5G ALTYAPISI ÖZELİNDE POTANSİYEL TEKNOLOJİK TEHDİT VEKTÖRLERİ

TERÖRİZM ARAŞTIRMALARI MERKEZİ MÜDÜRLÜĞÜ
TEMATİK ANALİZ

5G ALTYAPISI ÖZELİNDE POTANSİYEL TEKNOLOJİK TEHDİT VEKTÖRLERİ RAPORU

TERÖRİZM ARAŞTIRMALARI MERKEZİ MÜDÜRLÜĞÜ

Hazırlayan
Dr. Alper BİLGİÇ

Kapak Tasarım
De.Me. Havva ARCA

Dizgi
De.Me. Serkan SIR

Baskı Ön Hazırlık
De.Me. İbrahim Halil BULDUK

JANDARMA VE SAHİL GÜVENLİK AKADEMİSİ YAYINLARI

Her hakkı saklıdır.

JSGA Yayın No : 0121
Terörizm Araştırmaları Merkezi Müdürlüğü
Yayın No : 0005
JSGA Eser No : 044
Eser Seri No : 01

ISBN : 978-625-445-056-3

1. Baskı 200 adet basılmıştır.
JSGA Basımevi Md.lüğü
Ankara, 2022

Bu yayının içeriği açık kaynak metinlerinden istifade ve tercüme edilerek derlenmiştir.

Bu kitabın basım, yayım ve satış hakları Jandarma ve Sahil Güvenlik Akademisine aittir ve bütün hakları saklıdır.

Tanıtım amacıyla, kaynak göstermek şartıyla yapılacak kısa alıntılar dışında Jandarma ve Sahil Güvenlik Akademisi'nden izin alınmadan kitabın bir kısmı ya da tümü; mekanik, elektronik, metin, görsel malzeme, fotokopi, manyetik kayıt veya başka şekillerde çoğaltılamaz, basılamaz ve dağıtılamaz.

Jandarma ve Sahil Güvenlik Akademisi, bu yayında atıfta bulunulan harici veya üçüncü taraf internet web sitelerinin URL'lerinin kalıcılığı veya doğruluğu konusunda hiçbir sorumluluğa sahip değildir ve bu tür web sitelerindeki herhangi bir içeriğin doğru veya uygun olduğunu veya öyle kalacağını garanti etmez.

Bu kitapta yer alan görüş ve düşünceler ile içerikteki bilim, hukuk ve dil sorumluluğu tamamen kitabın yazar/yazarlarına aittir. Bu konuda Jandarma ve Sahil Güvenlik Akademisi'nin herhangi bir sorumluluğu bulunmamaktadır.

JANDARMA VE SAHİL GÜVENLİK AKADEMİSİ
İncek Şehit Savcı Mehmet Selim Kiraz Bulvarı 06805 Beytepe, Çankaya-Ankara/Türkiye
http://www.jsga.edu.tr/
Tel : +90 (312) 464 74 74
Belgegeçer : +90 (312) 464 46 77

İÇİNDEKİLER

GİRİŞ 1

1. 5G Sistem Mimarisinin Temel Özellikleri.....8

1.1. 4G ve 5G Arasındaki Farklar 8

1.2. 5G Temel Çalışma Koşulları 9

2. Potansiyel Fayda Sahaları.....12

2.1. Nesnelerin İnterneti (IoT): Hacim Artışı ve Entegrasyon, Otomasyon, Senkronizasyon 12

2.2. Akıllı Şehirler ve Sanayi 4.0: Altyapı Gözetimi ve Otomasyon 13

3. Potansiyel Tehdit Vektörleri.....16

3.1. 5G Politika ve Standartlarıyla İlgili Riskler ve Güvenlik Açıkları ..20

3.2. Tedarik Zinciri Riskleri ve Güvenlik Açıkları.....24

3.3. 5G Sistem Mimarisiyle İlgili Riskler 33

4. 5G Güvenlik Endişeleri 36

4.1. Merkezi Olmayan Güvenliğin Olası Olumsuz Etkileri 36

4.2. Artan Bant Genişliğinin Mevcut Güvenlik Denetimlerini Zorlaştırması.....37

4.3. Nesnelerin İnterneti (Iot) Cihazlarının Üretim Kaynaklı Güvenlik Eksiklikleri 37

4.4. Bağlantı Kurarken İlk Aşamadaki Şifreleme Eksikliği Kaynaklı Muhtemel Zafiyet.....37

5. Ağ Koruması ve Denetim 40

5.1. 5G'de Siber Güvenlik İçin Sağlanması Gereken Temel Şartlar 40

SONUÇ.....49

KAYNAKÇA.....54

GRAFİK VE ŞEKİLLER

Grafik 1: 5G Tabanlı Hizmetlerin Sunumunda Karşılaşılan Sorunlar 19
Şekil 1: Kurumsal 5G'de Uçtan Uca Güvenlik 41

JANDARMA VE SAHİL GÜVENLİK AKADEMİSİ
İÇİŞLERİ BAKANLIĞI
1904

JANDARMA VE SAHİL GÜVENLİK AKADEMİSİ
İÇİŞLERİ BAKANLIĞI
1904

GİRİŞ

İnsanların birbirleriyle konuşma şeklini kökünden değiştiren ve olmasaydı ne yapardık diye düşünmeyi bile istemediğimiz cep telefonunun icadının, 20. yüzyılın tüm teknolojik gelişmeleri arasında en büyük kültürel etkiyi yaratan olay olduğu ileri sürülebilir. İletişim sektöründe devrim niteliğinde bir buluş olan cep telefonundan 1973'de ilk tarihi aramayı yapan kişi aynı zamanda onun mucidi de olan Martin Cooper'dır.[1] Süreç içinde gelişen mobil cihazlar dünyamızı yeniden şekillendirmiş olmakla birlikte, günümüzde de etkilemeye ve değiştirmeye devam etmektedir. Bu bağlamda, finans sektöründen sağlık sektörüne insan hayatında bu denli büyük bir etki yaratan cep telefonunu kullanabilir kılan mobil kablosuz ağlar ve onların yapılandırma standartları da incelemeye değer bir konu olarak göze çarpmaktadır.

Mobil kablosuz standardının adlandırılmasında, kaçıncı kuşak olduğunu ifade etmek üzere, İngilizcede nesil anlamına gelen "Generation" kelimesinin ilk harfi olan "G" harfi kullanılmaktadır. Bu bağlamda, 5G (5th Generation) terimi, esasen beşinci nesil kablosuz hücresel ağları temsil eden bir kısaltmadır.[2] Bu teknolojinin tarihi seyrinde bugüne nasıl ulaştığımızı anlamlandırabilmek için kısaca önceki nesillerden de bahsetmek faydalı olacaktır.[3]

1 https://www.guinnessworldrecords.com/news/60at60/2015/8/1973-first-mobile-phone-call-392969, erişim tarihi: 01 Temmuz 2022

2 https://www.kaspersky.com/resource-center/threats/5g-pros-and-cons, erişim tarihi: 01 Temmuz 2022

3 https://www.brainbridge.be/en/blog/1g-5g-brief-history-evolution-mobile-standards, erişim tarihi: 01 Temmuz 2022

