,4	27,5

Tablo 4: Türkiye temel elektronik haberleşme verileri[107].

Türkiye, OECD ülkeleri içinde 2019-2020 yılları arasındaki bir yıllık süreçte sabit internet yaygınlığı en çok artan ülkeler arasında ilk sırada yer almaktadır. Bu dönemde OECD ülkelerinde bir yıllık ortalama yaygınlık artışı yüzde 1,4 iken ülkemizde bu oran yüzde 2,8 olarak gerçekleşmiştir[107].

Türkiye'de uydu destekli elektronik haberleşme altyapısı da ileri seviyededir. Türksat Uydu Haberleşme Kablo TV ve İşletme A.Ş. (Türksat), Türksat uyduları ve diğer uydular üzerinden her türlü uydu haberleşmesini gerçekleştiren dünyanın önde gelen uydu operatörlerinden biridir. Avrupa, Asya ve Afrika başta olmak üzere geniş bir coğrafyada uydular üzerinden ses, veri, internet, TV ve radyo yayıncılık hizmetleri sağlayan Türksat, sahip olduğu kablo altyapısı üzerinden yurtiçindeki bir milyondan fazla abonesine analog ve dijital TV, genişbant internet, sabit telefon hizmetleri de sağlamaktadır. Türksat A.Ş. ayrıca bilişim ve e-Devlet hizmetleri kapsamında e-Devlet Kapısı'nı işletmekte, kamu hizmetlerinin elektronik ortamda verilmesine dönük projeler yürütmektedir. Ülkemizde TV yayıncılık sektörünün büyümesine, yerli içeriklerin gelişmesine ve ihracatına katkı sağlayan Türksat A.Ş. işlettiği Türksat 3A, Türksat 4A, Türksat 4B ve Türksat 5A uydularının da işletici kuruluşudur.

3.2 Elektronik Haberleşmede Yeni Eğilimler

Günümüzde EH sektörünü doğrudan etkileyen eğilimlerden bazılarını beş başlık altında toplamak mümkündür[109]:

- **Bilişim, ağlar ve elektronik haberleşme teknolojilerinin yakınsaması:** Yeni cihazlar ve uygulamalar nedeniyle bilişim ve elektronik haberleşme sektörü giderek daha fazla iç içe girmekte ve sınırlar belirsizleşmektedir. Yakınsama yeni ileri teknoloji çözümleri, ağlar ve hizmetlerin ortaya çıkmasına yol açmaktadır. Örneğin EH operatörleri, iş operasyonlarındaki verimliliği artırmak, yeni hizmetler ve uygulamalar sunmak ve içerik depolamak ve dağıtmak için kendilerini ağ şirketlerinden bulut hizmeti şirketlerine dönüştürmektedir. Yeni nesil teknolojiler de bu yakınsamayı pekiştirmektedir. Örneğin nesnelerin internetinde çeşitli sensörlerden alınan veriler mobil şebekeler aracılığıyla sabit geniş bant internete aktarılmakta ve büyük veri analizi yapılabilmektedir. Böylece herhangi bir yerdeki cihazdan herhangi bir zamanda çeşitli verileri gerçek zamanlı olarak almak mümkün olabilmektedir.
- **Veri iletim hızı ve kanal kapasitesinde artış:** Dünya genelinde çevrimiçi faaliyetler artmakta ve elektronik haberleşme sektörü artan talebi karşılamak için mevcut EH altyapısını, bant genişliğini artıracak ve hızlandıracak şekilde iyileştirmeye zorlamaktadır. Bu açıdan EH sektöründe, daha geniş kanal kapasitesine ve iletim hızına sahip 5G altyapısına geçişin hızlanması beklenebilir.
- **Nesnelerin interneti ve endüstriyel internet uygulamaların çığ gibi büyümesi:** Bazı tahminlere göre nesnelerin interneti hâlen internet trafiğinin yüzde 70'ini oluşturmaktadır ve bu oran 2027 yılında 41 milyar nesnelerin interneti cihazının devreye girmesiyle daha da artacaktır. Söz konusu cihazlar arasında sürücüsüz araçlar, akıllı fabrikalar, ulaşım ve enerji kontrol sistemleri de önemli bir yer tutacaktır[110].
- **Uzaktan çalışma ve e-eğitim için ağ teknolojilerinin geliştirilmesi:** COVID-19 pandemisi uzaktan çalışma ve e-eğitime geçiş sürecini hızlandırmıştır. Genel eğilim, kontrolü kolay ve güvenli bir ağ üzerinden uzaktan çalışma ve eğitim modeline geçilmesi yönündedir. Bu alanda güvenli ve kesintisiz bağlantıların kurulması için daha fazla geliştirme yapmak gerekecektir[111].
- **Sosyal ağlar ve metaverse kullanımının hızla artması ve daha fazla yaygınlaşması**: Sosyal ağlar, internetteki temel iletişim kanallarından biridir. Dünya genelinde en az bir sosyal medya platformuna üye kullanıcıların sayısının Ekim 2021'de 4,5 milyarı aştığı bildirilmektedir[112]. Ağa bağlı sürücüsüz araçların artması ve metaverse uygulamaları[113] sosyal medyaya ulaşımı daha da artıracaktır.

3.3 Elektronik Haberleşmede Riskler

Yeni nesil mobil iletişim ve bilişim teknolojilerindeki gelişmeler EH sektöründe kapasite yatırım baskısını artırırken EH altyapısı, diğer tüm kritik altyapı gibi çok sayıda risk ve tehdit ile karşı karşıyadır.

- **Doğal afet riskleri**: EH altyapısı geniş coğrafyalara yayılmış ve dağınık bir yapı arz etse de doğal afetlerin etkilerinden muaf değildir. Depremler, seller, toprak kaymaları ve aşırı iklim olayları EH altyapısına doğrudan zarar vermektedir. Ayrıca, Türkiye'de 17 Ağustos 1999'daki Marmara Depremi'nden sonra yaşandığı üzere, doğal afet sonrası artan acil iletişim ihtiyacı ve şebekelerde aşırı yüklenmeler kısmi ve hatta genel erişim sorunları yaratabilmektedir.
- **Savaş, terör, suç ve sabotaj riskleri**: Terör ve suç grupları EH altyapısına[114] ve telekomünikasyon şirketlerinin çalışanlarına[115] yönelik saldırılar düzenleyebilmekte, hırsızlık vakaları EH altyapısına zarar verebilmekte, iletişimde kesintilere neden olabilmektedir. 2022 yılında Ukrayna krizinde açıkça görüldüğü gibi tüm kritik altyapılar gibi EH altyapısı savaşlarda fiziki ve siber saldırıların hedefi olmaktadır[116].
- **EH teknolojisi ve cihazlarında dışa bağımlılık**: Dünya genelinde EH sektörü altyapısı ve kullanıcı cihazları pazarlarında çok sayıda oyuncu olmakla birlikte, birkaç ülkenin üreticileri küresel pazarda büyük pay almaktadır. Telekomünikasyon ekipmanları sektöründe Çin (Huawei ve ZTE), Finlandiya (Nokia), İsveç (Ericcson), ABD (Cisco ve Ciena) ve Güney Kore'den (Samsung) firmaların pazar paylarının toplamı yüzde 90'ın üzerine çıkmaktadır[117]. Küresel cep telefonu piyasasında ise Güney Kore (Samsung), ABD (Apple), Çin'den (Xiomi, Oppo ve Vivo) firmaların toplam küresel pazar payı yüzde 70'i bulmaktadır[118]. EH altyapısının kritik bir bileşeni olan yarı iletkenler sektöründe durum benzerdir: Tayvanlı iki üretici (TSMC ve UMC) küresel yarı iletken pazarının yüzde 41'ini kontrol

etmektedir. Çin (SMIC), Güney Kore (Samsung) ve BAE (Global Foundries) firmalarının payları eklendiğinde yarı iletkenler pazarının üçte ikisinin beş şirketin kontrolünde olduğu görülmektedir[119]. EH sektörü açısından bir diğer önemli bileşen olan telekomünikasyon yazılımları sektöründe de benzeri bir oligopol yapısı bulunmaktadır: ABD'li dört şirket (Oracle, Microsoft, Salesforce, Adobe) telekom yazılımları pazarının yaklaşık dörtte birini kontrol etmektedir.

EH altyapısı ekipmanları, cihazları ve yazılımları pazarda kısıtlı oyuncunun bulunması söz konusu kritik sistemlerin güvenliği konusunda zafiyet yaratmaktadır. Bu zafiyet, 2022 yılında yaşanan çip krizinde[120] olduğu gibi tedarik sıkıntısı yaratarak ekonomik kayıpları artırmakta, EH altyapısını ve kullanıcıların güvenliğini tehlikeye atmaktadır. Örneğin geçmişte ABD'nin güvenlik ve istihbarat kuruluşlarının, dünyada yaygın olarak kullanılan söz konusu teknolojik ürünlere sızılabilmesi için "arka kapı" bırakılması için baskı yaptığı dünya kamuoyuna yansımıştır[121]. Bu durum, ulusal EH şebekelerinin, endüstriyel ve siyasi casusluğa maruz kalmasının yanı sıra kişisel verilerin kötü amaçlar için kullanılmasına kapı aralamaktadır. EH şebekelerinin zafiyetleri, bağlantılı akıllı yönetim sistemleri kullanan enerji, ulaşım ve diğer kritik endüstriyel tesis ve altyapıların da zafiyete uğramasına neden olmaktadır.

- **5G ve nesnelerin interneti uygulamalarının yaygınlaşmasının yarattığı riskler**: Nesnelerin interneti uygulamaları dünyada hızla artmaktadır. Fiziki olarak insani işgücü ile yapılması imkânsız, çok zor veya yıpratıcı olabilecek görevleri, hatasız ve anlık olarak yerine getirebilecek nitelikte olan nesnelerin interneti uygulamaları, sağladıkları verim, işlenebilir veri ve kontrol kabiliyetleri ile daha fazla uygulama alanı bulmaktadır[122]. Akıllı şehir ve akıllı ev uygulamalarından akıllı fabrikalara ve sürücüsüz araçlara kadar pek çok alanda nesnelerin interneti uygulamaları kullanılmaktadır. Bir tahmine göre 2022 yılı sonuna kadar dünya genelinde 29 milyardan fazla internete bağlı cihaza ulaşılacaktır ve bunların yaklaşık 18 milyonu, yani yüzde 62'sinden fazlası nesnelerin interneti bağlantılı olacaktır[123]. Nesnelerin interneti cihazlarının 2025 yılında ulaşacağı sayıya ilişkin çeşitli tahminler ise farklı olmakla birlikte 2022'ye kıyasla en az üç dört kat artış beklendiğini belirtmek mümkündür.

Nesnelerin interneti cihazlarının pazarına ilişkin tahminlerin gerçekleşmesi EH sektörü üzerinde çeşitli riskler yaratmaktadır. Bunların başında ağ yükü gelmektedir. Tek bir sunucu ile iletişim kurmaya çalışan binlerce sensör, ölçüm cihazı veya kamera, sunucuyu yıkabilecek bir veri trafiği akışı yaratacaktır. Ek olarak, sensörlerin çoğu iletişim kurmak için şifrelenmemiş bir bağlantı kullanır ve bu nedenle güvenlikte gecikme olasılığı vardır[124].

Daha fazla bağlı cihazın aktif hâle gelebilmesi, 5G mobil bağlantılarının yaygınlaşmasına bağlı olacaktır. Hâlen başta dünyada kurulu 5G baz istasyonlarının yarıdan fazlasına sahip olan Çin'in[125] yanı sıra Güney Kore, Japonya, ABD ve diğer ülkeler 5G altyapısına büyük yatırımlar yapmaktadır. Ayrıca 5G söz konusu ülkeler, özellikle Çin ile ABD arasında zaman zaman sertleşen bir rekabete yol açmıştır[126].

5G, EH'nin geleceğinde merkezi konuma doğru ilerlerken, birtakım riskleri de beraberinde getirmektedir. Bunların başında siber saldırılar gelmektedir. 1 km^2 alanda 1 milyon civarında cihazı destekleyebilen 5G'nin daha fazla bağlantıya ve bant genişliğine sebep olması siber güvenlik sorunlarını da beraberinde getirmektedir. Zira daha fazla cihaz bağlantısı daha fazla güvenlik açığı riski anlamına gelmektedir. Saldırının nereden geleceğini tahmin etmek güçleşmektedir. Örneğin 2018 yılında siber saldırganlar, ABD'nin Las Vegas kentindeki bir kumarhanenin müşterilerinin bilgilerine, kumarhane içinde bulunan bir akvaryumdaki balıkların yem, su sıcaklığı ve diğer ihtiyaçlarını otomatik olarak karşılayan sistemin internet bağlantısını kullanarak sızmışlardır[127]. Ayrıca nesnelerin interneti ve 5G enstrümanlarının, sensörlerinin ve yazılımlarının küçük arızaları bile bir dizi öngörülemeyen olumsuz etkiye neden olabilir. Massachussets Institute of Technology (MIT) tarafından yürütülen araştırmalara göre, yazılım hataları ve kusurlarından kaynaklanan iletişim, elektrik ve diğer hizmetlerdeki kesintiler ve arızalar günlük rutinimizin bir parçası olabilir ve her yıl yüzlerce vaka yaşanabilir[109].

- **Çalışanların ve tedarik zincirinin yarattığı riskler:** EH altyapısı ve ağlarına ilişkin riskler, telekomünikasyon şirketlerinin değer zincirinden de kaynaklanabilir. Ekipman tedarikçileri, çözüm ortakları, e-posta hizmeti sağlayıcıları, barındırma (hosting) hizmeti sağlayıcıları, hukuk firmaları, veri yönetimi şirketleri ve diğer taşeronlar dahil olmak üzere üçüncü taraflar, saldırganların sızması için önemli altyapıya kolayca sızılabilecek "arka kapılar" hâline gelebilirler.

  COVID-19 pandemisi ile birlikte uzaktan çalışma sisteminin EH sektöründe de yaygınlaşması bir başka riski doğurmuştur. Siber güvenlik önlemleri konusunda yeterli eğitimi almamış çalışanlar, güvenli olmayan ağlarla şirketlerinin bilişim sistemlerine bağlanabilmekte ve güvenlik zafiyeti yaratabilmektedir.
- **Siber saldırılar:** Elektronik haberleşme sektörü en çok siber saldırıya uğrayan sektörlerden biridir. Türkiye'de 2018 yılında EH sektöründeki şirketlere yönelik yaklaşık 73.000 saldırı bildirilirken, bu sayı 2020 yılında 118.000'in üzerine çıkmıştır[128]. Türkiye'de EH sektörüne yönelik en sık görülen siber saldırı türleri Dağıtık Servis Dışı Bırakma (DDoS) ve Oltalamadır (Phishing).

3.4 Uluslararası ve Ulusal Çerçevede Elektronik Haberleşmenin Güvenliği

Dünya genelinde bir kritik altyapı olarak kabul edilen EH'nin uçtan uça güvenliğinin sağlanması hem kamu kuruluşları hem de işletmeci kuruluşlar açısından bir önceliktir. Bulunan çözümlerin makul maliyetli ve sürdürülebilir olmasının yanı sıra EH elastikiyetini pekiştirmesi de beklenmektedir. EH alanında dünyanın çatı örgütü konumundaki Uluslararası Telekomünikasyon Birliğinin (ITU), 2003 yılında yayınladığı "Uçtan uca iletişim sağlayan sistemler için güvenlik mimarisi" başlıklı tavsiye belgesinde[129], "Güvenli bir ağ, kötü niyetli ve yanlışlıkla yapılan saldırılara karşı korunmalı ve yüksek kullanılabilirliğe, uygun yanıt süresine, güvenilirliğe, bütünlüğe, ölçeklenebilirliğe sahip olmalıdır" denilmektedir.

ITU söz konusu tavsiye metninde bir EH güvenlik mimarisinin çerçevesini de belirlemektedir. ITU, EH'ye yönelik tehditlerin sonuçlarını:

- Hizmetlerin kesintiye uğraması,
- Bilgilerin ve/veya diğer kaynakların yok edilmesi,
- Bilgilerin bozulması veya değiştirilmesi,
- Bilgi ve/veya diğer kaynakların çalınması, kaldırılması veya kaybedilmesi,
- Bilgilerin ifşası olarak sıralamaktadır.