Nippon Telgraf ve Telefon (NTT) şirketi bugün "1G" olarak adlandırabileceğimiz ilk nesil mobil ağı 1979'da Tokyo'da piyasaya sürmüş ve 1984'te tüm Japonya'yı kapsayacak şekilde kullanıma sunmuştu. Amerika Birleşik Devletleri (ABD), 1983'te ilk 1G işletimini onaylamasının ardından, Motorola'nın DynaTAC'ı (Dynamic Adaptive Total Area Coverage/Dinamik Uyarlanabilir Toplam Alan Kapsamı) ülkede yaygın olarak kullanılan ilk mobil telefonlardan biri olmuş, sonrasında başka ülkelerde kendi ağlarını kullanıma sunmuştur. Ancak, kapsama alanı zayıf ve ses kalitesi düşük olan analog 1G teknolojisinde çeşitli operatörler arasında dolaşım (roaming) desteği bulunmamakla birlikte, farklı sistemlerin farklı frekans aralıklarında çalışması nedeniyle sistemler arasında uyumluluk da yoktu. Söz konusu ilk nesil teknolojide aramalar şifreli olmadığından radyo tarayıcısı olan herkes yapılan aramaları dinleyebilmekteydi.[4] İkinci nesil mobil ağ olan 2G, Finlandiya'da GSM (Global System for Mobile Communications/Mobil İletişim İçin Küresel Sistem) standardına göre 1991'de piyasaya sürülmüştür. 1G'nin aksine bu dijital teknoloji sesli aramalarda daha net konuşma imkânı sağlarken aramaların şifrelenebilmesine de olanak sağlıyordu. Ayrıca, yine de nispeten yavaş hızlara rağmen işin devrim niteliğindeki yönü, bu teknolojide kullanıcıların metin mesajları (SMS), resimli mesajlar ve multimedya mesajları (MMS) gönderebilmeleriydi. Bu bağlamda çığır açan söz konusu teknolojinin sunduğu dijital gelecek kültürel bir etki de yaratmış oldu.[5] 2001 yılında NTT DoCoMo şirketi tarafından başlatılan üçüncü nesil mobil ağ olan 3G, satıcılar tarafından kullanılan ağ protokolünü standartlaştırmayı amaçladı. Böylelikle, 3G ile web bağlantısını yönlendiren "veri paketleri" standartlaştırıldığından, kullanıcıların dünyanın herhangi bir yerinden verilere erişebilecekleri uluslararası dolaşım hizmetlerini ilk kez gerçek bir olasılık haline getirmiştir. Sonrasında, 3G'nin 2G'ye kıyasla artan veri hızı ve aktarım yetenekleri IP (İnternet Protokolü) üzerinden ses ve görüntü aktarımı ve video konferans gibi yeni hizmetlerin yükselişine yol açmıştır.[6] Dördüncü nesil mobil ağ olan 4G, ilk olarak 2009'da Stockholm, İsveç ve Oslo, Norveç'te LTE (Long Term Evolution/Uzun Vadeli Evrim) 4G standardı olarak kurulmasından sonra tüm dünyaya tanıtılmıştır. 4G, oyun hizmetlerini ve yüksek kaliteli (High-Definition/HD) videoların yayımını kolaylaştıran hızlı mobil web erişimi sunmaktadır. Mobil ağ nesillerinde 2G'den 3G'ye geçiş, telefonlardaki SIM (Subscriber Identity Module) kartları değiştirmek kadar basitken 4G'ye geçişte mobil cihazların bunu desteklemek için özel olarak tasarlanması gerekmekteydi.[7]

4 https://www.brainbridge.be/en/blog/1g-5g-brief-history-evolution-mobile-standards, erişim tarihi: 01 Temmuz 2022

5 https://www.brainbridge.be/en/blog/1g-5g-brief-history-evolution-mobile-standards, erişim tarihi: 01 Temmuz 2022

6 https://www.brainbridge.be/en/blog/1g-5g-brief-history-evolution-mobile-standards, erişim tarihi: 01 Temmuz 2022

7 https://www.brainbridge.be/en/blog/1g-5g-brief-history-evolution-mobile-standards, erişim tarihi: 01 Temmuz 2022

Yaşanan teknolojik gelişimin sonucunda, özetle, ağa bağlı milyarlarca cihazın dünya çapında sorunsuz bir şekilde veri paylaşımını öngören "Nesnelerin İnterneti" (Internet of Things/IoT) terimiyle ifade edilen sistemin nitelik ve nicelik bakımından daha üst seviye veri trafiğini kaldıracak bir ağı gerektirdiği söylenebilir. 2000'lerin başında gecikme süresi bakımından gerçek zamanlı yanıtlar için çok yavaş kalacağı öngörülen 3G ve hatta 4G ağlarının böylesi bir ağı destekleyemeyeceğinden yeni nesil mobil ağları geliştirilmesi için çalışmalar başladı. 2008'de National Aeronautics and Space Administration (Ulusal Havacılık ve Uzay Dairesi/NASA), IoT ve M2M (Machine-to-Machine/Aygıtlar arası) teknolojisinin yanı sıra onu desteklemek için gereken 5G teknolojisini geliştirmek üzere Machine-to-Machine Intelligence (Aygıtlar arası Zekâ/M2Mi) Şirketinin kurulmasına öncülük etmiştir. İlk cep telefonu görüşmesinden bu yana baş döndürücü ilerlemeler kaydeden mobil endüstrisindeki bayrak yarışında 1 Aralık 2018'de 5G'yi sunan ilk ülke olarak Güney Kore ipi göğüslemiştir.[8]

Üstün bağlantı kalitesi ve hızıyla bankacılıktan sağlık hizmetlerine pek çok alanda iş modellemelerini dönüştürme vaadinde bulunan 5G; uzaktan yaşamsal belirti izleme, uzaktan ameliyatlar ve teletıp gibi hayat kurtarabilecek yenileşim imkânı sunmaktadır.[9] Ancak teknoloji her zaman iyi huylu değildir mottosuyla kavrama yaklaşılmalıdır. Bu bağlamda, 5G hakkında süregelen tartışmalar ve 5G'nin yarat-

8 https://www.brainbridge.be/en/blog/1g-5g-brief-history-evolution-mobile-standards, erişim tarihi: 01 Temmuz 2022

9 https://www.brainbridge.be/en/blog/1g-5g-brief-history-evolution-mobile-standards, erişim tarihi: 01 Temmuz 2022

masından endişe edilen komplikasyonlar olduğu da bilinmektedir. Örneğin; Amerika Birleşik Devletleri'nde (ABD) 5 Aralık 2021 olarak belirlenen 5G yüksek hızlı mobil geniş bant teknolojisinin piyasaya sürülme tarihi, Airbus ve Boeing havacılık şirketlerinin bu teknolojinin uçakların irtifa belirlemek için kullandıkları altimetre cihazlarının sinyalleriyle çakışma olasılığına yönelik endişelerini iletmesini müteakip 5 Ocak 2022 tarihine ertelenmişti. 5G sinyallerinin uçak altimetrelerinkiyle çakışabileceğine yönelik endişelerin, 2022 yılının başlarında ABD'de bazı havaalanlarında aksamalara yol açtığı görülmektedir. Sonuç olarak, ABD Federal Havacılık İdaresi'nin en son yaptığı açıklamada, hava taşıyıcılarının sinyal çakışmasıyla karşılaşmayacaklarından emin olmak için uçakları güçlendirmeye çalıştıklarını ve Verizon Communications ve AT&T telekomünikasyon şirketlerinin gönüllü olarak bazı 5G hizmetlerinin kullanımını 2023 yılının temmuz ayına kadar ertelemeyi kabul ettiğini ifade etmiştir. ABD'de kablosuz ağ hizmetleri sunan şirketler, bu tarihten sonra ağlarını kentsel alanlarda minimum kısıtlamalarla çalıştırmayı beklemektedirler.[10]

Bu endişeler bilinmekle birlikte, teknoloji odaklı genç bir nüfusa sahip olan ve 5G yolculuğuna çıkmaya hazırlanan Türkiye'nin mobil genişbant kullanımı açısından büyük bir büyüme potansiyeline sahip olduğu da görülmektedir. Opensignal şirketinin Türkiye'nin üç ulusal operatöründeki kullanıcı deneyimlerine dayalı analizine göre kilit bir konumda görülen mevcut ağların ülkede yeni nesil 5G ağlarına sorunsuz geçiş için önemli bir temel olacağı değerlendirilmektedir.[11]

10 https://www.cnbc.com/2022/06/17/verizon-att-agree-to-delay-some-5g-deployment-until-mid-2023.html, erişim tarihi: 01 Temmuz 2022

11 https://www.opensignal.com/reports/2020/06/turkey/mobile-network-experience, erişim tarihi: 01 Temmuz 2022

1.

5G Sistem Mimarisinin Temel Özellikleri

1. 5G Sistem Mimarisinin Temel Özellikleri

1.1. 4G ve 5G Arasındaki Farklar

Mobil iletişimde 5G (beşinci nesil mobil kablosuz standardı) teknolojisine geçişin birden değil kademeli olarak gerçekleşmesi beklenmekle birlikte, bu yeni teknolojiye ilişkin standartlar ise henüz tam olarak kesinleşmemiştir. Başlangıçta önceki nesil ağlara dayanması beklenen 5G ağlarının zamanla onların yerini alması öngörülmektedir. Bu nedenle, 4G'ye kıyasla 5G'nin ne gibi bir fark yaratacağını gözden geçirmek faydalı olacaktır:[12]

- 5G, mobil iletişim ağı üzerinde iletilebilen saniyedeki daha fazla bit nedeniyle veri yükleme ve indirme daha hızlıdır.
- 5G, ağa bağlı cihazlardan bağlı oldukları ağa iletişim için geçen süreyi ifade eden daha düşük gecikme süresi nedeniyle cihaz-ağ arasındaki veri iletim hızının yüksekliği bakımından taleplere daha iyi cevap verir.
- 5G, hücresel telsizler kullanılmadığında hızla düşük enerji kullanımına geçebildiği için daha az güç kullanır ve mobil cihazın şarj edilme sıklığını azaltarak pil ömrünü uzatır.