ITU söz konusu olumsuz sonuçların engellenmesi için güvenliği altyapı, hizmetler ve uygulamalar olmak üzere üç düzeyde ele almaktadır:

- Altyapı güvenliği düzeyi,
- Hizmet güvenliği düzeyi,
- Uygulama güvenliği düzeyi.

ITU, her düzeyde tüm önemli güvenlik tehditlerine karşı koruma sağlayan sekiz önlem belirlemiştir:

- **Erişim denetimi:** Ağ öğelerine, depolanan bilgilere, bilgi akışlarına, hizmetlere ve uygulamalara yalnızca yetkili personel veya cihazların erişimine izin verilmesinin sağlanmasıdır.
- **Kimlik doğrulama:** İletişime katılan varlıkların (kişi, cihaz, hizmet veya uygulama) yetkisiz olmadığına dair güvence sağlar.
- **İnkar edilemezlik:** Bir bireyin veya kuruluşun verilerle ilgili belirli bir eylemi gerçekleştirdiğini inkâr etmesini önlemek için araçlar sağlar.
- **Veri gizliliği:** Şifreleme, erişim kontrol listeleri, dosya izinleri vb. ile veri içeriğinin yetkisiz kişiler tarafından ifşasının engellenmesi ve yetkisiz kişilerce anlaşılamamasının sağlanmasıdır.
- **İletişim güvenliği:** Bilginin yalnızca yetkili uç noktalar arasında, her türlü etkiden muaf olarak akmasının sağlanmasıdır.
- **Veri bütünlüğü:** Verilerin doğruluğunu veya doğruluğunun sağlanmasını ifade etmektedir. Veriler yetkisiz değişiklik, silme, oluşturma ve çoğaltmaya karşı korunur ve bu yetkisiz faaliyetlerin bir göstergesini sağlar.
- **Kullanılabilirlik**: Ağı etkileyen olaylar nedeniyle ağ öğelerine, depolanan bilgilere, bilgi akışlarına, hizmetlere ve uygulamalara yetkili erişimin reddedilmemesinin sağlanmasıdır. Olağanüstü durum kurtarma çözümleri bu kategoriye dahildir.
- **Mahremiyet güvenliği**: Bir kullanıcının ziyaret ettiği sitelerin, coğrafi konumunun, cihazların IP adreslerinin ve DNS adlarının gizli kalmasının sağlanmasıdır.

ITU'nun vurguladığı üzere, elektronik haberleşme altyapı güvenliği, EH güvenliğinin sadece bir bölümünü

oluşturmaktadır. Haberleşme güvenliği bir bütün olarak ele alınmalıdır. EH güvenliğinin sağlanması için kamudan işletmeci kuruluşlara, tedarikçilerden son kullanıcılara tüm paydaşların üzerine düşen görevler bulunmaktadır.

EH altyapısı, Türkiye'de 2008'de yayınlanan "Elektronik Haberleşme Kanunu"nda[91], "Elektronik haberleşmenin, üzerinden veya aracılığıyla gerçekleştirildiği anahtarlama ekipmanları, donanım ve yazılımlar, terminaller ve hatlar da dahil olmak üzere her türlü şebeke birimleri, ilgili tesisleri ve bunların bütünleyici parçaları" olarak tanımlanmaktadır.

2014'te yayınlanan EH sektöründe faaliyet gösteren işletmeciler tarafından şebeke ve bilgi güvenliğinin sağlanmasına yönelik olarak alınması gereken tedbirlerin tanımlandığı Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği[130] kapsamında işletmeciler, siber saldırılara karşı gerekli önlemleri almak ve iş sürekliliği planlarını yapmakla yükümlü kılınmıştır. Söz konusu yönetmeliğin temel ilkelerinin ITU'nun tavsiyeleriyle uyumlu olduğu görülmektedir:

- İşletmecilerin yükümlülüklerinin belirlenmesinde, şebeke ve bilgi güvenliğinin sağlanmasına yönelik tedbirlerin tespitinde ve uygulanmasında mümkün olduğu ölçüde risk temelli değerlendirmelerin yapılması,
- Tüketici haklarının korunması,
- Hizmet kalitesinin yükseltilmesi,
- Ulusal düzenleme ile ulusal ve/veya uluslararası standartların dikkate alınması,
- Güvenlik ile kullanılabilirlik arasında denge kurulması,
- Azami ölçüde milli kaynakların kullanılması.

Cumhurbaşkanlığı Dijital Dönüşüm Ofisinin Temmuz 2020'de yayınladığı "Bilgi ve İletişim Güvenliği Rehberi" de[131] yukarıdaki ilkeleri tekrarlamakla birlikte yeni ilkeler de belirlemektedir (Şekil 6).

Elektronik haberleşme ve bilişim sektörünün tüm değer zincirinde altyapı hizmetleri ve kullanıcı güvenliğine ilişkin ayrıntılı bir denetim listesi sunan rehberde, kritik haberleşme altyapısının korunmasına ilişkin öneriler de sıralanmaktadır. Bunlardan bazıları Tablo 5'te özetlenmiştir.

Şekil 6: Cumhurbaşkanlığı Dijital Dönüşüm Ofisinin belirlediği bilgi ve iletişim güvenliği ilkeleri[131].

Tedbir Adı	Tedbir Tanımı
Hizmet Güvenliği ve Sürekliliği	Sağlanan iletişim hizmetlerinin güvenliğini ve sürekliliğini ele alan bir güvenlik politikası belirlenmeli ve uygulanmalıdır. Güvenlik politikası; geçmişte yaşanan güvenlik olayları ve ihlalleri, hizmet kesintileri ve sektördeki diğer sağlayıcıları etkileyen olaylar dikkate alınarak periyodik olarak güncellenmelidir. Özellikle kilit personelin belirlenen güvenlik politikasına yönelik farkındalığı artırılmalıdır.
Üçüncü Taraflara İlişkin Güvenlik Gereksinimleri	Üçüncü taraflardan temin edilen BT ürünlerine, BT hizmetlerine, dış kaynaklı iş süreçlerine, çağrı merkezlerine, ara bağlantılara, ortak tesislere vb. yönelik güvenlik gereksinimleri sözleşmelerde ele alınmalıdır.
Altyapı Servislerinin Güvenliği	Haberleşme hizmetlerindeki altyapı servislerinin kötüye kullanımından kaynaklanacak tehditler için gerekli önlemler alınmalıdır.
Sahtecilik İşlemlerini Tespit ve Önleme	Sinyalleşme trafiğindeki olası sahtecilik işlemlerini tanımlamak, tespit etmek ve önlemek için bir sistem kurulmalı ve işletilmelidir.
Güvenilir İletişimin Tesisi	İletişim hizmetlerinde müşterilerin kaynak IP adreslerinin doğrulanmasını sağlayan sistemler kullanılmalı; hatalı, değiştirilmiş (spoofed) IP adreslerinin şebekede dolaşımını engellemelidir.
Sıkılaştırma Faaliyetleri	Sunucular, yönlendiriciler ve diğer şebeke elemanlarının saldırı yüzeyini azaltmak için gerekli sıkılaştırma kontrolleri uygulanmalıdır
Ekipman Arızalarının İzlenmesi	Güvenlik ve iş sürekliliği gereksinimlerini sağlamak amacıyla altyapıda yer alan ekipmanlara ait arıza sinyallerinin izlenmesi için alarm mekanizması kurulmalıdır.
Ekipman Güvenliğinin Sağlanması	Haberleşme sistemlerinde kullanılan ekipmanı, çevresel tehditler ile enerji destek sistemlerinden kaynaklanacak olumsuz etkilere karşı korumak amacıyla gerekli önlemler alınmalıdır.
Tehdit İstihbaratı Yönetimi	Siber güvenlik tehdit istihbaratı ile ilgili güncel ve güvenilir bilgiyi almak için gerekli tehdit istihbaratı çalışmaları yapılmalı ve tehdit istihbaratı verilerini yönetmek amacıyla bir süreç/mekanizma tanımlanmalıdır.
Otoritelerle İletişim	Tehdit yönetim faaliyetlerini destekleyecek otoritelere ilişkin iletişim listesi tanımlanmalıdır.
Arayan Hat Bilgisi Kullanımı	Haberleşme hizmetinde, arayan numara manipülasyonunu (Caller ID Manipulation) engellemeye yönelik teknik ve hukuki tedbirler alınmalıdır.
İnternet Değişim Noktası	Yurtiçi iletişim trafiğinin ülke sınırları içerisinde kalması sağlanmalı, bu trafiğin ve abone kayıtlarının yurtdışına çıkarılarak tekrar yurtiçine yönlendirilmesi engellenmelidir.
Kritik Haberleşme Güvenliği	Telekomünikasyon hizmeti veren işletmelerce yerine getirilmek üzere, Cumhurbaşkanlığı ve milli güvenliğin sağlanması kapsamında görev yürüten kamu kurumlarında iletişimin gizliliği ve güvenliğini artırmak amacıyla, bu kurumların merkez birimlerine ve talep edeceği diğer birimlerine doğrudan hizmet sağlayan haberleşme ve transmisyon altyapısında ilk toplama noktasına kadar radyolink vb. kablosuz teknolojiler kullanılmamalı, kullanımın zorunlu olması durumunda ihtiyaç duyulan gizlilik seviyesine uygun donanımsal veya yazılımsal milli kripto sistemleriyle birlikte kullanılmalıdır.

Tablo 5: Cumhurbaşkanlığı Dijital Dönüşüm Ofisinin önerdiği EH kritik altyapısı güvenliği tedbirleri[131].

Rehber, ayrıca EH altyapısının fiziki güvenliğinin sağlanması için yapılması gerekenler konusunda da ayrıntılı tavsiyelerde bulunmaktadır. EH altyapı tesislerinin, ekipmanlarının ve ara bağlantılarının (kablo vb.) kapalı ve erişim kontrolü olması; yangın, sel, deprem vb. risklere karşı yapısal tedbirlerin alınması ve görevli personelin eğitilmesi; tesislerin kameralarla izlenmesi ve alarm sistemlerinin kurulması önerilen tedbirler arasında bulunmaktadır.

Türkiye'de kamu otoritesi EH güvenliği için temel ilke ve esasları belirlediği gibi uygulamada da öncü adımlar atmaktadır. Örneğin AFAD, büyük afetlerde ve acil durumlarda afet veya acil durumun yönetilebilmesi için 81 ile uydu telefonlu Kesintisiz ve Güvenli Haberleşme Sistemi (KGHS) kurmuştur[132].

EH güvenliğinin sağlanması yönünde bir diğer önemli adım iletişim altyapısı ve yazılımlarında yerli ve milli çözümlerin sayısının artırılmasıdır. 2015-2016 döneminde mobil işletmecilerin yerli malı belgeli donanım ve yazılım yatırımlarının toplam yatırım içindeki oranı yüzde 0,98'de kalırken kamu, özel sektör işbirliği ile bu oran 2021 yılında yüzde 23'e yükselmiştir. Söz konusu dönemde 66 farklı üreticiden yaklaşık 153 farklı ürün temin edilmiştir[133]. Öte yandan Uçtan Uca Yerli ve Milli 5G Projesi'nde önemli ilerlemeler kaydedilmiş ve ilk yerli ve milli 5G altyapısı üzerinde ilk görüşme Haziran 2021'de yapılmıştır[134].

4. BİLGİ VE İLETİŞİM TEKNOLOJİLERİ İLE BAĞLANTILI YAPILARIN GÜVENLİĞİ

Günümüzde diğer kritik altyapılar, kritik öneme haiz endüstriler, kamu ve özel sektör kuruluşları, üniversiteler ve diğer eğitim kurumları, sağlık sistemi ve diğerleri giderek Bilgi Teknolojisi (BT) sektörü işlevlerine daha fazla bağımlı hâle gelmiştir. Bu nedenle BT sektörü ulusun güvenliği, ekonomisi, halk sağlığı ve güvenliği için merkezi konumdadır.

BT altyapısı, kurumsal BT hizmetlerinin ve BT ortamlarının işletimi ve yönetimi için gereken bileşenleri ifade etmektedir. Veri merkezleri, barındırma (hosting) merkezleri, sunucular, ağ anahtarları, yönlendiriciler (routers), sabit veya taşınabilir terminal cihazlar ve yazılımlar BT altyapısının unsurlarından bazılarıdır. BT altyapısı EH sistemleri ile birlikte dünyanın herhangi bir noktasından ve/veya uzaydaki uydular ile birlikte çalışabilmektedir. BT altyapısının bu doğası onu sınır ötesi hâle getirmiştir. Sektörün karmaşık ve dinamik ortamı, tehditleri belirlemeyi ve güvenlik açıklarını değerlendirmeyi zorlaştırır ve bu görevlerin işbirlikçi ve yaratıcı bir şekilde ele alınmasını gerektirir.

4.1 Dünyada ve Türkiye'de BT Altyapısının Genel Durumu

BT, giderek daha fazla iç içe geçtiği EH sektörü ile birlikte (Genellikle Bilişim ve İletişim Sektörü -BİT olarak anılmaktadır) hayatın her alanında dönüşüme yol açmaktadır. BİT sektörü, doğrudan veya dolaylı olarak küresel ekonominin en önemli büyüme kaynağı hâline gelmiştir. 2022 yılı itibarıyla küresel BİT pazarının 5,3 trilyon dolara ulaştığı tahmin edilmekte[135] ve 2024 yılına kadar ortalama yüzde 5 oranında büyümesi beklemektedir. Küresel BİT sektörünün, 2022 yılında ilk kez 100 trilyon doları aşması beklenen küresel ekonominin[136] yüzde 5'inden fazlasını oluşturacağı tahmin edilmektedir. Türkiye'de BİT sektörünün büyüklüğünün 2020 yılı sonunda 26,9 milyar dolara çıktığı tahmin edilmektedir[137].

BİT sektöründe büyümeye yüksek harcamalar neden olmaktadır. Gartner Araştırma ve Danışmanlık şirketine göre, dünya genelinde BİT yatırımlarının tutarının 4,4 trilyon doları bulması beklenmektedir. Şirketin hesaplamalarına göre, 2022 yılında dünya genelinde veri merkezleri için 218,6 milyar dolar, yazılıma 675 milyar dolar, cihazlara 825 milyar dolar, BT hizmetlerine 1,27 trilyon dolar ve elektronik haberleşmeye ise 1,4 trilyon dolar harcanması beklenmektedir[138].

BİT sektörünün temel bileşenlerinin küresel pazardaki paylarına bakıldığında ise;

- Elektronik haberleşmenin yüzde 25,
- Cihazlar ve altyapı sektörünün yüzde 22,
- Bilişim ve işletme hizmetlerinin yüzde 20,
- Yeni teknolojilerin (IoT, blokzinciri, yapay zekâ vb.) yüzde 19,
- Yazılımların ise yüzde 14 pay aldığı görülmektedir.

BT altyapısının bileşenleri, birbirine bağımlı öğelerden oluşur ve iki temel bileşen grubu donanım ve yazılımdır. Donanım, çalışmak için yazılımı bir işletim sistemi gibi kullanır. Benzer şekilde, bir işletim sistemi, sistem kaynaklarını ve donanımı yönetir. İşletim sistemleri, ayrıca ağ bileşenlerini kullanarak yazılım uygulamaları ile fiziksel kaynaklar arasında bağlantılar da kurar. Veri merkezleri, sunucular, ağ anahtarları, yönlendiriciler (routers) ve kullanıcı terminalleri (taşınabilir veya sabit bilgisayarlar, tabletler, el terminalleri vb.) donanımları oluşturmaktadır. İşletim sistemleri, içerik yönetimi sistemleri ve analiz yazılımları da yazılım örneklerinden bazılarıdır.

Veri merkezleri, BİT altyapısının sinir merkezlerini oluşturmaktadır. Verileri depolamak ve işlemek için veri sunucularının tutulduğu alanlar olan veri merkezleri, dünya genelinde veri talebi katlanarak arttıkça hızla büyümüştür. Enerji tüketimi yüksek olduğu için genellikle elektrik fiyatlarının görece düşük olduğu bölgelerde kurulan veri merkezleri, bir kamu veya özel kuruluşa hizmet edebileceği gibi bulut bilişim teknolojisi ile çok sayıda kurum, kuruluş ve kişilere de hizmet verebilmektedir.

2021 yılı rakamlarına göre 110 ülkede yaklaşık 8.000 veri merkezi bulunmaktadır. Dünyadaki veri merkezlerinin yüzde 33'ü ABD, yüzde 5,7'si İngiltere, yüzde 5,5'i Almanya'da ve yüzde 5,2'si ise Çin'dedir. Ancak bu ülkenin veri merkezlerine yatırımlar hızla artmaktadır. Dünyada ortalama bir veri merkezi yaklaşık 10.000 m^2 iken[139], Çin bir milyon m^2den geniş bir alana yayılan dünyanın en büyük veri merkezine sahiptir. Çinlilere ilişkin verilerin Çin'de kalması şartını getiren Pekin yönetimi, ağırlıklı olarak ülkenin daha az gelişmiş batı bölgesinde olmak üzere sekiz bilişim merkezi ve 10 veri merkezi kümesi inşa etmeyi planlamaktadır[140]. Türkiye'de yarısından biraz fazlası İstanbul'da olmak üzere 72 veri merkezi bulunmaktadır[141].

BİT altyapısı açısından ikinci önemli unsur süper bilgisayarlardır. Veri merkezleri kadar geniş alanları kapsayabilen veya farklı coğrafyalardaki yüzlerce sunucu ve binlerce çekirdeği entegre biçimde kullanarak saniyede trilyonlarca işlem yapabilen süper bilgisayarların sayısı dünya genelinde artmaktadır. Türkiye'de İstanbul Teknik Üniversitesi ve Yıldız Teknik Üniversitesinin süper bilgisayarları bulunmaktadır.

Taşınabilir ve sabit bilgisayarlar ve işlem kapasitesi giderek artan akıllı cep telefonları da BT altyapısının önemli bileşenleridir. Dünyada 2021 yılında 340 milyonun üzerinde bilgisayar[142] ve 1,4 milyarın üzerinde[143] akıllı cep telefonu satılmıştır. Türkiye'de hane halklarının yüzde 57,25'inde bilgisayar bulunmaktadır ve her 100 kişiden yaklaşık 97'sinin cep telefonu aboneliği bulunmaktadır[144]. Akıllı cep telefonu kullanımının yaygınlaşmasıyla Türkiye'de internete erişebilenlerin oranı yüzde 92'yi bulmaktadır[145].

BİT kullanıcılarının her geçen gün artması, güvenli internet sunucularına olan ihtiyacı da artırmıştır. Bu sebeple, bir milyon kişilik nüfusa düşen güvenli internet sunucusu sayısı oldukça önemli bir istatistik olarak kabul edilmektedir[144]. Özellikle COVID-19 pandemisinde uzaktan çalışma, e-eğitim ve e-ticaret faaliyetlerinin

yoğunlaşması güvenli internet ağları yatırımlarının artırılmasını zorunlu kılmış, tüm ülkelerde kişi başına düşen güvenli internet sunucusunda artış meydana gelmiştir. Türkiye'de bir milyon kişiye düşen güvenli internet sunucusu sayısı 2019 yılında 5.438 iken, bu sayı 2020 yılında 6.760'a yükselmiştir. Buna karşılık ABD'de 141.000'in, Hollanda'da ise 137.000'in üzerinde güvenli internet sunucusu bulunmaktadır[144].

4.2 Kritik Bilişim Teknolojilerine Yönelik Tehditler

Bilişim teknolojileri altyapısı, tüm diğer kritik altyapılar gibi, terör, savaş, sabotaj ve doğal afetler riskleri ile karşı karşıyadır. Ancak günümüzde BT altyapısı için en önemli tehdit siber saldırılardır. Kritik altyapılar bankacılıktan sağlığa, enerjinin üretimi, iletimi ve dağıtımından su sistemlerine, ulaşımdan kritik üretim tesislerine kadar çok geniş bir alana yayıldığı için birçok farklı kontrol sistemini ve bilgi teknolojisini barındırmaktadır. Her sektör kendine has ihtiyaçları çerçevesinde farklı bilgi ve iletişim teknolojilerini kullanmaktadır. Söz konusu teknolojilerin kullanımı sektörlere bilgiyi hızlıca iletme ve yayma, süreçler üzerinde kontrol ve izleme, otomasyon, raporlama ve anlık geri bildirim gibi birçok kolaylık sağlıyor olsa da siber tehdit ve riskleri de beraberinde getirmektedir. Ayrıca kullanılan teknolojilerin çeşitliliği, kritik altyapılarda ortaya çıkabilecek tehditlerin de çeşitlenmesine; bununla beraber tüm kritik altyapı sektörlerine uygulanabilecek genelgeçer bir çözümün belirlenebilmesinin ise zorlaşmasına sebep olmaktadır[146].

Toplumların hayatına yön verebilme potansiyeli bulunan verinin dijital ortama taşınmasıyla, siber tehdit ve saldırıların doğası da değişmiştir. Geçmişte daha sade yöntemler, basit amaçlar ve belirli yetkinlikte kişiler tarafından gerçekleştirilen siber saldırılar artık bazen devletler düzeyinde, otomatik hâle getirilmiş; daha sık, karmaşık, yıkıcı, tespiti zor ve hedef odaklı olmaya başlamıştır.

Son dönemde yaşanan olaylar, ülkenin sınırlarını korumak kadar ülkenin verisinin ve dijital altyapılarının korunmasının önemini göstermiştir. Yapılan küresel araştırmalar, siber saldırıların 2021 yılında yıllık altı trilyon dolar tutarında zarara sebep olduğunu ve bu zararın 2025 yılında 10 trilyon doları aşabileceğini göstermektedir[147].

BİT sektörü, siber saldırıların hem silahı, hem savaş alanı hem de hedefi olabilmektedir. Siber saldırıların silahı yazılımlardır ve saldırılar bilişim altyapısı üzerinden yapılmaktadır. BİT sektörü siber saldırganların başlıca hedefleri arasındadır. Hatta bir siber güvenlik firmasının ölçümlerine göre, 2021 yılında bilişim ve iletişim firmalarına haftada 150.000'den fazla saldırı düzenlenmiştir[148]. 2020 yılında daha çok bankalar ve sigorta kuruluşlarını hedef alan siber saldırganların, bilişim firmalarının kamu ve özel sektör kuruluşları için geliştirdikleri yazılımlara sızabilmek için, BT firmalarının açık yazılım geliştirme platformlarını kullanmaya çalıştıkları belirtilmektedir[148].

Siber tehditler, saldırıyı gerçekleştirenlerin amaçlarına göre farklılıklar arz etmektedir (Tablo 6). Siber saldırıların yaklaşık dörtte üçünün siber suç kapsamında olduğu değerlendirmektedir.

Siber dünyada, bireylerin, işletmelerin, devletlerin ve siber güvenlik uzmanlarının dahi kendilerini ve kendi bilgi işlem servislerini korumalarını zorunlu kılan pek çok yol ve yöntem bulunmaktadır (Tablo 7). Siber saldırı tekniklerini kullanan kişiler sızdıkları bilgisayar ve bilgisayar sistemlerini değiştirilebilir, sunulan hizmeti aksatabilir, verileri silebilir veya erişilemez hâle getirebilir. Bu saldırılar, kişileri, işletmeleri veya kamu kurumlarını maddi zarara uğrattığı gibi ciddi itibar kaybı da yaratmaktadır.

Siber saldırılar öncelikle günümüzün en önemli kaynağı hâline gelen bilgi güvenliğini riske atmaktadır.

Bilgi güvenliği, fiziksel ve sayısal olarak tutulan verinin, yetkisiz erişimlerden, kullanımlardan, bozulmalardan veya değiştirmelerden korunmasıdır. Bilgi güvenliği, BİT sektörünün altyapısının ve sağladığı hizmetlerin güvenlik altına alınmasıyla sağlanabilir. Siber güvenlik, bilgisayarların, verinin ve ağların yetkisiz sayısal ataklardan, erişimden veya tahripten, çeşitli yöntem ve teknolojilerin kullanımı ile korunmasıdır.

Günümüzde verinin üretilmesi kadar güvenli olarak muhafaza edilmesi, gerekli yer ve zamanda kullanılabilecek şekilde transfer edilmesi önemle üzerinde durulması gereken bir husustur. Savunma ve güvenlik kapsamında fiziki güvenliğe paralel olarak siber güvenliğin de öne çıkarılması ve üretilen veri ve bilgilerin vatanın korunması gibi korunması gereklidir. Öte yandan günümüzde özel kuruluşların, ülkelerin ve diğer sorumlu kuruluşların bile orduya, merkez bankalarına, savunmalara yönelik önemli siber saldırılardan istisna olduğunu söylemek mümkün değildir. Siber saldırı tehdidi hızla büyümekte

	Motivasyon	Aktör	Hedef
Hacktivizm	Politik değişim, egoizm	Aktivist, hacktivist ve bireyler	Ülkeler, işletmeler ve bireyler
Siber Suç	Ekonomik, finansal	Suçlular	İşletmeler, kişiler ve çeşitli kazançlar
Siber Sabotaj	Bilgi çalma	Milletler ve organizasyonlar	Devletler, organizasyonlar ve bireyler
Siber Terörizm	Politik değişim, korku, politik, dini veya ideolojik amaçlar	Teröristler, milletler	Altyapılar, genel hedefler, organizasyonlar ve bireyler
Siber Savaş	Politik veya sosyal değişimler	Milletler, bireysel bilgisayar korsanları, terörist gruplar	Kritik altyapılar, ülkeler, askeri güçler, kritik hedefler

Tablo 6: Siber tehditlerin motivasyon, aktör ve hedef bakımından türleri[149].

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. Rastgele hedeflere yönelik olduğu gibi hedef gözeterek (spare-phishing) de yapılabilmektedir.	- 2020'de bildirilen siber saldırıların yüzde 80'ini oluşturmuştur[150]. - 2020'de her ay 200.000'den fazla oltalama sitesi kurulmuştur[151]. - Veri sızıntılarının ortalama maliyeti 2021'de 4,24 milyona çıkmıştır[152].
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.	- 2019'da şirketlere ve kuruluşlara vaka başına maliyeti 2,6 milyon dolara ulaşmıştır[153]. - 2020'de malware saldırıları bir önceki yıla göre yüzde 43 azalmasına rağmen, 5,6 milyar saldırı gerçekleşmiştir[154]. - Kötücül yazılım saldırıları işletmelerin ortalama 50 gün iş durdurmasına neden olmaktadır.
Hizmeti Engelleme (DoS/DDoS) Saldırıları	Siber saldırılar ile resmi bir kuruluşun ya da şirketin bilgi iletişim ağlarını kilitlemek ve verdiği hizmeti engellemeye çalışmaktır. Günümüzde hizmet engelleme saldırılarının büyük çoğunluğu virüslerle "zombi bilgisayar" (BOTNET) hâline getirilen birden çok bilgisayar kullanılarak gerçekleştirilmektedir.	- 2021 yılında yaklaşık 9,75 milyon DDoS saldırısı düzenlenmiştir[155]. - Dos ve DDoS saldırılarına maruz kalan şirketlerin her saat yaklaşık 20.000 ila 40.000 dolar zarar ettiği hesaplanmıştır[156].
Sosyal Mühendislik (Social Engineering) Saldırıları	İnsanlar arasındaki iletişimdeki ve davranışlardaki modelleri "zafiyetler" olarak tanımlayıp, bu zafiyetlerden faydalanarak güvenlik süreçlerini atlatma yöntemine dayanan eylemlere verilen isimdir. Hedefe güvenilir bir kaynak olduğunu hissettirmek, ortak tanıdıklar üzerinden yakınlık kurmak, özellikle iletişim araçları ile başkasını taklit etmek, gizlice zor bir durum oluşturarak yardım ediyormuş izlenimi vermek, hedef sistemin çöp olarak attığı kişisel bilgileri karıştırmak başvurulan yöntemler arasındadır.	- 2021 yılında sosyal mühendislik saldırıları yüzde 270 artmıştır[157]. - 2021'de çalışanların sosyal medya platformu Linkedin'e yapılan iki saldırıda bir milyardan fazla kişinin verileri çalınmıştır[157]. - Sosyal medyadan çalınan verilerle yapılan yolsuzlukların 30 milyar dolardan fazla zarara yol açtığı tahmin edilmektedir[157].
Gelişmiş Kalıcı Tehdit Saldırıları (Advanced Persistent Threat-APT)	Yetkisiz bir ağa erişildikten sonra orada tespit edilmeden erişilen ağda 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, ulusal savunma, imalat ve finans sektörü gibi bilgi değeri yüksek olan sektörler hedef alınarak gerçekleştirilir.	- 2021 yılında İran destekli Infy APT adlı grup, Avrupa, Ortadoğu ve Güney Asya'da büyük APT saldırıları gerçekleştirmiştir ancak verdikleri zarar belirli değildir[158]. - Kuzey Kore devleti destekli grupların 2010'ların ortalarında 150'den fazla ülkedeki bankalara aylarca süren operasyonlarla APT tipi siber saldırı düzenlediği, bir milyar doların üzerinde dolandırıcılık yaptığı ve Güney Kore ordusundan 200 terabayt bilgi çaldığı iddia edilmektedir[159].
Ortadaki Adam Saldırıları (MITM)	Ağda, iki bağlantı arasındaki iletişimin dinlenmesi ile çeşitli verilerin ele geçirilmesi veya iletişimi dinlemekle kalmayıp her türlü değişikliğin yapılmasını da kapsayan bir saldırı yöntemidir. MITM'de iki taraf arasındaki iletişim kesilebilir ya da yanıltıcı bir iletişim oluşturulabilir.	- Tespit etmek çok güç olduğu için kesin rakamlar belli olmamakla birlikte istismara yönelik siber saldırıların en az üçte birinde bu yöntemin kullanıldığı tahmin edilmektedir[160].

Tablo 7: Bazı siber saldırı yöntemleri ve yol açtıkları sonuçlara dair örnekler.

olup karşılık vermek, saldırıyı tespit etmek ve kaynağını bulmak konusunda sorunlar bulunmaktadır.

4.3 Türkiye'de Siber Güvenlik Durumu

Türkiye, bilişim teknolojilerini yoğun olarak kullanan bir ülke olarak siber saldırı riski altındadır. Ülkemize yönelik siber saldırılar; çoğunlukla elektronik haberleşme altyapısını ve kamu kurumları başta olmak üzere enerji, bankacılık, sağlık gibi kritik sektörlerde faaliyet gösteren kuruluşları hedef almaktadır. Ulusal Siber Olaylara Müdahale Merkezine (USOM) 2017 yılında 99.600, 2018'de 72.975, 2019'da 150.546, 2020'de 118.469 adet siber saldırı bildirilmiştir[128]. 2021 yılında ise 84.113 siber saldırı vakası kayıtlara geçmiştir. Bildirilen saldırı sayısı gerilemiş olmakla birlikte, Türkiye yoğun biçimde siber saldırı girişimlerine maruz kalmaktadır. Bazı tahminlere göre, bildirilmeyenlerle birlikte Türkiye'de 2021 yılında kurum ve kuruluşlarının maruz kaldığı siber saldırı sayısı 600.000'den fazladır ve saate 72 saldırı gerçekleşmiştir[161]. Ulaştırma ve Altyapı Bakanlığına göre yerli imkânlarla geliştirilen KASIRGA, AVCI ve AZAD uygulamaları ile 2020 yılı sonu itibariyle üç yılda Türkiye'yi

hedef alan 325.000 siber saldırı engellenmiştir[162]. Söz konusu saldırıların da yüzde 90'ından fazlasını Dağıtık Servis Dışı Bırakma (DDoS) ve Oltalama (Phishing) saldırıları oluşturmuştur[128].