12 https://www.kaspersky.com/resource-center/threats/5g-pros-and-cons, erişim tarihi: 01 Temmuz 2022

- 5G, bant genişliğinin daha iyi kullanımı ve daha fazla bağlantı noktası sunması nedeniyle ağ üzerinde daha az stresle daha güvenli ve hızlı hizmet sunar.
- 5G, mevcut radyo dalgalarını genişlettiğinden daha fazla cihaz taşıyabilecek ve ağ üzerinde tıkanıklık sorunlarını azaltacaktır.

Hâlihazırdaki 4G ağlarıyla aynı alanı kapsayabilmesi için daha fazla vericiye ihtiyaç duyulması ve bazı bölgelerde yükseltme yaparken korumaya tabi tarihi alanlar, zorlu coğrafya gibi fiziksel zorluklarla karşılaşılması, önceki nesil teknolojinin tamamen değiştirilerek yerine 5G'nin kurulmasının ve yayılmasının önündeki zorluklardan biri olarak görülmekte, kullanıma geçişini yavaşlatmaktadır. Ancak, bu yavaşlamanın; ilk bakışta sadece olumsuzluk gibi görünse de, güvenlik konusunda dile getirilen önemli bazı endişeleri giderebilmek için servis sağlayıcılara zaman tanıdığı da söylenebilir.[13]

1.2. 5G Temel Çalışma Koşulları

Mevcut 4G ağları güçlü olsa da büyük şehirlerde yoğun trafiğin tecrübe edildiği zamanlarda sınırları zorlanan bu ağlar aşırı yüklenmekte ve ihtiyaca cevap verme-yebilmektedir. İnternete bağlı akıllı cihazların artışına koşut, hâlihazırda var olan milyarlarca cihazı desteklemek için daha hızlı ve daha yüksek kapasiteli bir sisteme olan ihtiyaç da artmaktadır. Beşinci nesil mobil ağlar; dördüncü nesilden daha yüksek kapasitelidir, diğer bir deyişle hareket halindeyken bile bağlantı sinyallerinin ve ağın kendisinin hızına ve tutarlılığına yardımcı olacak şekilde çok fazla veriyi daha kısa mesafeler üzerinden sorunsuzca aktarmak için kullanılabilir. Daha az güç kullanımına olanak sağlayan enerji verimli bir teknoloji olan 5G ağı, yeni sinyal spektrumlarının kullanılması nedeniyle, daha fazla cihazı destekleyebilmektedir. Böylelikle, mobil verilerin maliyeti azalmak, daha az güç tüketimi yapmak ve bugün mümkün olandan çok daha fazla cihazı daha hızlı bağlamak mümkün hale gelmektedir. Kendinden önceki neslin bıraktığı altyapının üstüne inşa edilebilen 3G ve 4G gibi önceki nesillerin aksine, uygulanması çok daha pahalı ve karmaşık olan 5G; 4G'den çok daha fazla sayıda baz istasyonunu ve bunların birbirine daha yakın konumlandırılmasını gerektirmektedir.[14]

13 https://www.kaspersky.com/resource-center/threats/5g-pros-and-cons, erişim tarihi: 01 Temmuz 2022

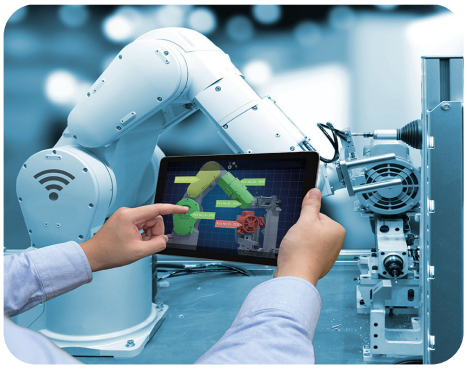
14 https://www.kaspersky.com/resource-center/threats/5g-pros-and-cons, erişim tarihi: 01 Temmuz 2022

JANDARMA VE SAHİL GÜVENLİK AKADEMİSİ
İÇİŞLERİ BAKANLIĞI
1904

2.
Potansiyel Fayda Sahaları

2. Potansiyel Fayda Sahaları

2.1. Nesnelerin İnterneti (IoT): Hacim Artışı ve Entegrasyon, Otomasyon, Senkronizasyon



Beşinci nesil mobil geniş bant ağ sisteminin en temel sonucunun kullanıcılar için daha iyi internet deneyimleri olduğu değerlendirilmektedir. Bu deneyimde akıllı cihazların kullanımı da önem kazanmaktadır. IoT, gündelik yaşantıda kullanılan genel ağa (internete) ve birbirine bağlantısı olan akıllı cihazların, diğer bir deyişle bu sistemin nesne bileşenlerinin, ağ üzerinden diğer nesnelerle veri alışverişi yapabilmesini ve birbiriyle senkronizasyon halinde olmalarını sağlayan bir teknolojidir.[15] IoT teknolojisinde web bağlantılı akıllı cihazlar çeşitli ortamlardan verileri toplama, toplanan veriler üzerinde işlem yapma ve verileri diğer ortamlara gönderme işlevini yerine getirmektedir.[16] IoT, "adreslenebilir nesnelerin kendi aralarında oluşturduğu, yaygın bir ağ ve bu ağdaki nesnelerin belirli bir protokol üzerinden iletişim hâlinde olması" şeklinde tanımlanmaktadır.[17] Bu bağlamda, yüksek kaliteli ve hızlı mobil ağların; IoT olarak adlandırılan sistemde, ağa bağlı milyarlarca cihaz arasındaki veri trafiğini küresel anlamda nitelik ve nicelik bakımından daha üst seviyeye taşıyacağı varsayılmaktadır. Küresel anlamda düşünüldüğünde bu şekilde yüksek seviyeli devasa bir IoT sistemi, hem tüketici kesimi hem de üretimi yapan sanayi sektörü için teknoloji tabanlı büyümenin önünü daha da açacaktır. Mevcut internet çerçevesi ile sınırlı olan IoT cihazları hâlihazırda kullanımda bulunmaktadır. Ancak 5G; pille çalışan cihazların, daha az ayar ile aktif ve ağa bağlı kalabilmesine olanak tanıyarak uzak, ulaşılması zor ya da elverişsiz alanlarda tamamen kablosuz kullanımına imkân yaratmaktadır. Akıllı cihazlar, hayatın akışında sensörler sayesinde daha da aktif bir rol üstlenebilecektir.[18]

15 https://www.gtech.com.tr/nesnelerin-interneti-iot-nedir/, erişim tarihi: 01 Temmuz 2022

16 https://www.gtech.com.tr/nesnelerin-interneti-iot-nedir/, erişim tarihi: 01 Temmuz 2022

17 https://www.akillisehirler.gov.tr/wp-content/uploads/EylemPlani.pdf, erişim tarihi: 01 Temmuz 2022

18 https://www.kaspersky.com/resource-center/threats/5g-pros-and-cons, erişim tarihi: 01 Temmuz 2022

2.2. Akıllı Şehirler ve Sanayi 4.0: Altyapı Gözetimi ve Otomasyon

Ortak tek bir tanımı bulunmamakla birlikte, farklı çalışmalarda çözüm aranan ihtiyaçlara göre şekillendiği değerlendirilen "Akıllı Şehirler" kavramı, "2020-2023 Ulusal Akıllı Şehirler Stratejisi ve Eylem Planı"nda "paydaşlar arası işbirliği ile hayata geçirilen, yeni teknolojileri ve yenilikçi yaklaşımları kullanan, veri ve uzmanlığa dayalı olarak gerekçelendirilen ve gelecekteki problem ve ihtiyaçları öngörerek hayata değer katan çözümler üreten daha yaşanabilir ve sürdürülebilir şehirler" olarak tanımlanmaktadır.[19] Birden fazla bileşenin ve varlığın entegrasyonundan oluşan Akıllı Şehir çözümlerinde bilgi teknolojileri alanında geliştirilen yeni teknolojiler ve yaklaşımlar önemli bir konumda bulunmaktadır. Bu bağlamda, Akıllı Şehir alanında yer alan cihazlar arasında doğrudan iletişim sağlayan teknolojiler ve bunlar arasındaki bağlantılar önem kazanmaktadır.[20]