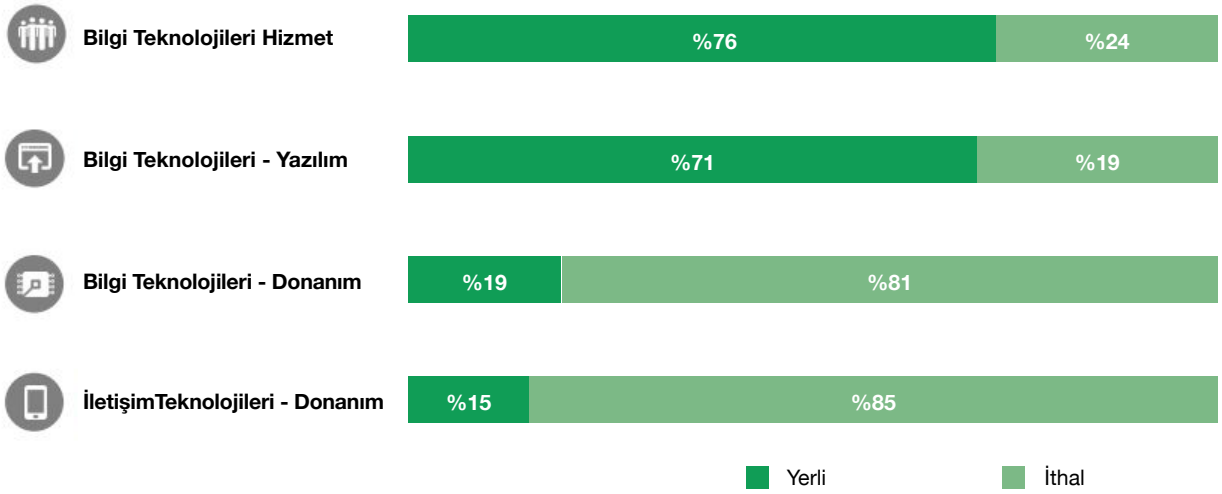
Türkiye önemli miktarda siber saldırıya maruz kalmakla birlikte, siber saldırılara karşı mücadele kapasitesi açısından dünya geneliyle karşılaştırıldığında ileri bir konumdadır. Uluslararası Telekomünikasyon Birliğinin (ITU), yasal tedbirler, teknik önlemler, kurumsal tedbirler ve kapasite geliştirme tedbirleri kriterleri üzerinden derecelendirme yaptığı "Küresel Siber Güvenlik Endeksi 2020"ye göre Türkiye 100 üzerinden 97,49 puanla 200'den fazla ülke arasında 11'inci sırada yer almıştır[163].

ITU Endeksi'nde Türkiye özellikle yasal düzenlemeler ve kurumsal tedbirler açısından yüksek puan elde etmiştir. Türkiye'de siber güvenlik alanında yasal tedbirler ve kurumsallaşma 2012 yılında Siber Güvenlik Kurulunun kurulması ile başlamıştır. Ardından 2013'te USOM kurulmuştur. Aynı yıl "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı"[164] yayınlanmıştır. Strateji ve Eylem Belgesi, 2016-2019 ve 2020-2023 dönemleri için güncellenerek yeniden yayınlanmıştır. Söz konusu belgelerin temel amacı ulusal siber güvenlik altyapısının güçlendirilmesi, bir başka deyişle tüm kamu kurum ve kuruluşlarının BT altyapılarıyla sunulan her türlü işlemin, oluşturulan verilerin ve bu verilerin kullanılmasındaki sistemlerin güvenliğinin sağlanmasıdır. Belgede ayrıca siber güvenlikte yerli teknolojilerin geliştirilmesi hedefi de yer almıştır. Stratejiler ve yol haritaları kapsamında önemli çalışmalar yapılmıştır.

- Bütün kamu kuruluşlarında siber olaylara müdahale ekipleri (SOME) kurulmuştur. Şubat 2022 itibariyle 2.074 SOME kurulmuştur[165]. Bunların bir kısmı kritik altyapı sektöründeki düzenleyici ve denetleyici kuruluşlarca kurulan "Sektörel SOME"ler, kalan kısmı ise kamu kurum, kuruluşları ve kritik altyapı sektörlerindeki özel kurumlar tarafından kurulan "Kurumsal SOME"dir.
- USOM faaliyete geçmiş SOME'ler arasında koordinasyonu sağlamaya başlamıştır.
- "SOME İletişim Platformu" kapsamında 6.099 siber güvenlik uzmanı platforma kayıt yaptırmıştır[165].Yerli imkânlarla siber saldırılara karşı KASIRGA, AVCI VE AZAD yazılımları geliştirilmiştir.
- Kurulan Siber İletişim Platformu (SİP) ile resmi siber saldırı uyarıları yapılmaktadır.
- Farklı kurumlar altında ayrı ayrı sürdürülen dijital dönüşüm (e-Devlet), siber güvenlik, milli teknolojiler, büyük veri ve yapay zekâ ile ilgili çalışmaların tek çatı altında toplanması amacıyla, 10 Temmuz 2018'de T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi kurulmuştur.
- Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, "Ülkemizin verisinin ülkemizde kalması, kurumların, şirketlerin ve hatta bireylerin veri mahremiyeti konusunda riskli yaklaşımlara karşı bilinçli olması, yerli ve milli çözümler geliştirilmesi ve kullanılması, karşılaşılan güvenlik risklerinin azaltılması, etkisiz kılınması ve özellikle gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına yol açabilecek kritik türdeki verilerin güvenliğinin sağlanması"[166] amacıyla Aralık 2019'da "Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi"[167] ve "Bilgi ve İletişim Güvenliği Rehberi"ni[131] hazırlamıştır. Rehberde, "Varlık Grupları Güvenliği Tedbirleri", "Uygulama ve Teknoloji Alanlarında Güvenlik Tedbirleri" ve " Sıkılaştırma Tedbirleri" ana başlıkları altında 659 adet tedbir sıralanmıştır.
- STM Savunma Teknolojileri, Mühendislik ve Ticaret A.Ş. (STM) ve Sakarya Üniversitesi işbirliği ile "Ulusal Test Yatağı Merkezi" Şubat 2021'de faaliyete geçmiştir[168]. Merkezin amacı elektrik enerji şebekesi ve su yönetiminden başlayarak Türkiye'nin tüm kritik altyapılarının modellenmesinin çıkarılıp, kritik altyapıların güvenliği ile alakalı koruyucu ve önleyici çözümlerin araştırılması ve geliştirilmesi amacıyla bir çalışma ortamının sunulması ve siber güvenlik ekosistemine katkıda bulunulmasıdır[169].
- Kamuya ait bilgi işleme kaynaklarının kontrol altında tutularak bir ortamda yönetilmesi, verilerin saklanması, işletilmesi ve tek bir noktadan sunulması için Ulusal Kamu Entegre Veri Merkezi (UKEVM) kurulması çalışmaları başlatılmıştır[170].
- T.C. Cumhurbaşkanlığı Savunma Sanayii Başkanlığı (SSB) tarafından, TSK'ye ait bilgi sistemlerinin siber güvenliğinin milli yazılımlar vasıtasıyla güçlendirilmesi ve TSK'nin siber olaylara anında tepki vererek söz konusu olayların muhtemel etkilerinin azaltılması amacıyla 2017 yılında SİSAMER projesi başlatılmıştır. Proje kapsamında, ihtiyaç duyulan siber güvenlik yazılımlarının milli olarak geliştirilmesi ve TSK bünyesinde gerçekleştirilen siber savunma faaliyetlerinin tek bir noktadan koordine edilmesini sağlayan Siber Savunma Harekât Merkezi kurulmuştur. Merkez, 2020 yılı ilk çeyreğinde milli olarak geliştirilen siber güvenlik yazılımlarını TSK'nin kullanımına sunmuştur[171].
- 2017 yılında SSB öncülüğünde bir Türkiye Siber Güvenlik Kümelenmesi kurulmuştur. Türkiye'nin siber güvenlik alanında teknoloji üreten ve dünya ile rekabet edebilen bir ülke hâline gelmesi ana hedefi doğrultusunda Türkiye'de siber güvenlik ekosisteminin geliştirilmesi amacıyla kurulan bir platform olan Türkiye Siber Güvenlik Kümelenmesine Mayıs 2022 itibariyle 203 kuruluş ve şirket üye olmuştur[172].
- Kamu kuruluşları arasında veri alışverişi güvenliğinin artırılması için KAMUNET ağı[173], savunma sektöründe faaliyet gösteren kamu ve özel kuruluşlar arasında güvenli veri değişimi için ise SAVNET kurulmuştur.

2012-2022 döneminde yasal düzenlemelerin yapılması, kurumsal yapıların kurulması, kılavuz belgelerin yayınlanması ve Ar-Ge merkezlerinin kurulmasıyla Türkiye, özellikle kritik altyapı ve verinin korunması açısından dünyada önde gelen bir ülke hâline gelmiştir.

Ancak "Bilgi ve İletişim Güvenliği Rehberi"nde belirtildiği üzere siber alanda "dünyanın hiçbir yerinde yüzde



Şekil 7: 2020 yılında Türkiye'de BİT sektöründe yerli ve ithal ürün ve hizmetlerin payları[175].

100 güvenlikten bahsetmek mümkün değildir[131]." Yine de insan, teknoloji, organizasyon yapısı, yasal düzenleme ile ulusal ve uluslararası işbirliği boyutlarının her birinde atılacak doğru ve bilinçli adımlarla yıkıcı etkilerden korunmak mümkündür. Türkiye'de kritik altyapının siber güvenliğinin pekiştirilmesi için atılması gereken adımlar bulunmaktadır. Bunların başında bilişim ve iletişim teknolojilerinde yerli ve milli donanım ve yazılımların geliştirilmesini teşvik etmek gelmektedir. Bu hedef, 2000'li yıllardan bu yana yayınlanan kalkınma planları, sektöre ilişkin strateji belgeleri ve yol haritalarının hepsinde yer almıştır[174]. BİT sektöründe yerli ve milli kaynakların geliştirilmesi stratejik kabul edilmekle birlikte sektörde yerli payı, özellikle donanımda düşük seviyelerde kalmaktadır (Şekil 7).

BİT sektöründe, özellikle donanım alanında yerli payını artırmak için bazı girişimler başlatılmıştır. Uçtan uça yerli ve milli 5G altyapısı geliştirme projesi bunlardan biridir ve testleri sürmektedir[134].

Nisan 2022 itibariyle Türkiye'de makineden makineye (M2M) mobil bağlantı aboneliğinin 7,4 milyona çıktığı[176] dikkate alınırsa, nesnelerin interneti donanımı ve yazılımında yerli ve milli çözümlerin artırılması da kritik önem kazanmaktadır. Bölüm 3.2'de belirtildiği üzere Türkiye, EH altyapı ekipmanları, mobil cihazlar, bilgisayarlar ve işlemciler konusunda da dışa bağımlı durumdadır.

BİT sektöründe dışa bağımlılık ithal BİT ekipmanlarının kullanıldığı alanlarda, özellikle kritik altyapıda büyük güvenlik zafiyeti yarattığı gibi büyük bir ekonomik kayıp yaratmaktadır. Sadece SSB Siber Güvenlik ve Bilişim Sistemleri Dairesinde yürütülen projelerde yıllık 200 milyon dolara yakın bir harcama olduğu belirtilmektedir[177]. Bilişimde dışa bağımlılık stratejik önem de kazanmıştır. Bugün "dijital uçurum" dünyanın en önemli sorunlarından biri hâline gelmiştir[178]. Dijital uçurum, ağ ve bilgi teknolojilerinin hızlı gelişimi ile dinamik ve acil bir konu hâline gelmiştir. Bilgi ve iletişim teknolojilerinin gelişimi, bütünleştirici sosyoekonomik süreçlere ivme kazandırmaktadır. Ancak aynı zamanda çeşitli insan grupları, bölgeler ve ülkeler arasında büyüyen bir kutuplaşma yaratmaktadır[179]. Bu nedenle Türkiye'nin BİT alanında ithalatçı konumdan çıkıp teknoloji geliştiren ve ihraç eden ülke hâline gelmesi stratejik önem taşımaktadır.

4.4 Türkiye'de Siber Güvenliğin Artırılması İçin Öneriler

Hayatın hemen her alanında merkezi bir rol edinmiş olan bilgi ve iletişim teknolojileri, sağladığı geniş imkânlar yanında güvenlik risklerini de beraberinde getirmektedir. Bugün siber güvenlik, farklı kurumların, sektör ve paydaşların sorumluluklarıyla kesişen çok boyutlu, stratejik ve "bütüncül" olarak ele alınması gereken bir konu hâline gelmiştir. STM ThinkTech, bu amaçla 3 Kasım 2021'de farklı kurumlardan paydaşların katıldığı "Bütünleşik Güvenlik Bağlamında Siber" başlıklı bir odak toplantısı düzenlemiştir[177]. Toplantıya katılan uzmanlar siber güvenlik alanında önemli hususların altını çizmişlerdir. Bu bölümde söz konusu hususlar ve öneriler özetlenmeye çalışılacaktır.

4.4.1 Son Kullanıcılar Uygulamalı Olarak Bilinçlendirilmeli

Tüm dünyada olduğu gibi Türkiye'de de siber güvenlik konusunda hazırlanan strateji ve yol haritalarında kurum içinde ve kurumların değer zincirindeki tüm paydaşların siber güvenlik konusunda farkındalığının artmasının öneminin altı çizilmektedir. Bu konunun önemi odak toplantısında da gündeme gelmiştir. SSB Siber Güvenlik ve Bilişim Sistemleri Daire Başkanı Muhammet Sami Ulukavak, savunma sanayiinde son dönemde yaşanan siber saldırı vakalarına, son kullanıcının çok kolay tespit edilebilir, öngörülebilir, sosyal mühendislikle çok rahat elde edilebilir parolalar belirlemesi nedeniyle maruz kalındığına dikkat çekmiştir. Ulukavak, "Siber güvenlikle ilgili en önemli tedbirler, son kullanıcıya ilişkin alınacak tedbirlerdir. Böylelikle muhtemelen siber güvenlikle ilgili sorunların yüzde 70-80'ini aşmak da mümkün olacaktır. Çok basit uygulama, düzenleme ya da politikalarla

tedbirler alabiliriz. Spektrumun bir ucu böyleyken, diğer ucu da aslında işin uygulanması zor ve çok para harcamanız gereken tarafıdır" demiştir.

TUSAŞ Yazılım Mühendisliği Direktörü Güray Yıldız, eğitime daha fazla ağırlık vererek farkındalığın artırılması görüşündedir. Yıldız, "Siz ne kadar güçlü bir sistem oluşturursanız oluşturun en zayıf halka kadar güçlüsünüz. Bu en zayıf halka da son kullanıcıdır" görüşünü savunmuştur.

Son kullanıcıların siber güvenlik farkındalığının artması için eğitim gerektiği, toplantıda sık sık dile getirilmiştir. Örneğin Trend Micro Bölge Müdürü Serbülend Zeren, "siber güvenlikli insan" yetiştirilmesine ilkokulda başlanması gerektiği görüşündedir.

TÜBİTAK BİLGEM Siber Güvenlik Hizmetleri Birim Yöneticisi Abdurrahman Emre Özkök ise örgün eğitim yerine uygulamalı bilinçlendirme çalışmalarının önemine işaret etmiştir. Özkök, son kullanıcıların, özellikle sosyal mühendislik sızıntılarına karşı savunmasız olduğunu belirtmiş, ancak bu sorunun farkındalık eğitimleri veya yayınlar yoluyla sağlanmasının güç olduğunu kaydetmiştir. Özkök, eğitim çalışmaları yerine kuruluşlarda sızıntı testlerinin yapılmasını önermektedir: "İnsanlar maalesef bir şeyleri yaşamadan tam olarak sosyal mühendislikle ilgili sızma testleri yapıyoruz. Maalesef çoğunlukla yüksek başarı oranında sonuçlarla karşılaşıyoruz. Bu çalışma sonucunda kurumun bir farkındalığı oluşuyor."

4.4.2 Yerli ve Milli Donanım ve Siber Çözümler Geliştirilmeli

Bilişim ve iletişim teknolojileri altyapısının siber güvenliğinin sağlaması, ön önemli konulardan biridir. STM'nin "Bütünleşik Güvenlik Bağlamında Siber" başlıklı odak toplantısına katılan uzmanlar donanım ve yazılım olarak yerli ve milli üretimin teşvik edilmesinin stratejik önemde olduğunu kaydetmişlerdir.

Donanım açısından yerli çözüm geliştirilmesi gereken ürün yarı iletkenler ve daha spesifik olarak mikroçiplerdir. STM Teknoloji Genel Müdür Yardımcısı Enis Müçteba Memiş, Türkiye'nin savunma sanayiinde geliştirilen sistemlerde ithal çiplerin kullanıldığına dikkat çekip, "İşlemcilerimizin içine gömdüğümüz çiplerin güvenliğine dair pek çok bilinmeyen var. Bu bizim için ciddi tehditlerden biri. Bununla ilgili yapılacak en önemli girişim Türkiye'de bir çip yatırımının başlatılması" görüşünü savunmuştur.

Türk Telekom Siber Güvenlik Direktörü Mahmut Küçük ise, EH güvenliği için özellikle yerli ve milli cep telefonu geliştirilmesinin önemini vurgulamıştır. Mahmut Küçük, "Üretim, üretim, üretim diyoruz. Kendi donanımımızı, yazılımımızı, işletim sistemimizi, güvenlik ürünlerimizi ve mobil uygulamalarımızı üretebilme hedefiyle ilerlememiz lazım. Kullandığımız bütün erişim araçlarında, elektronik ekipmanlarda bunları sağlamamız gerekiyor" şeklinde ifade etmiştir.