Sanayide teknolojik ilerlemeler vasıtasıyla tecrübe edilen verimlilik artışında gelinen aşamaları tasvir için kullanılan sanayi devriminin evriminde; ilk aşama fabrikalarda buhar gücüyle çalışan makinelerin kullanılmaya başlanması 18. yüzyılın sonlarına, ikinci aşama elektrik enerjisi ile seri üretime başlanılması 20. yüzyılın başlarına, üçüncü aşama elektronik ve bilgi teknolojilerinin kullanımıyla sanayide otomasyonun yaygınlaşması 1970'lere isabet eden bir tarihsel seyir izlemiş ve nihayetinde dördüncü aşama olan ve entegre, otomatize ve optimal üretim akışı

19 https://www.akillisehirler.gov.tr/wp-content/uploads/EylemPlani.pdf, erişim tarihi: 01 Temmuz 2022

20 https://www.akillisehirler.gov.tr/wp-content/uploads/EylemPlani.pdf, erişim tarihi: 01 Temmuz 2022

sağlamayı hedefleyen "Sanayi 4.0" yaklaşımı siber-fiziksel sistemler ve dinamik veri işleme ile değer zincirlerinin uçtan uca bağlanması içinde bulunduğumuz döneme tekabül eden bir süreç olarak deneyimlendiği değerlendirilmektedir.[21] Sanayi 4.0, özetle, "imalat sanayi sistemleri ile ürünlerin tasarımı, üretimi, operasyonu ve hizmetlerinde dijitalleşmeye yönelik hızlı değişime" işaret eden bir kavramdır.[22] Ancak, mevcut durumda sınırlı yapay zekaya ve otomasyon kontrol mekanizmalarına sahip sensörlerin ve makinelerin ancak bir kısmı ağa bağlı şekilde tümleşik veri işlemeyi gerçekleştirebilmektedir.[23]

Daha verimli, daha güvenli ve daha üretken iş ve yaşamlar sunmayı amaçlayan Akıllı Şehirler ve Sanayi 4.0 kavramları temelinde düşündüğümüzde de 5G destekli IoT, şehirlerde daha iyi altyapı işlevlerinin gözetiminde ve fabrikalarda iş süreçlerini dinamik olarak değiştirerek akıllı otomasyon sağlanmasında kullanılabilecektir.[24]

21 https://tusiad.org/tr/yayinlar/raporlar/item/download/7494_67a3aa94bcfce900229f42280fa1ba68, erişim tarihi: 01 Temmuz 2022

22 https://www.ab.gov.tr/siteimages/resimler/Sanayi%204_0%20web.pdf, erişim tarihi: 01 Temmuz 2022

23 https://tusiad.org/tr/yayinlar/raporlar/item/download/7494_67a3aa94bcfce900229f42280fa1ba68, erişim tarihi: 01 Temmuz 2022

24 https://www.kaspersky.com/resource-center/threats/5g-pros-and-cons, erişim tarihi: 01 Temmuz 2022

3.
Potansiyel Tehdit Vektörleri

3. Potansiyel Tehdit Vektörleri[25]

Telekomünikasyon ağlarının yeni bir boyuta evrimini simgeleyen 5G kablosuz iletişim teknolojisi, kullanıcılar ve üreticiler için yeni bağlantı, yetenek ve hizmet kümeleri bağlamında çok çeşitli gelişmelere imkân yaratmaktadır. Milyarlarca cihaz için bağlantı sağlayarak küresel anlamda yeni pazarlar yaratacak ve yeni inovasyonların önünü açacak olan bu gelişmeler, aynı zamanda ulusal ve ekonomik güvenliği tehdit eden ve diğer ulusal ve küresel çıkarları etkileyen önemli riskleri de barındırdığı değerlendirilmektedir. Bu bağlamda, 5G ağları; teröristler dâhil suçlu düşünen beyinler ve ülke güvenliğine yönelik diğer tehdit kaynakları için değerli bilgi ve istihbarattan yararlanabilecekleri çekici bir hedef olması muhtemeldir.[26] Bir ülkedeki ekonomik hayatın resmedilmesinde önemli aktörler olan işletmeler; öncelikle, ulaşılabilirliği, güvenliği, gizliliği ve uyumluluğu artırırken veri akış trafiğinin gecikmesini azaltmalarına imkân yaratan ve daha fazla kontrol sağlayabilecekleri söz konusu özel ağları seçmektedirler. Bu nedenle, büyük ölçekli kamuya açık 5G ağlarının kurulumuna rağmen, özel kurumsal ağların gelecekte operatörler için önemli bir gelir kaynağı olacağı ancak güvenlik konusunun operatörler için giderek daha önemli bir farklılaştırıcı etki yaratacağı değerlendirilmektedir. 5G'nin taşıdığı yeni riskler nedeniyle, bu operatörlerin birçoğunun bu tür kablosuz iletişim ağlarını güvenli bir şekilde yönetmek için gereken araçlara veya kaynaklara sahip olduğu şüphelidir.[27]

25 https://media.defense.gov/2021/May/10/2002637751/-1/-1/1/POTENTIAL%20THREAT%20VECTORS%20TO%205G%20INFRASTRUCTURE.PDF, erişim tarihi: 10 Temmuz 2022

26 https://media.defense.gov/2021/May/10/2002637751/-1/-1/1/POTENTIAL%20THREAT%20VECTORS%20TO%205G%20INFRASTRUCTURE.PDF, erişim tarihi: 10 Temmuz 2022

27 https://www.trendmicro.com/en_us/research/21/g/with-5g-coming-its-time-to-plug-security-gaps.html, erişim tarihi: 07 Temmuz 2022

Bu yöndeki endişelere binaen, ülkeler farklı tedbirler geliştirme çabası göstermektedir. Örneğin; ABD Ulusal Telekomünikasyon ve Bilgi İdaresi (The United States National Telecommunications and Information Administration/NTIA), ABD'nin yurt içinde ve dışında 5G altyapısını nasıl güvence altına alacağına ilişkin stratejisinin genel hatlarını ortaya koymak üzere "5G'nin Güvenliğini Sağlamak için Ulusal Strateji" ("the National Strategy to Secure 5G") belgesini geliştirdiği bilinmektedir. ABD Ulusal Siber Stratejisi (the National Cyber Strategy) ile uyumlu olarak, söz konusu 5G strateji belgesi; 5G'nin yurt içinde yaygınlaştırılmasını kolaylaştırma, 5G yeteneklerine ve altyapısına yönelik siber güvenlik risklerini değerlendirme ve temel güvenlik ilkelerini belirleme, küresel anlamda 5G altyapısının geliştirilmesi ve konuşlandırılması sırasında ABD'nin ekonomik ve ulusal güvenliğine yönelik riskleri ortaya koyma ve güvenli/güvenilir 5G altyapısının sorumlu küresel gelişimini ve dağıtımını teşvik etme yönünde dört ana alanda çalışılması gereğine işaret etmektedir. Bu doğrultuda, ABD'nin söz konusu 5G strateji belgesi hükümlerine uyumlu olarak, 5G altyapısına yönelik risklerin ve güvenlik açıklarının değerlendirilmesine katkı sağlamak maksadıyla, istihbarata dayalı olarak ortak siber güvenlik sorunları üzerinde çalışmak için özel ve kamu sektörlerinden temsilcilerini bir araya getirmek üzere ABD Kalıcı Güvenlik Çerçevesi (the Enduring Security Framework/ESF)[28] de belirlenmiştir.[29] Bu yönde, tedarik zinciri riskinin değerlendirilmesi ve yönetilmesinde mevcut yeteneklerin üzerine inşa edilmesine yönelik olarak, ABD Kalıcı Güvenlik Çerçevesi 5G Tehdit Modeli Çalışma Paneli (the ESF 5G Threat Model Working Panel) kurulmuştur. Bir girizgâh olarak 5G ortamına yönelik bilinen ve potansiyel tehditlerin toplu bir listesini yapmak için mevcut çalışmaları gözden geçirerek 5G'nin uygulanabileceği alanlara ilişkin örnek senaryoları oluşturan ve 5G çekirdek teknolojilerine yönelik riskleri değerlendiren bahse konu panel, ilk olarak 5G bağımsız olmayan (non-standalone/NSA) ağların kullanımına yönelik potansiyel tehdit vektörlerini araştırmaya ve önceliklendirmeye odaklanmıştır.[30]

28 ABD'de kamu kesiminden uzmanların yanı sıra bilgi teknolojisi, iletişim ve savunma sanayi sektörlerinden gelen temsilcilerden oluşan ABD Kalıcı Güvenlik Çerçevesi (ESF); ABD ulusal güvenlik sistemlerinin güvenlik ve istikrarına yönelik tehditlere ve risklere yönelik olarak Kritik Altyapı Ortaklığı Danışma Konseyi (the Critical Infrastructure Partnership Advisory Council/CIPAC) himayesinde faaliyet gösteren sektörler arası bir çalışma grubudur.