SSB Siber Güvenlik ve Bilişim Sistemleri Daire Başkanı Muhammet Sami Ulukavak ise yerli siber güvenlik çözümlerinin gerekliliğine dikkat çekmiştir. Ulukavak, "SSB olarak milli ürün kullanımını artırmanın çok önemli olduğunu düşünüyoruz. Savunma sanayiinde, siber güvenlikten önce epeyce bir yol katetmiş vaziyetteyiz ama siber güvenlik sektöründe, savunma sektörünün 15 sene gerisindeyiz gibi görünüyor. Fakat yavaş yavaş ilerliyoruz" ifadelerini kullanmıştır.

Sakarya Üniversitesi Kritik Altyapılar Ulusal Test Yatağı Merkezi Koordinatörü Prof. Dr. İbrahim Özçelik ise Endüstriyel Kontrol Sistemleri (EKS) siber güvenliği konusunda uzman ve yazılım eksikliğine çözüm bulunması gerektiğini belirtmiştir. Prof. Özçelik, "EKS donanımları ve bunların üzerinde çalışan yazılımlar yabancı. Bu sistemlerin güvenliğini sağlayacak siber güvenlik yazılımlarımız da yabancı. Dolayısıyla neyin siber güvenliğinden bahsettiğimiz burada büyük bir soru işareti hâline geliyor"

ifadelerini kullanmıştır. Prof. Özçelik üniversitenin STM ile birlikte kurduğu Ulusal Test Yatağı Merkezinin öncelikli amacının bu açığı kapatmak olduğunu, öncelikli alan olarak elektrik ve su altyapısını seçtiklerini, ancak petrol, doğalgaz, ulaştırma gibi diğer kritik altyapılarla ilgili test yatağı merkezlerinin kurulması gerektiğini vurgulamıştır.

TUSAŞ Yazılım Mühendisliği Direktörü Güray Yıldız da yerli ve milli donanım ve yazılım ihtiyacı olduğu görüşündedir. Yıldız, "Bizim en başta işletim sistemi, sonra donanım tasarımı ve kendi yazılımlarımızı geliştirmemiz lazım. Biz bu bilinçle projemizi kurguladık, işletim sistemi ve donanım anlamında TÜBİTAK BİLGEM ile beraber çalışıyoruz" demiştir.

4.4.3 Sürdürülebilir Siber Güvenlik Anlayışı Geliştirilmeli

Siber güvenlikte önemli kavramlardan biri de sürdürülebilirliktir. Siber saldırıların 7/24 sürdüğünün altını çizen STM Odak Toplantısı katılımcıları, özellikle hem kamu kuruluşları hem de özel sektörü kapsayacak kalıcı mekanizma ve kurumların kurulmasının gerektiğini vurgulamışlardır.

SSB Siber Güvenlik ve Bilişim Sistemleri Daire Başkanı Muhammet Sami Ulukavak, "Farkındalık ve bilinç oluşturmamız gereken konulardan biri sürdürülebilir güvenliktir. Bugün aldığımız tedbirler bugünün tehditlerine karşı bir koruma sağlıyor, yarın eskimiş oluyor. Onun için siber güvenlikte tedbirlerimizi periyodik olarak alabilecek bir mekanizma kurgulamak gerekiyor" demiş ve ortak kriterler üzerine inşa edilecek bir sertifikasyon projesi geliştirilebileceğini belirtmiştir.

Kamu tarafında sivil kurum ve kuruluşlar için bir ortak operasyon merkezi kurulabileceğini belirten STM Teknoloji Genel Müdür Yardımcısı Enis Müçteba Memiş, bu tür bir merkezin, güvenlik kurumları tarafından da kurulması önerisinde bulunmuştur.

Farklı sektörlere ilişkin siber kurulların oluşturulması da toplantıda dile getirilmiştir. TUSAŞ Yazılım Mühendisliği Direktörü Güray Yıldız, havacılık sanayiinde bir Siber Güvenlik Kuruluna ihtiyaç olduğunu düşünmektedir. Bu kurul, hava aracı platformuna uçuş izni verirken, sistemi siber güvenlik açısından değerlendirip izin vermelidir. Yapı Kredi Teknoloji Bilgi Sistemleri Güvenlik Yönetimi Genel Müdür Yardımcısı Ahmet Gökhan Yalçın ise daha genel kapsamlı bir kurul önermektedir. Yalçın, ülkemizdeki kamu ve özel bütün kurumları etkileyen herhangi bir saldırının istihbaratının, ülke çapında güvenli bir şekilde paylaşılacağı bir ortam oluşturacak bir "ulusal tehdit istihbarat ağı" oluşturulması gerektiğini vurgulamıştır. Türk Telekom Siber Güvenlik Direktörü Mahmut Küçük ise, daha kapsamlı bir kuruluş önermektedir. Küçük, Türkiye'de "insan kaynağı da yetiştirecek üst seviye bir organizasyon" kurulması gerektiği görüşünü savunmuştur.

4.4.4 Siber Güvenlik İçin İnsan Kaynakları Geliştirilmeli

Sakarya Üniversitesi, Kritik Altyapılar Ulusal Test Yatağı Merkezi Koordinatörü Prof. Dr. İbrahim Özçelik, sektörün şu anda siber güvenlikle ilgili çok ciddi yetişmiş uzman insan kaynağına ihtiyacı olduğunu dile getirmektedir: "Ulusal Siber Güvenlik Eylem Planları -eğer buna önem veriyorsa- ile bu programlar çok rahat açılabilir. Bunun adı siber güvenlik mühendisliği olmayabilir, bilgi güvenliği mühendisliği olabilir. Eğer böyle bir program söz konusu olmazsa da, şu anda SSB'nin siber güvenlik kümelenmesi Türkiye'de otorite olarak üstte görünüyor. Dolayısıyla üniversitelerle özel sektör bir araya getirilerek bu tür eğitim programları açılabilir ve sektörün ihtiyacı olan uzman insan kaynağı yetiştirilebilir."

TUSAŞ Yazılım Mühendisliği Direktörü Güray Yıldız, siber güvenlik konusunda eğitimin genellikle yüksek lisans seviyesinde olduğunu; bunun lisans, hatta STM'nin de ortağı olduğu İstanbul Teknopark tarafından İstanbul'da açılan Siber Güvenlik Mesleki ve Teknik Anadolu Lisesi'nin gösterdiği başarıdan feyz alınarak lise seviyesine çekilmesi gerektiğini belirtmiştir.

5. SONUÇ

Kritik altyapıların güvenliğini ele aldığımız Araştırma Raporumuzun ikinci bölümünde ulaştırma, haberleşme ve bilişim teknolojileri sektörleri ele alınmıştır. Bu üç sektör küresel ekonominin en geniş ve en dinamik sektörleri olup yeni teknolojilerle birlikte inovasyon eksenleri hâline gelmişlerdir. Söz konusu sektörler, aynı zamanda diğer sektörlerin verimi için büyük önem taşıdığı gibi toplumsal ve kültürel alanlara da şekil vermektedir. Bu açıdan ulaştırma, haberleşme ve bilişim sektörlerini zamanın sinir sistemi ve hatta "zamanın ruhu" olarak görmek de mümkündür.

Son derece önemli üç sektörün kritik altyapısının korunmasını yakın gelecekte sadece "bilgi güvenliği" olarak nitelemek mümkündür. Elektronik haberleşme ve bilişim teknolojileri öteden beri veriye odaklanmıştır. Elektrikli ve sürücüsüz araçların yaygınlaşması, akıllı yol ağları ve kontrol sistemleri ile ulaşım sistemleri de veri ve bilgi odaklı hâle gelmektedir.

Bu açıdan bakıldığında söz konusu sektörlerde kritik altyapının korunmasında temel riskin siber güvenlik olacağı öngörüsü ağırlık kazanmaktadır. STM ThinkTech Koordinatörü Emekli Korgeneral Alpaslan Erdoğan'ın "Bütünleşik Güvenlik Bağlamında Siber" odak toplantısında belirttiği üzere, "Günümüzde verinin üretilmesi kadar güvenli olarak muhafaza edilmesi, gerekli yer ve zamanda kullanılabilecek şekilde transfer edilmesi" önemle üzerinde durulması gereken bir konudur. Savunma ve güvenlik kapsamında fiziki güvenliğe paralel olarak siber güvenliği de öne çıkarmamız ve ürettiğimiz veri ve bilgileri de "artık sınırlarımızı ve vatanımızı koruduğumuz gibi korumamız gerekmektedir".

KAYNAKÇA

[1] Genco, Abdullah; (2021), "TÜRKİYE'DE KRİTİK ALTYAPI VE KRİTİK ALTYAPIYA YÖNELİK TEHDİTLER", *Dergipark*, (12 Ocak 2021), https://dergipark.org.tr/tr/download/article-file/1456164. (Erişim Tarihi: 21 Haziran 2022)

[2] *United States Environmental Protection Agency*, "Climate Impacts on Transportation", https://19january2017snapshot.epa.gov/climate-impacts/climate-impacts-transportation_.html#:~:text=Key%20Points,and%20capacity%20of%20transportation%20systems. (Erişim Tarihi: 21 Haziran 2022)

[3] A. Mack, Elizabeth; (2021), "The impacts of the COVID-19 pandemic on transportation employment: A comparative analysis", *ScienceDirect*, (Aralık 2021), www.sciencedirect.com/science/article/pii/S2590198221001755. (Erişim Tarihi: 21 Haziran 2022)

[4] *Statista*, "Global container freight rate index from January 2019 to May 2022", https://www.statista.com/statistics/1250636/global-container-freight-index/. (Erişim Tarihi: 21 Haziran 2022)

[5] *IRU*, (2021), "COVID-19 Impact on the Road Transport Industry", (Haziran 2021), https://www.itf-oecd.org/sites/default/files/docs/covid-19_impact_on_the_road_transport_industry_-_june_2021.pdf. (Erişim Tarihi: 21 Haziran 2022)

[6] *ic4r.net*, (2020), "How resilient is the Turkish transportation system? Lessons learnt from COVID-19", https://www.ic4r.net/wp-content/uploads/2020/10/Network-Industries-Turkey-Volume-1-Issue-1-September.pdf. (Erişim Tarihi: 21 Haziran 2022)

[7] Joi, Priya; (2020), "5 reasons why pandemics like COVID-19 are becoming more likely", (10 Haziran 2020), https://www.gavi.org/vaccineswork/5-reasons-why-pandemics-like-covid-19-are-becoming-more-likely?gclid=Cj0KCQjwvLOTBhCJARIsACVldV-1KaBJgZMGA5GyUKjCV7k6M2wdmNI5LPksGy4zP-Svp_Ni-1GkqOwr0aAmhnEALw_wcB. (Erişim Tarihi: 21 Haziran 2022)

[8] Yong, Ed; (2022), "We Created the 'Pandemicene'", *Atlantic*, (28 Nisan 2022), https://www.theatlantic.com/science/archive/2022/04/how-climate-change-impacts-pandemics/629699/. (Erişim Tarihi: 21 Haziran 2022)

[9] Thomas, Leigh; (2019), "French 'Yellow Vests' protests cost 0.2 percentage points of growth - Le Maire", *Reuters*, (28 Şubat 2019), https://www.reuters.com/article/uk-france-economy-gdp-idUKKCN1QH17P. (Erişim Tarihi: 21 Haziran 2022)

[10] *United Nations News*, (2021), "With 1.3 million annual road deaths, UN wants to halve number by 2030", (3 Aralık 2021), https://news.un.org/en/story/2021/12/1107152. (Erişim Tarihi: 21 Haziran 2022)

[11] *Dünya*, (2013), "Yolların kilidini açan Ro Ro yatırımcıların yıldızı oldu", (25 Aralık 2013), https://www.dunya.com/sektorler/lojistik/yollarin-kilidini-acan-ro-ro-yatirimcilarin-yildizi-oldu-haberi-232115. (Erişim Tarihi: 21 Haziran 2022)

[12] *Start*, "SEARCH RESULTS: 201183 INCIDENTS", https://www.start.umd.edu/gtd/search/Results.aspx?charttype=pie&chart=target&casualties_type=&casualties_max. (Erişim Tarihi: 21 Haziran 2022)

[13] *Frachtbox*, (2021), "SEARCH RESULTS: 201183 INCIDENTS", (5 Eylül 2021), https://www.frachtbox.com/blog/cargo-theft-in-the-transport-industry. (Erişim Tarihi: 21 Haziran 2022)

[14] *Safety4Sea*, (2018), "Maersk Line: Surviving from a cyber attack", (31 Mayıs 2018), https://safety4sea.com/cm-maersk-line-surviving-from-a-cyber-attack/. (Erişim Tarihi: 21 Haziran 2022)

[15] *Guardian*, (2021), "'Cyber-attack' hits Iran's transport ministry and railways", (11 Temmuz 2021), https://www.theguardian.com/world/2021/jul/11/cyber-attack-hits-irans-transport-ministry-and-railways. (Erişim Tarihi: 21 Haziran 2022)

[16] Gallagher, Ryan; (2022), "Belarus Hackers Allegedly Disrupted Trains to Thwart Russia", *Bloomberg*, (28 Şubat 2022), https://www.bloomberg.com/news/articles/2022-02-27/belarus-hackers-allegedly-disrupted-trains-to-thwart-russia. (Erişim Tarihi: 21 Haziran 2022)

[17] Kurnaz, Salim; Karatepe, Belma; (2019), "KAMUSAL KRİTİK TESİSLERİN GÜVENLİĞİ KAPSAMINDA TÜRKİYEDEKİ HAVA ALANLARININ SİBER GÜVENLİĞİ", *ASSAM*, (23 Eylül 2019), https://dergipark.org.tr/tr/pub/assam/issue/48907/573927. (Erişim Tarihi: 21 Haziran 2022)

[18] Telli, Resul; (2020), "TÜRKİYE'DE ULAŞIM ALTYAPISININ BÖLGESEL KALKINMAYA ETKİLERİ", *Türk Sosyal Bilimler Araştırmaları Dergisi*, (Nisan 2020), http://tursbad.hku.edu.tr/tr/download/article-file/1079424. (Erişim Tarihi: 21 Haziran 2022)

[19] Alpar, Güray; (2020), "Ulaşım Ağı ve Altyapısı Güvenliği Kritik Altyapı ve Tesislerin Korunması", Nobel Yayınları, (Temmuz 2020), https://www.academia.edu/44396192/Hava_Ula%C5%9F%C4%B1m%C4%B1_Kritik_Altyap%C4%B1lar%C4%B1n%C4%B1n_G%C3%BCvenli%C4%9Fi. (Erişim Tarihi: 21 Haziran 2022)

[20] *SUSTAINABLE MOBILITY FOR ALL*, "Global Roadmap of Action Toward Sustainable Mobility", https://www.sum4all.org/gra. (Erişim Tarihi: 21 Haziran 2022)

[21] *Research4Committees*, (2022), "The future of transport in the context of the Recovery Plan: Overview briefing", (Ocak 2022), https://research4committees.blog/2022/01/27/the-future-of-transport-in-the-context-of-the-recovery-plan-overview-briefing/#:~:text=The%20EU's%20main%20transport%20policy,the%20transport%20system%20more%20resilient. (Erişim Tarihi: 21 Haziran 2022)

[22] *T.C. Ulaştırma ve Altyapı Bakanlığı*, "Ulusal Akıllı Ulaşım Sistemleri Strateji Belgesi ve 2020-2023 Eylem Planı", https://www.uab.gov.tr/uploads/announcements/ulusal-akilli-ulasim-sistemleri-strateji-belgesi-v/ulusal-akilli-ulas-im-sistemleri-strateji-belgesi-ve-2020-2023-eylem-plani.pdf. (Erişim Tarihi: 21 Haziran 2022)

[23] VANDYCKE, NANCY; VIEGAS, JOSÉ; (2020), "Cost-benefit of building resilience in transport systems: What do we know?", *World Bank*, (27 Ekim 2020), https://blogs.worldbank.org/transport/cost-benefit-building-resilience-transport-systems-what-do-we-know. (Erişim Tarihi: 21 Haziran 2022)

[24] Rozenberg, Julie; (2019), "FROM A ROCKY ROAD TO SMOOTH SAILING Building Transport Resilience to Natural Disasters", *World Bank*, https://openknowledge.worldbank.org/bitstream/handle/10986/31913/From-A-Rocky-Road-to-Smooth-Sailing-Building-Transport-Resilience-to-Natural-Disasters.pdf?sequence=1&isAllowed=y. (Erişim Tarihi: 21 Haziran 2022)