29 https://media.defense.gov/2021/May/10/2002637751/-1/-1/1/POTENTIAL%20THREAT%20VECTORS%20TO%205G%20INFRASTRUCTURE.PDF, erişim tarihi: 10 Temmuz 2022

30 https://media.defense.gov/2021/May/10/2002637751/-1/-1/1/POTENTIAL%20THREAT%20VECTORS%20TO%205G%20INFRASTRUCTURE.PDF, erişim tarihi: 10 Temmuz 2022

Verilerinin üretilmesinin yanında nasıl değerlendirildiğinin de ayrıca önem taşıdığı göz önünde bulundurulduğunda, artan bağlantı hızıyla birlikte artan veri trafiği hacmi içerisinde doğru verinin doğru zamanda doğru yere güvenli bir biçimde belli standarda göre iletilebilme kapasitesinin faydalı bilgi elde edilmesindeki payı da yadsınamayacaktır. 1995'te küresel mobil operatör standartlarını geliştirmek üzere kurulan Groupe Spéciale Mobile Association (GSMA), Afganistan'dan Zimbabwe'ye kadar dünya çapında farklı ülkelerde hizmet vermekte olan mobil operatör gruplarını, şebekelerini ve mobil sanal ağ operatörlerini (Mobile Virtual Network Operator/MVNO) kapsayan aboneliğe dayalı veri platformu olan "GSMA Intelligence" üzerinden mobil ağ ve gruplara dair operasyonel ve finansal sektör verileri ile ülkelere ait çeşitli mobil iletişim kullanım verilerine her an erişim imkânı sunmaktadır.[31] Bu bağlamda, Trend Micro ve GSMA Intelligence'ın kamuoyuyla paylaştığı ve küresel ağ operatörlerinden ve sektördeki küresel işletmelerden kişileri kapsayan iki ayrı GSMA anketine dayanan bir rapora göre operatörlerin %51'i özel ağ güvenliğini artırmak için bilişim teknolojileri (BT) ve bulut tedarikçi ortaklıklarına öncelik vermesine rağmen, %22'si özel güvenlik sağlayıcılarından hizmet alacaktır. Kısacası, çoğu müşterileri ve gelir beklentileri için tehditlerden korunmanın önemini anlamakla birlikte genel anlamda operatörlerin, güvenlik sağlayıcıları ile olması gerektiği değerlendirilen seviyede ortaklıklara hâlâ öncelik vermedikleri ileri sürülmektedir. Söz konusu raporda; kaç telekom şirketinin bu anlamda güvenliği artırmayı amaçladığına dair uygulamada karşılaşılan belirsizliğin, muhtemel tehditlere karşı bazı korumaların 5G'de hâlihazırda yerleşik biçimde geldiği ve ek güvenliğe daha az ihtiyaç duyulduğuna dair yanlış varsayımlara dayanıyor olabileceği önermesi yapılmaktadır.[32] Rapora konu olan araştırmaya göre, operatörlerin; %68'inin şu anda kurumsal müşterilere özel kablosuz ağlar sattığını, geri kalanının ise 2025 yılına kadar bunu yapmayı planladığını ortaya koymakta, %45'inin uzun vadeli kurumsal gelir hedeflerine ulaşmak için siber güvenliğe yatırım yapmanın "son derece önemli" olduğunu ifade ettiği belirtilmektedir.[33] Raporda, 5G teknolojisi yüzünden bulut, veri ve IoT tehditleri iç içe geçtikçe dikkate alınması gereken yeni ve potansiyel olarak daha büyük güvenlik risklerinin ortaya çıktığı savıyla,

31 https://webrazzi.com/2013/06/14/gsma-intelligence/, erişim tarihi: 01 Temmuz 2022

32 https://www.trendmicro.com/en_us/research/21/g/with-5g-coming-its-time-to-plug-security-gaps.html, erişim tarihi: 07 Temmuz 2022

33 https://www.trendmicro.com/en_us/research/21/g/with-5g-coming-its-time-to-plug-security-gaps.html, erişim tarihi: 07 Temmuz 2022

operatörlerin %32'sinin artan bir saldırı yüzeyine işaret ettiği söylenmektedir. Bu arada, tecrübe edilen pandemi döneminin, başta fidye yazılımıyla ilgili ihlal riski olmak üzere bu tür sorunları yalnızca yoğunlaştırdığı iddia edilmektedir. Bu bulgulara rağmen, operatörlerin %48'inin güvenlik açıklarıyla başa çıkmak için yeterli bilgiye ya da araca sahip olmamalarının bir numaralı zorluk olduğunu kabul ettiği ve mevcut nitelikli insan gücü kaynağı bağlamında %39'luk bir oranla sınırlı bir güvenlik uzmanı havuzunun bulunmasının kurum içi kapasiteyi daha da azalttığı ifade edilmektedir (Grafik 1).[34]

Kaynak: The GSMA Intelligence Operators in Focus: Enterprise Opportunity 2021 anketi
*https://www.trendmicro.com/en_us/research/21/g/with-5g-coming-its-time-to-plug-security-gaps.html

Grafik 1: 5G Tabanlı Hizmetlerin Sunumunda Karşılaşılan Sorunlar

Kablosuz iletişimde 5G teknolojisine geçiş, zengin fırsatlar ve yetenekler sunarken, yeni güvenlik açıklarını ve tehditlerini de beraberinde getirdiğinden, ABD Kalıcı Güvenlik Çerçevesi ve 5G Tehdit Modeli Çalışma Paneli tarafından ülke 5G'ye geçerken karşılaşılabilecek riski artırma potansiyeline sahip üç tehdit vektörü tanımlanmaktadır. Söz konusu tehdit vektörleri her türlü ihtimalatı içeren kapsayıcı bir liste olarak görülmese de çeşitli 5G kablosuz iletişim teknolojileri alanındaki

34 https://www.trendmicro.com/en_us/research/21/g/with-5g-coming-its-time-to-plug-security-gaps.html, erişim tarihi: 07 Temmuz 2022

tehditlerin bir girizgâhını temsil etmekte ve tehdit aktörlerinin istismar edebileceği ek güvenlik açığı noktalarını tanımlayan alt tehditleri de içermektedir.[35]

3.1. 5G Politika ve Standartlarıyla İlgili Riskler ve Güvenlik Açıkları

5G teknolojilerinin dayandığı iletişim altyapısının şekillendirilmesine ilişkin güvenlik tasavvurlarında bu teknolojiye yönelik olarak geliştirilen politika ve standartlar belirleyici olmaktadır. Sınır bilişim (edge computing), otonom araçlar ve teletıp gibi yeni teknolojilerin tasarımını ve mimarisini etkileyecek teknik standartlar ve güvenlik kontrolleri geliştirme çalışmaları, küresel standartlar belirleme yönünde faaliyet gösteren kuruluşlar[36] vasıtasıyla yürütülmektedir. Bahse konu kuruluşlarca 5G teknolojisi için politika ve standart belirlemeye yönelik alınan kararlar bu teknolojinin uygulanması ve benimsenmesi üzerinde etki etmektedir. Bununla birlikte, geliştirme sürecinin katkı sağlayabilecek tüm katılımcılara açık, paydaşların denetimini kolaylaştıran şeffaf bir anlayışa dayalı ve üzerinde fikir birliğine varılmış bir şekilde inşasının sağlanamadığı bir ortamda, yeni 5G politika ve standartlarının yayımlanması son kullanıcıyı etkileyen tehdit potansiyelinin varlığının devamına hizmet edeceği değerlendirilmektedir. Örneğin, küresel anlamda düşünüldüğünde

35 https://media.defense.gov/2021/May/10/2002637751/-1/-1/1/POTENTIAL%20THREAT%20VECTORS%20TO%205G%20INFRASTRUCTURE.PDF, erişim tarihi: 10 Temmuz 2022