[25] Rebally, Aditya; (2021), "Flood Impact Assessments on Transportation Networks: A Review of Methods and Associated Temporal and Spatial Scales", *Frontiersin*, (21 Eylül 2021), https://www.frontiersin.org/articles/10.3389/frsc.2021.732181/full. (Erişim Tarihi: 21 Haziran 2022)

[26] *World Bank*, "STRENGTHENING RESILIENCE IN THE TRANSPORT SECTOR", https://thedocs.worldbank.org/en/doc/705861593475198613-0090022020/original/RIRGlobalTF0A320520200617.pdf. (Erişim Tarihi: 21 Haziran 2022)

[27] Hirata, Enna; (2021), "Shipping Digitalization and Automation for the Smart Port", (3 Aralık 2021), *IntechOpen*, https://www.intechopen.com/online-first/80276. (Erişim Tarihi: 21 Haziran 2022)

[28] Donnelly, Jack; (2021), "How can digital twins help ports?", *Port Technology*, (20 Temmuz 2021), https://www.porttechnology.org/news/how-can-digital-twins-help-ports/. (Erişim Tarihi: 21 Haziran 2022)

[29] Rivero, Nicolás; (2022), "Japan is home to the world's first autonomous container ships", *Quartz*, (12 Şubat 2022), https://qz.com/2126751/japan-is-home-to-the-worlds-first-autonomous-container-ships/. (Erişim Tarihi: 21 Haziran 2022)

[30] *Digital Twin Unit*, "Case Study: Hong Kong International Airport Terminal 1", https://www.digitaltwinunit.com/media/4742/hong-kong-international-airport-case-study.pdf. (Erişim Tarihi: 21 Haziran 2022)

[31] *Cyber Management*, (2021), "easyJet Cyber-attack Timeline", (30 Mart 2021), https://www.cm-alliance.com/cybersecurity-blog/easyjet-cyber-attack-timeline. (Erişim Tarihi: 21 Haziran 2022)

[32] Briginshaw, David; (2022), "Italian railway IT system suffers major cyber-attack", *International Railway Journal*, (29 Mart 2022), https://www.railjournal.com/infrastructure/italian-railway-it-system-suffers-major-cyber-attack/. (Erişim Tarihi: 21 Haziran 2022)

[33] *Euronews*, (2022), "Oil terminals disrupted after European ports hit by cyberattack", (3 Şubat 2022), https://www.euronews.com/2022/02/03/oil-terminals-disrupted-after-european-ports-hit-by-cyberattack. (Erişim Tarihi: 21 Haziran 2022)

[34] Tabak, Nate; (2022), "Oil terminals disrupted after European ports hit by cyberattack", *FreightWaves*, (7 Şubat 2022), https://www.freightwaves.com/news/minnesota-trucking-company-hit-in-2nd-ransomware-attack. (Erişim Tarihi: 21 Haziran 2022)

[35] Bailie, Malcolm; (2021), "The Cyber Risks of Transportation's Connected OT/IoT Systems", *Automation*, (9 Şubat 2021), https://www.automation.com/en-us/articles/february-2021/cyber-risks-transportation-connected-ot-iot-system. (Erişim Tarihi: 21 Haziran 2022)

[36] *Highways*, (2019), "Report warns 3,000 people could die in connected car cyber attacks", (6 Ağustos 2019), https://www.highwaysmagazine.co.uk/report-warns-3000-people-could-die-in-connected-car-cyber-attacks/7922. (Erişim Tarihi: 21 Haziran 2022)

[37] Timur, Mustafa Caner; (Editörler: Çalışkan, Zehra Doğan; Beşballı, Sinem Gözde); (2021), "TÜRKİYE'DE ULAŞTIRMA SEKTÖRÜNÜN GELİŞİMİ VE EKONOMİDEKİ ÖNEMİ", *Academia*, https://www.academia.edu/attachments/78216129/download_file?st=MTY1MDg5MjE4NCw5NC41NC4yMzIuMjM0LDM0NjYwNDE%3D&s=profile. (Erişim Tarihi: 21 Haziran 2022)

[38] Türkiye Cumhuriyeti Çevre, Şehircilik ve İklim Değişikliği Bakanlığı, "10.2 Ulaştırma Türlerine Göre Taşınan Yolcu ve Yük Miktarı", https://cevreselgostergeler.csb.gov.tr/ulastirma-turlerine-gore-tasinan-yolcu-ve-yuk-miktari-i-85789. (Erişim Tarihi: 21 Haziran 2022)

[39] *UTİKAD*, (Utikad verilerinden derlenmiştir). https://www.utikad.org.tr/. (Erişim Tarihi: 21 Haziran 2022)

[40] *Ulaştırma ve Altyapı Bakanlığı Karayolları Genel Müdürlüğü*, "Devlet ve İl Yolları Envanteri", https://www.kgm.gov.tr/sayfalar/kgm/sitetr/istatistikler/devletveilyolenvanteri.aspx. (Erişim Tarihi: 21 Haziran 2022)

[41] *Ulaştırma ve Altyapı Bakanlığı Karayolları Genel Müdürlüğü*, "Yol Ağı Bilgileri", https://www.kgm.gov.tr/Sayfalar/KGM/SiteTr/Kurumsal/YolAgi.aspx. (Erişim Tarihi: 21 Haziran 2022)

[42] *Ulaştırma ve Altyapı Bakanlığı Karayolları Genel Müdürlüğü*, "Tünel Bilgileri", https://www.kgm.gov.tr/Sayfalar/KGM/SiteTr/Projeler/TunelProjeleri.aspx#:~:text=T%C3%BCnel%20Bilgileri,art%C4%B1%C5%9Fla%20651%20km'ye%20ula%C5%9Ft%C4%B1r%C4%B1lm%C4%B1%C5%9Ft%C4%B1r. (Erişim Tarihi: 21 Haziran 2022)

[43] *Ulaştırma ve Altyapı Bakanlığı Karayolları Genel Müdürlüğü*, "KARAYOLLARI GENEL MÜDÜRLÜĞÜ SORUMLULUĞUNDAKİ DEVLET VE İL YOLLARI ÜZERİNDE BULUNAN VİYADÜK VE KÖPRÜLERİN YILLARA GÖRE

TOPLAM SAYI VE UZUNLUKLARI", https://www.kgm.gov.tr/SiteCollectionDocuments/KGMdocuments/Istatistikler/KopruveTunelBilgileri/kopruenvanterbilgileri.pdf. (Erişim Tarihi: 21 Haziran 2022)

[44] Nogay, Gazi; (2022), "Yeni Zigana Tüneli'nde ışık göründü", *Anadolu Ajansı*, (13 Ocak 2022), https://www.aa.com.tr/tr/gundem/yeni-zigana-tunelinde-isik-gorundu/2472916. (Erişim Tarihi: 21 Haziran 2022)

[45] *Ulaştırma ve Altyapı Bakanlığı Karayolları Genel Müdürlüğü*, "Önemli ve Global Projeler", https://www.kgm.gov.tr/Sayfalar/KGM/SiteTr/Projeler/UluslararasiProjeler/uluslararasiYolGuzargahi.aspx. (Erişim Tarihi: 21 Haziran 2022)

[46] *Ulaştırma ve Altyapı Bakanlığı*, (2020), "Veri Seti Ocak 2021", (23 Şubat 2020), https://sgb.uab.gov.tr/uploads/pages/istatistikler/2021-01-veriseti.pdf. (Erişim Tarihi: 21 Haziran 2022)

[47] T.C. *Ulaştırma ve Altyapı Bakanlığı*, "ULAŞAN VE ERİŞEN TÜRKİYE İSTATİSTİKLERİ 2003-2023", https://sgb.uab.gov.tr/uploads/pages/yayin-sunum-ve-tablolar/istatistik-2003-2020.pdf. (Erişim Tarihi: 21 Haziran 2022)

[48] Özgan, Osman; (2022), "Taşımacılık üssü olacağız: Lojistik merkezi yirmi beşe çıkacak", *Yeni Şafak*, (7 Mart 2022), https://www.yenisafak.com/ekonomi/tasimacilik-ussu-olacagiz-lojistik-merkezi-yirmi-bese-cikacak-3768305#:~:text=T%C3%BCrkiye%27nin%20bir%20ula%C5%9F%C4%B1m%20koridoruna,olan%2010%20lojistik%20merkezi%20vard%C4%B1r. (Erişim Tarihi: 21 Haziran 2022)

[49] Saraç, Zeliha; (2022), "Antrepolarda yer yok", *Bloomberg*, (6 Nisan 2022), https://www.bloomberght.com/antrepolarda-yer-yok-2303320. (Erişim Tarihi: 21 Haziran 2022)

[50] *Unimar*, (2021), "E-Ticaret Depolama Hizmetlerine Hız Kattı", (8 Ekim 2021), https://globelink-unimar.com/e-ticaret-depolama-hizmetlerine-hiz-katti/. (Erişim Tarihi: 21 Haziran 2022)

[51] *Intermodal*, "Intermodal Rail: Three Ways to Greater Value for Shippers", http://www.intermodal.com/index.cfm/resource-center/information-kits/intermodal-101-part-two-the-benefits-of-intermodal-rail-shipping/. (Erişim Tarihi: 21 Haziran 2022)

[52] *Association of American Railroads*, "Innovative Engineering & Technology Fuel Greener Rail Operations", https://www.aar.org/issue/freight-rail-and-the-environment/. (Erişim Tarihi: 21 Haziran 2022)

[53] Uğur, Alper; (2019), "Investigation of the World Railway Sector Development Prospects and Turkey's Status", *alphanumeric journal*, (31 Aralık 2019), https://dergipark.org.tr/tr/download/article-file/916211. (Erişim Tarihi: 21 Haziran 2022)

[54] *Global Times*, (2022), "China opens 233 km of high-speed rail in Q1, makes progress on Xinjiang, Xizang links", (10 Nisan 2022), https://www.globaltimes.cn/page/202204/1258939.shtml. (Erişim Tarihi: 21 Haziran 2022)

[55] *Statista*, "Total length of the high-speed railway lines in use in selected European countries in 2020", https://www.statista.com/statistics/451818/length-of-high-speed-railway-lines-in-use-in-europe-by-country/. (Erişim Tarihi: 21 Haziran 2022)

[56] *English News*, "China-Europe freight train services surge in 2021", (4 Ocak 2022), https://english.news.cn/20220104/7c0a7e37a0fa4b7ea76a2932db3dea57/c.html. (Erişim Tarihi: 21 Haziran 2022)

[57] *Global Times*, (2022), "China-Europe freight train trips top 50,000, yearly growth of 55% from 2016 to 2021", (29 Ocak 2022), https://www.globaltimes.cn/page/202201/1250227.shtml. (Erişim Tarihi: 21 Haziran 2022)

[58] Dasgupta, Saibal; (2022), "War in Ukraine Challenging China's Train Routes to Europe", *VOA*, (15 Nisan 2022), https://www.voanews.com/a/war-in-ukraine-challenging-china-s-train-routes-to-europe/6530632.html. (Erişim Tarihi: 21 Haziran 2022)

[59] *KargoHaber*, (2020), "War in Ukraine Challenging China's Train Routes to Europe", (9 Temmuz 2020), https://www.kargohaber.com/yuk-treni-cinden-turkiyeye-12-gunde-ulasti-5752h.htm. (Erişim Tarihi: 21 Haziran 2022)

[60] Pektaş, İlhami; Kahraman, Yalgın; (2021), "Raylı Sistemler Sektör Raporu", *ARUS*, https://www.anadoluraylisistemler.org/content/upload/document-files/rayli-sistemler-sektor-ra-20211224173243.pdf. (Erişim Tarihi: 21 Haziran 2022)

[61] *TCDD İŞLETMESİ GENEL MÜDÜRLÜĞÜ*, "Demiryolları Sektör Raporu (TCDD)", https://www.utikad.org.tr/images/BilgiBankasi/

tcdddemiryolusektorraporu-262.pdf. (Erişim Tarihi: 21 Haziran 2022)

[62] *Ray Haber*, "Türkiye'deki Tren Garları ve İstasyonları Listesi", https://rayhaber.com/2020/08/turkiyedeki-tren-garlari-ve-istasyonlari-listesi/. (Erişim Tarihi: 21 Haziran 2022)

[63] Turasaş, https://www.turasas.gov.tr/. (Erişim Tarihi: 21 Haziran 2022)

[64] T.C. Ulaştırma ve Altyapı Bakanlığı, "Demiryolu", https://www.uab.gov.tr/uploads/pages/demiryolu/demiryolu.pdf. (Erişim Tarihi: 21 Haziran 2022)

[65] *International Maritime Organization*, "Introduction to IMO", https://www.imo.org/en/About/Pages/Default.aspx. (Erişim Tarihi: 21 Haziran 2022)

[66] *T.C. Başbakanlık Devlet Planlama Teşkilatı*, (2007), "Denizyolu Ulaşımı Özel İhtisas Komisyonu Raporu", https://www.sbb.gov.tr/wp-content/uploads/2018/11/09_DenizyoluUla%C5%9F%C4%B1m%C4%B1.pdf. (Erişim Tarihi: 21 Haziran 2022)

[67] *UNCTAD*, (2020), "REVIEW OF MARITIME TRANSPORT 2020", https://unctad.org/system/files/official-document/rmt2020fas_en.pdf. (Erişim Tarihi: 21 Haziran 2022)

[68] *T.C. Kalkınma Bakanlığı*, (2018), "On Birinci Kalkınma Planı 2019-2023", https://www.sbb.gov.tr/wp-content/uploads/2020/04/UlastirmaOzelIhtisasKomisyonuRaporu.pdf. (Erişim Tarihi: 21 Haziran 2022)

[69] *T.C. Ulaştırma ve Altyapı Bakanlığı*, "Türkiye Ulaştırma Politika Belgesi", https://www.uab.gov.tr/uploads/pages/stratejik-yonetim/turkiye-ulastirma-politikasi-141220.pdf. (Erişim Tarihi: 21 Haziran 2022)

[70] *T.C. Ulaştırma ve Altyapı Bakanlığı*, "2053 Ulaştırma ve Lojistik Ana Planı", https://www.uab.gov.tr/uploads/pages/bakanlik-yayinlari/2053-ulastirma-ve-lojistik-ana-plani-rev.pdf. (Erişim Tarihi: 21 Haziran 2022)

[71] *Mevzuat.org*, (1988), "SABOTAJLARA KARŞI KORUMA YÖNETMELİĞİ", (28 Aralık 1988), https://www.mevzuat.gov.tr/MevzuatMetin/3.5.8813543.pdf. (Erişim Tarihi: 21 Haziran 2022)

[72] *Resmi Gazete*, (2018), "KARAYOLU ALTYAPISI GÜVENLİK YÖNETİMİ HAKKINDA YÖNETMELİK", (21 Ekim 2018), https://www.resmigazete.gov.tr/eskiler/2018/10/20181021-1.htm. (Erişim Tarihi: 21 Haziran 2022)

[73] *Ray Haber*, (2021), "Karayollarında Dijitalleşme Dönemi Başlıyor", (5 Nisan 2021), https://rayhaber.com/2021/04/karayollarinda-dijitallesme-donemi-basliyor/. (Erişim Tarihi: 21 Haziran 2022)

[74] *NTV*, (2020), "Akıllı otoyolun tüm özellikleri", (3 Eylül 2020), https://www.ntv.com.tr/galeri/ekonomi/akilli-otoyolun-tum-ozellikleri,9gOtF8UhlUCcb-RFXvnBqg. (Erişim Tarihi: 21 Haziran 2022)

[75] *International Maritime Organization*, "SOLAS XI-2 and the ISPS Code", https://www.imo.org/en/OurWork/Security/Pages/SOLAS-XI-2%20ISPS%20Code.aspx. (Erişim Tarihi: 21 Haziran 2022)

[76] *Congress.gov*, "SECURITY AND ACCOUNTABILITY FOR EVERY PORT ACT OF 2006", https://www.congress.gov/109/plaws/publ347/PLAW-109publ347.pdf. (Erişim Tarihi: 21 Haziran 2022)