36 The 3rd Generation Partnership Project (3. Nesil Ortaklık Projesi), Internet Engineering Task Force (İnternet Mühendisliği Görev Kuvveti) ve the International Telecommunication Union (Uluslararası Telekomünikasyon Birliği) gibi

açık, şeffaf ve fikir birliğine dayalı olmayan bir süreçte ulus-devletler; müseccel yani mülkiyet hakkına sahip oldukları kendi teknolojilerinin faydasını artıran ve bu tür teknolojileri satın alan müşterilerin başka ülke teknolojilerine ait yazılım ya da ekipmanları tam desteklemeyerek kullanım seçeneklerini kendilerinkiyle sınırlayan standartlar geliştirilmesi yönünde orantısız bir etki gösterme eğiliminde bulunabilirler. Ayrıca, standart belirleme yönünde faaliyet gösteren kuruluşların, bağlayıcı olmayan ve operatörlerin isteğine bırakılan kontroller geliştirmesinin de uygulanmayan standartların oluşturacağı öznel güvenlik önlemlerine dayalı sahte güvenlik algısı neticesinde küresel ağda boşluklar oluşturarak tehdit aktörlerince istismar edebilecek bir açık kapı bırakma olasılığı da göz ardı edilmemelidir.[37]

3.1.1. Birlikte Çalışabilirlik Standartlarına İlişkin Riskler

Genel bir tanımlamayla, "bir sistemin ya da sürecin, ortak standartlar çerçevesinde bir diğer sistemin ya da sürecin bilgisini ve/veya işlevlerini kullanabilme yeteneği" birlikte çalışabilirlik olarak ifade edilmektedir.[38] Teknolojiye dayalı küresel rekabetin yaşandığı bir ortamda, milli menfaatleri çatışan rakip ülkeler 5G için teknik standartların geliştirilmesine katkıda bulunduğundan, geliştirilen standartların; bahse konu ülkelerdeki geliştiricilerin kendi sistemlerine özgü olan ancak karşı ülke tarafından güvenilir kabul edilmeyen teknolojileri ve ekipmanı içerme potansiyeli göz önünde bulundurulmalıdır. Bu çerçevede, farklı üreticilere ait ağ teknolojilerinin birlikte çalışabilirliğine yönelik standartların varlığı da ayrı bir önem kazanmaktadır.[39]

Bir ülkenin müseccel teknolojisinin kullanıcılarının, satın aldıkları teknolojinin şart koştuğu yazılım ya da ekipmanları edinme mecburiyetinde kalma ihtimali, re-

37 https://media.defense.gov/2021/May/10/2002637751/-1/-1/1/POTENTIAL%20THREAT%20VECTORS%20TO%205G%20INFRASTRUCTURE.PDF, erişim tarihi: 10 Temmuz 2022

38 http://www.bilgitoplumu.gov.tr/wp-content/uploads/2014/04/Birlikte_Calisabilirlik_Esaslari_Rehberi_2.1.pdf, erişim tarihi: 10 Temmuz 2022

39 https://media.defense.gov/2021/May/10/2002637751/-1/-1/1/POTENTIAL%20THREAT%20VECTORS%20TO%205G%20INFRASTRUCTURE.PDF, erişim tarihi: 10 Temmuz 2022

kabeti sınırlama ve karşı ülkedeki müşterileri de rakibin güvenilmeyen, yeni teknolojisini benimsemeye zorunlu kılma olasılığı taşımaktadır. Diğer bir ülkenin ürettiği teknolojinin, rakip ülkelerin söz konusu güvenilirliği şüpheli müseccel teknolojileriyle birlikte çalışabilirliğinin sağlanamaması durumunda da 5G ticari bir bağlamda ele alınıp yeni bir pazar olarak değerlendirilirse o pazarda şirketlerin rekabet etme yeteneklerinin görece sınırlanacağını söylemek yanlış olmayacaktır. Örneğin, bir hizmet sektörüne özgü veya gelişmekte olan teknoloji standardında, ilk atılımı yaparak donanım ve yazılım geliştirmeye başlayan bir ulus-devlet o alanda küresel bir lider konumuna yükseldiğinde, üretim veya siber kapasite yönünden kendi faydasını maksimize eden de facto ulusal standartları da belirlemiş olması beklendik bir durumdur. Ancak bu ulus-devletin milli menfaatler yönünden karşıt bir ülke olması durumunda, bahse konu sektörde vatandaşlarına hizmet sunmak isteyen diğer bir devlet ya bu rakip ve güvenilirliği şüpheli olan ülkenin teknolojisini kullanmak veya nispeten güvenilir kabul edilen başka bir tedarikçiden söz konusu rakip ülkenin de facto standartlarına göre tasarlanmış benzer teknolojileri temin ederek kullanmak zorunluluğunda kalabileceği değerlendirilmektedir. Karşıt ulus-devlet, o hizmete erişmeye çalışan diğer ülkeyi dezavantajlı duruma sokacak ve pazar büyümesini engelleyecek teknolojiler geliştirmeleri veya kullanmaları için bahse konu tedarikçiler üzerinde etki yaratma çabası gösterebilir. Bu bağlamda ulus-devletler, 5G teknolojileri üzerindeki küresel etkilerini artırarak diğer devletlerin bu teknoloji ağlarında güvenilmeyen bileşenleri kullanmaya mecbur kalacağı bir ortam yaratmak için gelişmekte olan teknolojilerinin erken bir safhada benimsenmesini sağlama yönünde gayret birliğinde bulunmaları ihtimal dahilindedir.[40]

Birlikte çalışabilirlik standardını karşılamayan ve ülkelerin kendilerine özgü 5G teknolojilerinin güncellenmesi, onarılması ve değiştirilmesi küresel çapta kullanıcılar için bazı zorluklar yaratabileceği gibi esasen küresel bir etkileşimi hedef alan 5G teknolojilerinden bir kısmının bazı kullanıcılar için görülüp erişilemez bir alanda kalması da mümkündür. Bu durum, söz konusu teknolojik ürünlerin yaşam döngüsü maliyetini artırma ve ekipman değiştirilmesi gerektiğinde 5G teknolojisinin dağıtımını geciktirme potansiyeli de taşıyacağı değerlendirilmektedir.[41]

40 https://media.defense.gov/2021/May/10/2002637751/-1/-1/1/POTENTIAL%20THREAT%20VECTORS%20TO%205G%20INFRASTRUCTURE.PDF, erişim tarihi: 10 Temmuz 2022

41 https://media.defense.gov/2021/May/10/2002637751/-1/-1/1/POTENTIAL%20THREAT%20VECTORS%20TO%205G%20INFRASTRUCTURE.PDF, erişim tarihi: 10 Temmuz 2022

3.1.2. Tercihe Bağlı Güvenlik Kontrollerine İlişkin Riskler

Küresel standartlar belirleme yönünde faaliyet gösteren kuruluşların mobil telekomünikasyon için geliştirdikleri protokollerin bazıları mecburi veya tercihe bağlı güvenlik kontrollerini içerebilmektedir. Güvenlik kontrollerinin tercihe bağlı olarak tasarlanması durumunda, bunları uygulamamayı tercih eden kuruluşların/iletişim sağlayıcılarının işlettikleri ağlar daha savunmasız kalma ve siber saldırılara hedef olma bakımından daha yüksek risk taşıma olasılığı barındırmaktadır. Bu çerçevede, 5G teknolojilerinde tercihe bağlı güvenlik kontrollerini uygulamayan sistemlerdeki güvenlik açıklarının farkında olan karşıt ulus-devlet aktörleri, söz konusu kuruluşları/iletişim sağlayıcılarını hedef alarak bu tür özel ağları istismar etmek için yöntemler kullanabilir.[42] 5G kablosuz iletişim ağlarının, kamudan özel sektöre günlük hayatta da etkisini gösterecek şekilde Wi-Fi'nin yerini almaya başlamasıyla kötü niyetli olabilecek aktörlerin bazı ağlara etki edebilme ve erişim sağladıkları ağların boyutu, kullanım amacı ve kullanıcı sayısıyla birlikte düşünüldüğünde de yaratabilecekleri tesirin ve verebilecekleri zararın artış gösterme ihtimali bulunmaktadır. Örneğin, bir üniversite; kampüsünde kurulan 5G ağında önerilen, ancak tercihe bağlı bırakılan güvenlik kontrollerinin tümünü önerilen şekilde yapılandırmaz ya da uygulamaz ise söz konusu 5G ağında kötü niyetli aktörlerin istismarına açık önemli siber güvenlik boşluklarına neden olarak o ağa bağlı tüm cihazlar ve kullanıcıları için zarar riskini artırması beklendik bir durumdur.[43]

42 https://media.defense.gov/2021/May/10/2002637751/-1/-1/1/POTENTIAL%20THREAT%20VECTORS%20TO%205G%20INFRASTRUCTURE.PDF, erişim tarihi: 10 Temmuz 2022

43 https://media.defense.gov/2021/May/10/2002637751/-1/-1/1/POTENTIAL%20THREAT%20VECTORS%20TO%205G%20INFRASTRUCTURE.PDF, erişim tarihi: 10 Temmuz 2022