[77] *T.C. Cumhurbaşkanlığı Mevzuat Bilgi Sistemi*, (2004), "ÖZEL GÜVENLİK HİZMETLERİNE DAİR KANUNUN UYGULANMASINA İLİŞKİN YÖNETMELİK", (7 Ekim 2004), https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=7190&MevzuatTur=7&MevzuatTertip=5. (Erişim Tarihi: 21 Haziran 2022)

[78] *Köroğlu*, (2022), "AKILLI DEMİRYOLU ULAŞIM SİSTEMLERİ'Nİ KURUYORUZ", (23 Mart 2022), https://www.koroglugazetesi.com/haber/akilli-demiryolu-ulasim-sistemlerini-kuruyoruz.html. (Erişim Tarihi: 21 Haziran 2022)

[79] Sarıkavak, Yasin; "Demiryolu endüstrisinde akıllı ulaştırma sistemleri ve Türkiye'deki uygulama örnekleri", *Dergipark*, https://dergipark.org.tr/tr/download/article-file/549964. (Erişim Tarihi: 21 Haziran 2022)

[80] *Deutsche Welle*, (2004), "Madrid'de terör dehşeti", (11 Mart 2004), https://www.dw.com/tr/madridde-ter%C3%B6r-deh%C5%9Feti/a-2526915. (Erişim Tarihi: 21 Haziran 2022)

[81] *Cumhuriyet*, (2010), "Moskova kan gölü: 37 ölü", (29 Mart 2010), https://www.cumhuriyet.com.tr/haber/moskova-kan-golu-37-olu-131156. (Erişim Tarihi: 21 Haziran 2022)

[82] *Resmi Gazete*, (2015), "DEMİRYOLU EMNİYET YÖNETMELİĞİ", (19 Kasım 2015), https://www.resmigazete.gov.tr/eskiler/2015/11//20151119-31.htm#:~:text=MADDE%2011%20%E2%80%93%20(1)%20Demiryolu,altyap%C4%B1%20i%C5%9Fletmecileri%2C%20i%C5%9Fletmecilik%20faaliyeti%20yapamazlar. (Erişim Tarihi: 21 Haziran 2022)

[83] Kaya, Murat; (2021), "Atatürk Havalimanı'ndaki terör saldırısının üzerinden 5 yıl geçti, sanıkların dosyası Yargıtay'da", *Anadolu Ajansı*, (27 Haziran 2021), https://www.aa.com.tr/tr/gundem/ataturk-havalimanindaki-teror-saldirisinin-uzerinden-5-yil-gecti-saniklarin-dosyasi-yargitayda/2286718. (Erişim Tarihi: 21 Haziran 2022)

[84] *Statista*, "Number of aircraft hijackings in the aviation industry worldwide from 1990 to 2021", https://www.statista.com/statistics/1240246/aircraft-hijackings-worldwide/. (Erişim Tarihi: 21 Haziran 2022)

[85] *PA Consulting*, "AIRPORT CYBER SECURITY Overcome the silent threat", https://www.paconsulting.com/insights/2018/cyber-security-in-airports/. (Erişim Tarihi: 21 Haziran 2022)

[86] *Air News Times*, (2020), "Havacılık Sektöründe Siber Güvenlik", (26 Kasım 2020), https://www.airnewstimes.com/havacilik-sektorunde-siber-guvenlik.html. (Erişim Tarihi: 21 Haziran 2022)

[87] *Habertürk*, (2012), "THY'ye siber saldırı", (25 Ağustos 2012), https://www.haberturk.com/ekonomi/teknoloji/haber/770944-thy-ye-siber-saldiri. (Erişim Tarihi: 21 Haziran 2022)

[88] *TEKNOBH*, "Pegasus Hacklendi! Durum Çok Vahim!", https://www.teknobh.com/pegasus-hacklendi-durum-cok-vahim/. (Erişim Tarihi: 21 Haziran 2022)

[89] *STM ThinkTech*, (2021), "Havaalanlarının Güvenliği Artıyor", (23 Kasım 2021), https://thinktech.stm.com.tr/tr/havaalanlarinin-guvenligi-artiyor. (Erişim Tarihi: 21 Haziran 2022)

[90] Kurnaz, Salim; Karatepe, Selma; "KRİTİK ALT YAPILARIN GÜVENLİĞİ KAPSAMINDA TÜRKİYE'DEKİ HAVA ALANLARININ SİBER GÜVENLİĞİ", *ASSAM*, https://dergipark.org.tr/en/download/article-file/811393. (Erişim Tarihi: 21 Haziran 2022)

[91] *Mevzuat.gov*, (2008), "ELEKTRONİK HABERLEŞME KANUNU", (5 Kasım 2008), https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5809.pdf. (Erişim Tarihi: 21 Haziran 2022)

[92] *Grand View Research*, ("Telecom Services Market Size, Share & Trends Analysis Report By Service Type (Mobile Data Services, Machine-To-Machine Services), By Transmission (Wireline, Wireless), By End-use, By Region, And Segment Forecasts, 2021 – 2028", https://www.grandviewresearch.com/industry-analysis/global-telecom-services-market. (Erişim Tarihi: 21 Haziran 2022)

[93] O'Dea, S.; (2021), "Telecommunication services - Statistics & Facts", *Statista*, (3 Kasım 2021), https://www.statista.com/topics/2665/telecommunication-services/#dossierContents__outerWrapper. (Erişim Tarihi: 21 Haziran 2022)

[94] R. Sharafat, Ahmad; H. Lehr William; (2017), "ICT-centric economic growth, innovation and job creation", *International Telecommunication Union*, https://www.itu.int/dms_pub/itu-d/opb/gen/D-GEN-ICT_SDGS.01-2017-PDF-E.pdf. (Erişim Tarihi: 21 Haziran 2022)

[95] *International Telecommunication Union*, "Key ICT indicators for developed and developing countries, the world and special regions", https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ITU_regional_global_Key_ICT_indicator_aggregates_rev1_Jan_2022.xlsx. (Erişim Tarihi: 21 Haziran 2022)

[96] *GSMA*, "Make a difference", https://www.gsma.com/membership/. (Erişim Tarihi: 21 Haziran 2022)

[97] Chi, Zhang; (2019), "Why China's mobile coverage is superior to that of the US", *Global Times*, (6 Aralık 2019), https://www.globaltimes.cn/content/1172513.shtml#:~:text=According%20to%20reports%2C%20there%20are,about%20300%2C000%20in%20the%20US. (Erişim Tarihi: 21 Haziran 2022)

[98] Labrador, Virgil; "satellite communication", *Britannica*, https://www.britannica.com/technology/satellite-communication#:~:text=Approximately%202%2C000%20artificial%20satellites%20orbiting,one%20or%20many%20locations%20worldwide. (Erişim Tarihi: 21 Haziran 2022)

[99] *STM ThinkTech*, (2019), "6G İnterneti Düşünmek İçin Erken Değil", (24 Nisan 2019), https://thinktech.stm.com.tr/tr/6g-interneti-dusunmek-icin-erken-degil. (Erişim Tarihi: 21 Haziran 2022)

[100] Pedro Tomás, Juan; (2022), "China ends 2021 with 1.43 million 5G base stations", *RCR Wireless News*, (28 Ocak 2022), https://www.rcrwireless.com/20220128/5g/china-ends-2021-million-5g-base-stations. (Erişim Tarihi: 21 Haziran 2022)

[101] *Global mobile Suppliers Association*, (2022), "5G - 4G-5G Subscribers March 2022 – Quarterly update", (Mart 2022), https://gsacom.com/paper/4g-5g-subscribers-march-2022-quarterly-update/. (Erişim Tarihi: 21 Haziran 2022)

[102] *International Telecommunication Union*, (2021), "2.9 billion people still offline", (30 Kasım 2021), https://www.itu.int/en/mediacentre/Pages/PR-2021-11-29-FactsFigures.aspx. (Erişim Tarihi: 21 Haziran 2022)

[103] *STM ThinkTech*, (2019), "Küçük Uydular ve Başarı Potansiyelleri", (22 Şubat 2019), https://thinktech.stm.com.tr/tr/kucuk-uydular-ve-basari-potansiyelleri. (Erişim Tarihi: 21 Haziran 2022)

[104] Terry, QuHarrison; (2019), "By 2069, Every Person On Earth Will Have Internet Access", *Medium*, (15 Ocak 2019), https://medium.com/@quharrison/by-2069-every-person-on-earth-will-have-internet-access-9a9636beacdd#:~:text=Regardless%20of%20the%20logistical%20nightmare,population)%20by%20the%20year%202050. (Erişim Tarihi: 21 Haziran 2022)

[105] Glenday, John; (2022), "Global streaming subscriptions surge 100,000 to 1.3 billion in 2021" *The Drum*, (15 Mart 2022), https://www.thedrum.com/news/2022/03/15/global-streaming-subscriptions-surge-100000-13-billion-2021. (Erişim Tarihi: 21 Haziran 2022)

[106] Hekim Yılmaz, Derya; Kırışkan, Işın; (2020), "Türkiye'de Telekomünikasyon Altyapısı ve Ekonomik Büyüme", *Dergipark*, (31 Ocak 2020), https://dergipark.org.tr/tr/pub/bilig/issue/45419/683907. (Erişim Tarihi: 21 Haziran 2022)

[107] *Bilgi Teknolojileri ve İletişim Kurumu*, (2021), "Türkiye Elektronik Haberleşme Sektörü Üç Aylık Pazar Verileri Raporu", https://www.btk.gov.tr/uploads/pages/pazar-verileri/2021-4-pazar-verileri-raporu.pdf. (Erişim Tarihi: 21 Haziran 2022)

[108] Sarp Nebil, Füsun; (2022), "Bir Ar-Ge hikâyesi: Yerli ve milli 5G, ne kadar yerli/milli, ne kadar Ar-Ge?", *T24*, (11 Şubat 2022), https://t24.com.tr/yazarlar/fusun-sarp-nebil/bir-ar-ge-hikayesi-yerli-ve-milli-5-g-ne-kadar-yerli-milli-ne-kadar-ar-ge,34164#:~:text=Ama%20nedense%20T%C3%BCrkiye%20Cumhuriyeti%20ya,baz%20istasyonu%20say%C4%B1s%C4%B1%20197%20bin. (Erişim Tarihi: 21 Haziran 2022)

[109] *National Center for Biotechnology Information*, (2021), "Trends and Risks of Network Technologies", (10 Eylül 2021), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8431264/. (Erişim Tarihi: 21 Haziran 2022)

[110] Ayas, Meryem; (2017), "Dijital Devrimin İkinci Dalgası - Nesnelerin İnterneti", *STM ThinkTech*, (1 Aralık 2017), https://thinktech.stm.com.tr/tr/dijital-devrimin-ikinci-dalgasi-nesnelerin-interneti. (Erişim Tarihi: 21 Haziran 2022)

[111] *STM ThinkTech*, (2020), "Covid-19 Sonrası Çalışma Hayatının Geleceği", (29 Haziran 2020), https://thinktech.stm.com.tr/tr/covid-19-sonrasi-calisma-hayatinin-gelecegi. (Erişim Tarihi: 21 Haziran 2022)

[112] *We Are Social*, (2021), "SOCIAL MEDIA USERS PASS THE 4.5 BILLION MARK", (21 Ekim 2021), https://wearesocial.com/jp/blog/2021/10/social-media-users-pass-the-4-5-billion-mark/#:~:text=Social%20media%20users%20increased%20by,new%20users%20every%20single%20day. (Erişim Tarihi: 21 Haziran 2022)

[113] *STM ThinkTech*, (2022), "Metaverse: Fırsatlar ve Tehditler", (14 Şubat 2022), https://thinktech.stm.com.tr/tr/metaverse-firsatlar-ve-tehditler. (Erişim Tarihi: 21 Haziran 2022)

[114] *Anadolu Ajansı*, (2015), "Diyarbakır'da terör saldırısı", (4 Ekim 2015), https://www.aa.com.tr/tr/turkiye/diyarbakirda-teror-saldirisi/428628. (Erişim Tarihi: 21 Haziran 2022)

[115] *Vatan*, (2007), "Telekom çalışanlarına saldırı", (12 Kasım 2007), https://www.gazetevatan.com/gundem/telekom-calisanlarina-saldiri-146590. (Erişim Tarihi: 21 Haziran 2022)

[116] Çelik, Emine; (2022), "Rusya-Ukrayna savaşının 'siber' boyutu", *Anadolu Ajansı*, (3 Mart 2022), https://www.aa.com.tr/tr/analiz/rusya-ukrayna-savasinin-siber-boyutu/2522079. (Erişim Tarihi: 21 Haziran 2022)

[117] Pongratz, Stefan; (2022), "Key Takeaways – 2021 Total Telecom Equipment Market", *Dell'Oro Group*, (14 Mart 2022), https://www.delloro.com/key-takeaways-2021-total-telecom-equipment-market/#:~:text=Preliminary%20estimates%20suggest%20the%20overall,in%20RAN%20and%20Broadband%20Access. (Erişim Tarihi: 21 Haziran 2022)

[118] *Counterpoint*, (2022), "Global Smartphone Market Share: By Quarter", (29 Nisan 2022), https://www.counterpointresearch.com/global-smartphone-share/. (Erişim Tarihi: 21 Haziran 2022)

[119] Satyanarayana, Anil; (2021), "TSMC has the largest market share in the global semiconductor manufacturing industry: Counterpoints Research", *NotebookCheck*, (2 Mart 2021), https://www.notebookcheck.net/TSMC-has-the-largest-market-share-in-the-global-semiconductor-manufacturing-industry-Counterpoints-Research.518137.0.html. (Erişim Tarihi: 21 Haziran 2022)

[120] Leonard, Jenny; King, Ian; (2022), "Biden Team Says Global Chip Shortage to Stretch Through 2022", *Bloomberg*, (25 Ocak 2022), https://www.bloomberg.com/news/articles/2022-01-25/biden-team-says-global-chip-shortage-to-stretch-through-2022. (Erişim Tarihi: 21 Haziran 2022)

[121] Linder, Courtney; (2021), "The NSA Wants Big Tech to Build Software 'Back Doors.' Should We Be Worried?" *Popular Mechanics*, (21 Haziran 2021), https://www.popularmechanics.com/technology/security/a34533340/nsa-tech-back-doors-software/. (Erişim Tarihi: 21 Haziran 2022)

[122] Kabaş, Denizcan; "RİSK İLETİŞİMİ PERSPEKTİFİNDEN NESNELERİN İNTERNETİ ÜZERİNE BİR İNCELEME: YENİ TEKNOLOJİLERİN YENİ RİSKLERİ", *Dergipark*, https://dergipark.org.tr/tr/download/article-file/768125. (Erişim Tarihi: 21 Haziran 2022)

[123] Collela, Paolo; "Ushering In A Better Connected Future", *Ericsson*, https://bit.ly/3nboOpD. (Erişim Tarihi: 21 Haziran 2022)

[124] *EY*, (2020), "OT ve IoT sistemleriniz ne ölçüde güvenli?", (Kasım 2020), https://bilisimzirvesi.com.tr/documents/ot-ve-iot-sistemleriniz-ne-olcude-guvenli-pdf.pdf. (Erişim Tarihi: 21 Haziran 2022)

[125] *TRT Haber*, (2022), "Dünyadaki 5G baz istasyonlarının yüzde 60'ından fazlası Çin'de", (13 Şubat 2022), https://www.trthaber.com/haber/guncel/dunyadaki-5g-baz-istasyonlarinin-yuzde-60indan-fazlasi-cinde-654439.html. (Erişim Tarihi: 21 Haziran 2022)

[126] *STM ThinkTech*, (2019), "5G YARIŞI", (Nisan 2019), https://thinktech.stm.com.tr/uploads/docs/1608998414_stm-5g-yarisi.pdf. (Erişim Tarihi: 21 Haziran 2022)

[127] Farrell, Henry; (2018), "Hackers used a fish tank to break into a Vegas casino. We're all in trouble.", Washington Post, (4 Eylül 2018), https://www.washingtonpost.com/news/monkey-cage/

wp/2018/09/04/hackers-used-a-fishtank-to-break-into-a-vegas-casino-were-all-in-trouble/. (Erişim Tarihi: 21 Haziran 2022)

[128] *ICT Media*, (2021), "Siber güvenlik ulusal güvenliğin ayrılmaz bir parçasıdır", (7 Haziran 2021), https://www.ictmedia.com.tr/News/Index/11971/-siber-guvenlik-ulusal-guvenligin-ayrilmaz-bir-parcasidir-. (Erişim Tarihi: 21 Haziran 2022)