3.2. Tedarik Zinciri Riskleri ve Güvenlik Açıkları[44]

Tedarik zinciri; emtia ve hizmetlerin üretim ve dağıtım sürecinde ham bileşenlerden başlayarak nihai ürünün tüketiciye ulaştırılması için takip edilen akış sırası olarak tanımlanabilir.[45] Tehdit kaynaklarının; casusluk, sabotaj, dış müdahale ve suç işleme amacıyla bilgi ve iletişim teknolojilerini (BİT) ve ilgili tedarik zincirlerini istismar etme gayretleri tedarik zinciri riskini oluşturmaktadır. Kötücül yazılım ve donanımlar, taklit (sahte) bileşenler ile kötü tasarım, üretim ve bakım işlem/süreçleri gibi zarar yaratma olasılığı yaratan durumlar, diğer BİT'lerde olduğu gibi 5G tedarik zinciri için de hassasiyet yaratmaktadır. Milyarlarca cihazın erişim sağlaması beklenen 5G ağıyla daha önceki nesillerden daha yüksek hızlı ve yüksek kapasiteli kablosuz bağlantı imkânına bir an önce erişmek için oluşan beklentiye cevaben yapılacak ihtiyatsız bir yaygınlaştırma hamlesi, tedarik zincirine güvenilir olmayan veya taklit bileşenlerin eklenmesi riskini artırabileceği değerlendirilmektedir. Nihayetinde son kullanıcı cihazlarını da (bilgisayar, telefon vb.) etkileyen güvenliği ihlal edilmiş (dış aktörler tarafından sızılmış) bir iletişim altyapısını veya nesne bileşenlerini de içerecek şekilde, artan risk ortamı; 5G ağının bütünlüğüne olan güven kaybı, veri/fikri mülkiyet hırsızlığı ya da sistemin/ağın arızasıyla sonuçlanabilecek kötüye kullanım gibi istenmeyen durumlara zemin hazırlayabilir. Özellikle telekomünikasyon ağlarında önemli uluslararası pazar payına sahip ancak güvenilirliği şüpheli olan şirketler veya diğer ulus-devlet destekli tedarikçiler de, tedarik zinciri riski kapsamında ele alınabilmektedir. Tedarik zincirlerinin güvenliği ihlal edilmiş şirketlerden donanım ve yazılım temin eden ülkelerin, verilerinin dış aktörler tarafından ele geçirilmesi, manipülasyonu, bozulması ya da yok edilmesi tehdidine karşı hassas olabileceği

44 https://www.trendmicro.com/en_us/research/21/g/with-5g-coming-its-time-to-plug-security-gaps.html, erişim tarihi: 07 Temmuz 2022

45 https://www.ibm.com/topics/supply-chain-management, erişim tarihi: 07 Temmuz 2022

değerlendirilmektedir. Ayrıca bir ülkenin, güvenilir olduğu düşünülen kendi ağının başka bir ülkenin güvenirliği şüpheli ağına yaptığı bağlantı üzerinden uluslararası ortaklarına veri gönderirken maruz kalabileceği bu tür tehditlere karşı oluşan hassasiyetinde çeşitli zorluklar yaratabileceği de unutulmamalıdır.[46]

Bu durumun, özellikle çeşitli operatörler tarafından işletilen bu küresel ağ yapısı bakımından düşünüldüğünde, söz konusu operatörlerin sınırlı güvenlik uzmanı havuzunun yarattığı düşük kurum içi kapasitenin, kurumsal hizmet dağıtım süreçleri üzerinde dört temel alanda ciddi bir etki yaratabileceği değerlendirilmektedir.[47]

Bunlar, Sanallaştırma ve Ağ Güvenliği Riskleri, Nesnelerin İnterneti(IoT) ve Spektrum Frekanslarının Paylaşımına İlişkin Riskler, 4G Ağlarından Kalma Güvenli Riskleri, Çoklu Erişim Sınır Bilişimine(Multi-Access Edge Computing) İlişkin Riskler başlıklar altında özetlenebilir.

3.2.1. Sanallaştırma ve Ağ Güvenliği Riskleri

5G çekirdek ağı; yaygın olarak kullanımı ve bilinirlikleri nedeniyle bilgisayar korsanlığı açısından büyük bir hedef olarak kabul edilebilecek, HTTP (Hypertext Transfer Protocol/Bağlantılı Metin Aktarım Protokolü) ve REST API (Representational State Transfer Application Programming Interface/Temsilî Durum Aktarımı Uygulama Programlama Arayüzü) protokollerini kullanan Yazılım Tanımlı Ağ İletişimine (software-defined networking/SDN) ve Ağ İşlevlerini Sanallaştırmasına (network functions virtualisation/NFV) dayanır. Bu bağlamda, operatörlerin %41'ine göre sanallaştırma güvenlik açıkları 5G ağlarında büyük bir güvenlik sorunu olarak görülmektedir.[48]

Günümüzde, donanım merkezli anlayıştan ziyade daha esnek ve daha hızlı yenileşime imkân veren yazılım tabanlı bir ağ mimarisi modeline doğru bir dönüşümün yaşandığı kabul edilebilir. SDN ve NFV teknolojileri bu dönüşümü desteklemektedir. Açık standartlar geliştirerek SDN'nin benimsenmesi yolunda çaba harcayan bir kurum olan Open Network Foundation'a (ONF) göre SDN, "doğrudan programlanabilen ve ağ kontrolünün iletimden ayrıştırıldığı bir yapıyla ortaya çı-

46 https://media.defense.gov/2021/May/10/2002637751/-1/-1/1/POTENTIAL%20THREAT%20VECTORS%20TO%205G%20INFRASTRUCTURE.PDF, erişim tarihi: 10 Temmuz 2022

47 https://www.trendmicro.com/en_us/research/21/g/with-5g-coming-its-time-to-plug-security-gaps.html, erişim tarihi: 07 Temmuz 2022

48 https://www.trendmicro.com/en_us/research/21/g/with-5g-coming-its-time-to-plug-security-gaps.html, erişim tarihi: 07 Temmuz 2022

kan ağ mimarisi"dir. The European Telecommunications Standards Institute (ETSI) Industry Specification Group (ISG), önceden özel olarak geliştirilmiş donanımların sağladığı ağ fonksiyonlarının sanallaştırılması amacıyla NFV'yi ortaya koymuştur. Yazılım tabanlı bir çözümler olarak ağın bütüncül yönetimi yoluyla ağda daha fazla esnekliğe ve daha hızlı yenileşime olanak sağlayan SDN, büyük ve karmaşık ağların oluşturulup yönetimini kolaylaştırırken; azaltılmış ekipman maliyeti ve düşük güç tüketimi sunan NFV, yeni hizmetlerin geliştirilmesine, denenmesine ve düzenlenmesine ilişkin yatırım harcamalarına (CAPEX) ve operasyonel harcamalara (OPEX) bağlı maliyetleri azaltarak telekomünikasyon ağ kaynaklarının kullanımında verimliliği artırmayı amaçlamaktadır.[49]

Ancak yazılım temelli çözümlerin barındırdığı bazı temel hassasiyetleri de hatırda tutmak faydalı olacaktır. Bir ağdaki rotaları otomatik olarak yapılandırmaya yönelik bir mimari olarak tanımlanabilecek olan SDN; ağ esnekliğini geliştirir ve yönetimi kolaylaştırırken, bant genişliğini daraltabilecek ve işlemleri olumsuz yönde etkileyebilecek şekilde SDN denetleyici uygulamalarına kod yerleştirilerek istismara karşı hassastır.[50] 5G kablosuz ağ iletişim sistemlerinde aynı spektruma erişim için rekabet eden artan sayıda cihazın varlığı, spektrum paylaşımını daha yaygın hale getirmekte, spektrum paylaşımı da kritik iletişim ağlarını olumsuz yönde etkileme olasılığı olan kritik olmayan iletişim yollarının istismara karşı hassasiyetine yol açabilmektedir.[51] 5G teknolojileri, çok sayıda yeni yetenek ve yenileşimi destekleyerek milyarlarca ağ cihazının yüksek hız ve kapasite de kablosuz iletişim ağına bağlanmasını mümkün kılmakla birlikte, söz konusu ağ cihazlarının güvenliği bir ağ katmanı istismarı yoluyla ele geçirilmesi durumunda, dış aktörlerce 5G ağına yetkisiz erişim elde edilerek operasyonların kesintiye uğratılması ve kritik verilerin ele geçirilmesi, manipülasyonu, bozulması ya da yok edilmesi tehdidine karşı hassasiyet ve ağ güvenliği sorunu yaratabileceği değerlendirilmektedir.[52] Kullanıcıların yalnızca bir ağ alanı için kimlik doğrulanmasına izin vererek veri ve güvenlik yalıtımı sağlayan Ağ Dilimleme (Network Slicing) uygulamasının da ağ güvenliği