[129] *International Telecommunication Union*, "X.805 : Security architecture for systems providing end-to-end communications", https://www.itu.int/rec/T-REC-X.805. (Erişim Tarihi: 21 Haziran 2022)

[130] *Mevzuat.gov*, "ELEKTRONİK HABERLEŞME SEKTÖRÜNDE ŞEBEKE VE BİLGİ GÜVENLİĞİ YÖNETMELİĞİ", https://www.mevzuat.gov.tr/File/GeneratePdf?mevzuatNo=19880&mevzuatTur=KurumVeKurulusYonetmeligi&mevzuatTertip=5. (Erişim Tarihi: 21 Haziran 2022)

[131] *T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi*, (2020), "Bilgi ve İletişim Güvenliği Rehberi", (Temmuz 2020), https://cbddo.gov.tr/SharedFolderServer/Genel/File/bg_rehber.pdf. (Erişim Tarihi: 21 Haziran 2022)

[132] *AFAD*, "Kesintisiz Ve Güvenli Haberleşme Sistemi", https://www.afad.gov.tr/kesintisiz-ve-guvenli-haberlesme-sistemi. (Erişim Tarihi: 21 Haziran 2022)

[133] *T.C. Ulaştırma ve Altyapı Bakanlığı*, (2021), "BİLİŞİM VE İLETİŞİM SEKTÖRLERİNDE YERLİ VE MİLLİ ATILIM TÜM HIZIYLA SÜRÜYOR", (23 Şubat 2021), https://www.uab.gov.tr/haberler/bilisim-ve-iletisim-sektorlerinde-yerli-ve-milli-atilim-tum-hiziyla-suruyor. (Erişim Tarihi: 21 Haziran 2022)

[134] *Bilgi Teknolojileri ve İletişim Kurumu*, (2021), "Yerli ve Milli 5G Altyapısı üzerinden İlk Sesli Görüşme Yapıldı", (23 Haziran 2021), https://www.btk.gov.tr/haberler/yerli-ve-milli-5g-altyapisi-uzerinden-ilk-sesli-gorusme-yapildi. (Erişim Tarihi: 21 Haziran 2022)

[135] Alexandra Sava, Justina; (2022), "Global information technology industry forecast 2019-2022, by region", *Statista*, (24 Şubat 2022), https://www.statista.com/statistics/507365/worldwide-information-technology-industry-by-region/#:~:text=The%20global%20information%20technology%20(IT,approximately%205.3%20trillion%20U.S.%20dollars. (Erişim Tarihi: 21 Haziran 2022)

[136] *Reuters*, (2021), "World economy to top $100 trillion in 2022 for first time: report", (26 Aralık 2020), https://www.reuters.com/business/world-economy-top-100-trillion-2022-first-time-report-2021-12-26/. (Erişim Tarihi: 21 Haziran 2022)

[137] *TÜBİSAD*, (2021), "2020 Information and Communication Technologies Industry Market Data and Trends", (Temmuz 2021), https://www.tubisad.org.tr/en/images/pdf/tubisad_ict_2020_report_en.pdf. (Erişim Tarihi: 21 Haziran 2022)

[138] Rimol, Meghan; (2022), "Gartner Forecasts Worldwide IT Spending to Reach $4.4 Trillion in 2022", *Gartner*, (6 Nisan 2022), https://www.gartner.com/en/newsroom/press-releases/2022-04-06-gartner-forecasts-worldwide-it-spending-to-reach-4-point-four-trillion-in-2022. (Erişim Tarihi: 21 Haziran 2022)

[139] Allen, Mike; (2018), "And The Title of The Largest Data Center in the World and Largest Data Center in US Goes To...", *Data Centers*, (15 Haziran 2018), https://www.datacenters.com/news/and-the-title-of-the-largest-data-center-in-the-world-and-largest-data-center-in#:~:text=Data%20Centers%20are%20of%20Different%20Sizes&text=While%20most%20are%20small%2C%20the,as%20a%20med%2Dsized%20town. (Erişim Tarihi: 21 Haziran 2022)

[140] Huld, Arendse; (2022), "'Eastern Data, Western Computing' – China's Big Plan to Boost Data Center Computing Power Across Regions", *China Briefing*", (30 Mart 2022), https://www.china-briefing.com/news/china-data-centers-new-cross-regional-plan-to-boost-computing-power-across-regions/#:~:text=Infrastructure%20requirements&text=Specifically%2C%20the%20government%20plans%20to,center%20clusters%20within%20these%20hubs. (Erişim Tarihi: 21 Haziran 2022)

[141] *Data Center Map*, "Turkey Data Centers", https://www.datacentermap.com/turkey/#:~:text=Currently%20there%20are%2072%20colocation,areas%20in%20Turkey%20(T%C3%BCrkiye). (Erişim Tarihi: 21 Haziran 2022)

[142] *Brussels Times*, (2022), "Global computer sales boom in 2021", (14 Ocak 2022), https://www.brusselstimes.com/201510/global-computer-sales-boom-in-2021. (Erişim Tarihi: 21 Haziran 2022)

[143] *Gartner*, (2022), "Gartner Says Global Smartphone Sales Grew 6% in 2021", (2 Mart 2022), https://www.gartner.com/en/newsroom/press-releases/2022-03-01-4q21-smartphone-market-share. (Erişim Tarihi: 21 Haziran 2022)

[144] *TÜBİSAD*, ("Türkiye'nin Dijital Dönüşüm Endeksi 2021", https://www.tubisad.org.tr/tr/images/pdf/tubisad-2021-dde-raporu.pdf. (Erişim Tarihi: 21 Haziran 2022)

[145] *TÜİK*, (2021), "Hanehalkı Bilişim Teknolojileri (BT) Kullanım Araştırması, 2021", (26 Ağoustos 2021), https://bit.ly/3N3iCuw. (Erişim Tarihi: 21 Haziran 2022)

[146] Aras, Uğur; (2020), "KRİTİK ALTYAPILARIN SİBER GÜVENLİĞİNDE İÇ TEHDİT ETKİSİ", *GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ*, (Haziran 2020), https://avesis.gazi.edu.tr/dosya?id=cc6f88f9-35ed-48fb-b3ae-7f4259a29b8c. (Erişim Tarihi: 21 Haziran 2022)

[147] Morgan, Steve; (2020), "Cybercrime To Cost The World $10.5 Trillion Annually By 2025", *Cyber Security Ventures*, (13 Kasım 2020), https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/. (Erişim Tarihi: 21 Haziran 2022)

[148] *Cambridge Network*, "Darktrace reports ICT sector most targeted by cyber-attackers in 2021", https://www.cambridgenetwork.co.uk/news/darktrace-reports-ict-sector-most-targeted-cyber-attackers-2021. (Erişim Tarihi: 21 Haziran 2022)

[149] Arar, Doğan; (2018), "Siber Güvenlik ve Savunma: Farkındalık ve Caydırıcılık", *Academia*, https://www.academia.edu/41682778/Siber_G%C3%BCvenlik_ve_Savunma_Fark%C4%B1ndal%C4%B1k_ve_Cayd%C4%B1r%C4%B1c%C4%B1l%C4%B1k. (Erişim Tarihi: 21 Haziran 2022)

[150] Sobers, Rob; (2021), "134 Cybersecurity Statistics and Trends for 2021", *Varonis*, (16 Mart 2021), https://www.varonis.com/blog/cybersecurity-statistics. (Erişim Tarihi: 21 Haziran 2022)

[151] Carlson, Brian; (2021), "Top cybersecurity statistics, trends, and facts", (7 Ekim 2021), *CSO*, https://www.csoonline.com/article/3634869/top-cybersecurity-statistics-trends-and-facts.html. (Erişim Tarihi: 21 Haziran 2022)

[152] *dnx.solutions*, (2022), "What is the Real Cost of a Data Breach in 2022?", (17 Şubat 2022), https://dnx.solutions/what-is-the-real-cost-of-a-data-breach-in-2022/. (Erişim Tarihi: 21 Haziran 2022)

[153] *Accenture*, (2019), "Ninth Annual Cost of Cybercrime Study", (6 Mart 2019), https://www.accenture.com/us-en/insights/security/cost-cybercrime-study. (Erişim Tarihi: 21 Haziran 2022)

[154] *Sonicwall*, (2021), "SONICWALL CYBER THREAT REPORT", https://www.sonicwall.com/medialibrary/en/white-paper/2021-cyber-threat-report.pdf. (Erişim Tarihi: 21 Haziran 2022)

[155] *Help Net Security*, (2022), "Cybercriminals launched 9.75 million DDoS attacks in 2021", (28 Mart 2022), https://www.helpnetsecurity.com/2022/03/28/ddos-attacks-2021/#:~:text=During%20the%20second%20half%20of,million%2C%20a%20NETSCOUT%20report%20reveals. (Erişim Tarihi: 21 Haziran 2022)

[156] *SoftActivity*, "32 Remarkable DDoS Statistics for 2022", https://www.softactivity.com/ideas/ddos-statistics/#:~:text=More%20than%205.4%20million%20DDoS,company%20%2420%2C000%2D%2440%2C000%20hourly. (Erişim Tarihi: 21 Haziran 2022)

[157] *SlushNext*, (2021), "Social Engineering Threats Rose 270% in 2021 – Indicating a Shift to Multi-Channel Phishing Attacks as Apps and Browsers Move to the Cloud", (15 Ekim 2021), https://www.slashnext.com/blog/social-engineering-threats-ro-

se-270-in-2021-indicating-a-shift-to-multi-channel-phishing-attacks-as-apps-and-browsers-move-to-the-cloud/. (Erişim Tarihi: 21 Haziran 2022)

[158] *Kaspersky*, (2022), "APT attacks on industrial companies in H2 2021", (28 Şubat 2022), https://ics-cert.kaspersky.com/publications/reports/2022/02/28/apt-attacks-on-industrial-companies-in-h2-2021/#:~:text=Attacks%20of%20Iranian%20state%2Dsponsored%20APT%20actors&text=According%20to%20a%20report%20published,organizations%20and%20a%20utility%20company. (Erişim Tarihi: 21 Haziran 2022)

[159] Caesar, Ed; (2021), "The Incredible Rise of North Korea's Hacking Army", *New Yorker*, (19 Nisan 2021), https://www.newyorker.com/magazine/2021/04/26/the-incredible-rise-of-north-koreas-hacking-army. (Erişim Tarihi: 21 Haziran 2022)

[160] *CTEMPLAR*, "What is a Man-in-the-Middle Attack (MitM) and how to Prevent it", https://ctemplar.com/what-is-a-man-in-the-middle-attack-mitm-and-how-to-prevent-it/. (Erişim Tarihi: 21 Haziran 2022)

[161] *Mahalli Gündem*, (2022), "Türkiye'de 1 yılda 620 binden fazla siber saldırı gerçekleştil", (12 Ocak 2022), https://www.mahalligundem.com/turkiye-de-1-yilda-620-binden-fazla-siber-saldiri-gerceklesti/54218/. (Erişim Tarihi: 21 Haziran 2022)

[162] Kıvrak, Salih; (2020), "Yerli ve millî KASIRGA, AVCI ve AZAD uygulamaları Türkiye'yi hedef alan 325 bin siber saldırıyı engelledi", *Defence Turk*, (29 Aralık 2020), https://www.defenceturk.net/yerli-ve-milli-kasirga-avci-ve-azad-uygulamalari-turkiyeyi-hedef-alan-325-bin-siber-saldiri-engelledi. (Erişim Tarihi: 21 Haziran 2022)

[163] *International Telecommunication Union*, (2022), "Global Cybersecurity Index 2020", https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E. (Erişim Tarihi: 21 Haziran 2022)

[164] *Bilgi Teknolojileri ve İletişim 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-2013-2014-5a3412cf-8f45a.pdf. (Erişim Tarihi: 21 Haziran 2022)

[165] Böcüoğlu Bodur, Ayşe; (2022), "Türkiye'ye yönelik siber saldırılar 2021'de bir önceki yıla göre azaldı ", *Anadolu Ajansı*, (27 Şubat 2022), https://www.aa.com.tr/tr/bilim-teknoloji/turkiyeye-yonelik-siber-saldirilar-2021de-bir-onceki-yila-gore-azaldi/2516713. (Erişim Tarihi: 21 Haziran 2022)

[166] T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, "Bilgi ve İletişim Güvenliği Genelgesi", https://cbddo.gov.tr/sss/bilgi-iletisim-guvenligi/. (Erişim Tarihi: 21 Haziran 2022)

[167] *Resmi Gazete*, (2019), "GENELGE 2019/12", (6 Temmuz 2019), https://www.resmigazete.gov.tr/eskiler/2019/07/20190706-10.pdf. (Erişim Tarihi: 21 Haziran 2022)

[168] *STM*, (2019), "Kritik Altyapıların Güvenliğinin Sağlanmasında Türkiye'de Bir İlk Olan Ulusal Test Yatağı Merkezi Açıldı", (20 Kasım 2019), https://www.stm.com.tr/tr/medya/basin-bultenleri/kritik-altyapilarin-guvenliginin-saglanmasinda-turkiyede-bir-ilk-olan-ulusal-test-yatagi-merkezi-acildi. (Erişim Tarihi: 21 Haziran 2022)

[169] *Sakarya Üniversitesi*, "Kritik Altyapılar Ulusal Test Yatağı Merkezi", https://center.sakarya.edu.tr/. (Erişim Tarihi: 21 Haziran 2022)

[170] *T.C. Ulaştırma ve Altyapı Bakanlığı*, "Kamu Entegre Veri Merkezi Projesi", https://hgm.uab.gov.tr/kamu-entegre-veri-merkezi-projesi. (Erişim Tarihi: 21 Haziran 2022)

[171] *T.C. Cumhurbaşkanlığı Savunma Sanayii Başkanlığı*, "SİSAMER TSK SİBER SAVUNMA MERKEZİ PROJESİ", https://www.ssb.gov.tr/Website/contentList.aspx?PageID=1083&LangID=1. (Erişim Tarihi: 21 Haziran 2022)

[172] *Türkiye Siber Güvenlik Kümelenmesi*, https://siberkume.org.tr/Index#. (Erişim Tarihi: 21 Haziran 2022)

[173] *ISTTELKOM*, "KAMUNET PROJESİ TANITILDI", https://isttelkom.istanbul/kamunet-projesi-tanitildi/. (Erişim Tarihi: 21 Haziran 2022)

[174] *Bilgi Teknolojileri ve İletişim Kurumu*, "2019-2023 STRATEJİK PLANI", https://www.btk.gov.tr/uploads/pages/yayinlar-stratejik-planlar/btk-2019-2023-stratejik-plani.pdf. (Erişim Tarihi: 21 Haziran 2022)

[175] TÜBİSAD, (2021), "Bilgi ve İletişim Teknolojileri Sektörü 2020 Pazar Verileri", (Temmuz 2021), https://www.tubisad.org.tr/tr/images/pdf/tubisad_bit_2020_raporu_tr.pdf. (Erişim Tarihi: 21 Haziran 2022)

[176] Özkan, Sedef; (2022), "Bakan Karaismailoğlu elektronik haberleşme verilerini açıkladı", *BT Haber*, (14 Nisan 2022), https://www.bthaber.com/bakan-karaismailoglu-elektronik-haberlesme-verilerini-acikladi/#:~:text=Bu%20aboneler%205G%20ve%20%C3%B6tesi,bazda%20y%C3%BCzde%2017%20b%C3%BCy%C3%BCme%20g%C3%B6sterdi. (Erişim Tarihi: 21 Haziran 2022)

[177] *STM ThinkTech*, (2021), "Bütünleşik Güvenlik Bağlamında Siber", (3 Kasım 2021), https://thinktech.stm.com.tr/tr/butunlesik-guvenlik-baglaminda-siber. (Erişim Tarihi: 21 Haziran 2022)

[178] *United Nations*, (2020), "Digital Divide 'a Matter of Life and Death' amid COVID-19 Crisis, Secretary-General Warns Virtual Meeting, Stressing Universal Connectivity Key for Health, Development", (11 Haziran 2020), https://www.un.org/press/en/2020/sgsm20118.doc.htm. (Erişim Tarihi: 21 Haziran 2022)

[179] Opp, Robert; (2021), "The evolving digital divide", *UNDP*, (14 Temmuz 2021), https://www.undp.org/blog/evolving-digital-divide?utm_source=EN&utm_medium=GSR&utm_content=US_UNDP_PaidSearch_Brand_English&utm_campaign=CENTRAL&c_src=CENTRAL&c_src2=GSR. (Erişim Tarihi: 21 Haziran 2022)

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