49 https://www.karel.com.tr/blog/sdn-ve-nfv-nedir-aralarindaki-farklar-nelerdir, erişim tarihi: 10 Temmuz 2022

50 https://media.defense.gov/2021/May/10/2002637751/-1/-1/1/POTENTIAL%20THREAT%20VECTORS%20TO%205G%20INFRASTRUCTURE.PDF, erişim tarihi: 10 Temmuz 2022

51 https://media.defense.gov/2021/May/10/2002637751/-1/-1/1/POTENTIAL%20THREAT%20VECTORS%20TO%205G%20INFRASTRUCTURE.PDF, erişim tarihi: 10 Temmuz 2022

52 https://media.defense.gov/2021/May/10/2002637751/-1/-1/1/POTENTIAL%20THREAT%20VECTORS%20TO%205G%20INFRASTRUCTURE.PDF, erişim tarihi: 10 Temmuz 2022

yönetimi açısından kendine has bazı sorun alanları barındırdığını da hatırlamakta fayda olacaktır. Ağ dilimlemede, söz konusu dilimler ağa karmaşıklık katarak yönetimi zorlaştırabilir. Ayrıca ağ operatörlerinin işlettikleri 5G ağlarının kurulumunun nasıl olması gerektiğine ilişkin teknik özellikleri tanımlayan standartlar olsa da, bu operatörlerin ağ dilimleme için ağ güvenliği geliştirme ve uygulama için takip etmeleri gereken net teknik özellik tanımlamaları yoktur. Bu nedenle, uygun olmayan ağ dilimi yönetiminin; farklı dilimlerdeki verilerin yetkisiz dış aktörlerin erişimi veya öncelikli kullanıcıların erişimini engellemesi suretiyle ağın istismarına karşı hassasiyet yaratabileceği unutulmamalıdır.[53]

3.2.2. Nesnelerin İnterneti (IoT) ve Spektrum Frekanslarının Paylaşımına İlişkin Riskler

IoT'yi uygulamaya koyan kuruluşların içerisinde ağ işletim politikalarını güvenliği önceliklendiren bir strateji oluşturacak şekilde güncelleyenlerin oranının nispeten az olduğu bilinmektedir. Bunda IoT çözümlerinin tasarım gereği zaten güvenli olacağına yönelik bir beklentinin rol oynadığını söylemek yanlış olmayacaktır. Örneğin, ABD'de ülkede IOT'yi devreye alan kuruluşların oranı %63 olup bunların sadece %15'inin stratejisi "önce güvenlik" olarak güncellenmiştir. 5G ağının kapasitesi göz önünde bulundurulduğunda, çok sayıda bağlantı içerisinde güvenli olmayan cihazların oluşturabileceği büyük saldırı yüzeyi potansiyeli nedeniyle, bu ortamda operatörlerin güvenlik çözümlerinin kullanımında proaktif olmaları gerektiği değerlendirilmektedir.[54]

Ayrıca, üçüncü taraf tedarikçilerin, satıcıların ve hizmet sağlayıcıların meydana getirdiği genişletilmiş tedarik zincirlerinden devralınan nesne bileşenlerinin de ağ sisteminde zafiyet yaratma potansiyeli bulunmaktadır. Ürün geliştirme, üretim veya dağıtım hatlarında nispeten daha zayıf güvenlik kontrollerine ve denetimlerine sahip olabilecek ağ bileşeni tedarikçilerine ve söz konusu tedarikçilerin tedarikçilerine yönelik muhtemel saldırılar dolayısıyla tedarik zincirlerinin güvenliğinin ihlal edilme olasılığı ihmal edilmemelidir. Örneğin, ürün geliştirme aşamasının ilk safhalarında yerleştirilebilecek açık kapıların ya da kötücül yazılımların sonradan tespit edilmesi daha zor olacağından; geliştiricinin bu kusurları fark edemeden gü-

53 https://media.defense.gov/2021/May/10/2002637751/-1/-1/1/POTENTIAL%20THREAT%20VECTORS%20TO%205G%20INFRASTRUCTURE.PDF, erişim tarihi: 10 Temmuz 2022

54 https://www.trendmicro.com/en_us/research/21/g/with-5g-coming-its-time-to-plug-security-gaps.html, erişim tarihi: 07 Temmuz 2022

venlik açısından kusurlu olan bir bileşeni sorunsuz olarak tanımlaması ve bu tür bileşenlerin ağda kullanılmasıyla da istismara açık güvenlik açıkları oluşabilecektir.[55]

Güvenliği ihlal edilmiş taklit bileşenlerin; kuvvetle muhtemel düşük olan kaliteleri ve siber saldırılara karşı zayıflıkları da göz önünde bulundurulduğunda, ağa bağlı cihazlar arasında dolaşan verileri gizlilik, bütünlük veya kullanılabilirlik açısından etkileyebilecek ve ağın diğer daha hassas bölümlerine sirayete olanak sağlayabilecek şekilde istismara karşı hassasiyet yaratması beklendik bir durumdur.[56] Örneğin, kurumsal bir BİT bileşenleri ihalesini kazanan ve yasal şartları sağlayan bir yüklenici firma; maliyet açısından daha tassaruflu olacağı düşüncesiyle, bu tür değiştirilmiş/taklit ürünlerin indirimli fiyatlarla satışını yapan bir tedarikçiden aldığı parçaları bilmeden portföyüne ekleyebilir. Bu farazi yüklenici; ilgili sektördeki riskler konusunda yeterli farkındalık düzeyinde olmayabilir ve taklit parçalara karşı ön analiz yapma gibi bir prosedürü işletmiyor olabilir. Taklitçiler, tanınmış üreticilerin yüksek kaliteli parçalarını arayan müşterilere normal parçalar gibi görünen standart altı veya kusurlu parçalar satabilmektedir. Bu taklit parçalar kullanılabilirlik ve işlevsellik testlerinde de tespit edilemezse bunların ağ iletişiminde kullanımı sonucunda genel sistem ve son kullanıcı açısından sistem performansının düşmesi, kritik hizmetlerin kullanılabilirliğinde sorunlar veya veri kaybı gibi olumsuz etkiler yaşanması olasıdır.[57]

Ağ yapısında kullanılan yazılım veya ağ bileşenlerine yetkisiz erişime neden olabilecek yazılım/konfigürasyon kusurları, yetkisiz dış aktörlere; ağın güvenlik kontrollerini indirgemek, sisteme kötücül yazılım yüklemek veya üründeki zayıflıkları belirlemek için yapılandırmaları değiştirme ve ayrıcalıklı erişim fırsatı sunarak istismara açık güvenlik açıkları yaratabilir.[58] Hatalı risk yönetim kararlarına dayalı uygulamalar tedarik zincirinde ne kadar derinde olursa önceden tespit edilmesi de o kadar zor olacaktır. Yazılım tedarik zinciri saldırısı, hedef kullanıcılara gönderilen bir bileşene kasıtlı olarak kötücül kod eklenerek gerçekleştirilebilmektedir. Örneğin; güvenliği ihlal edilmiş bu bileşenleri; yetkili ve normal bir dağıtım

55 https://media.defense.gov/2021/May/10/2002637751/-1/-1/1/POTENTIAL%20THREAT%20VECTORS%20TO%205G%20INFRASTRUCTURE.PDF, erişim tarihi: 10 Temmuz 2022

56 https://media.defense.gov/2021/May/10/2002637751/-1/-1/1/POTENTIAL%20THREAT%20VECTORS%20TO%205G%20INFRASTRUCTURE.PDF, erişim tarihi: 10 Temmuz 2022

57 https://media.defense.gov/2021/May/10/2002637751/-1/-1/1/POTENTIAL%20THREAT%20VECTORS%20TO%205G%20INFRASTRUCTURE.PDF, erişim tarihi: 10 Temmuz 2022

58 https://media.defense.gov/2021/May/10/2002637751/-1/-1/1/POTENTIAL%20THREAT%20VECTORS%20TO%205G%20INFRASTRUCTURE.PDF, erişim tarihi: 10 Temmuz 2022

kanalının bir parçası dâhilinde gerçek durumundan bihaber olarak alan kullanıcılar kendi sistemlerine ve ağlarına katabilir. Bilindik uygulama ve yazılım testlerinden gizlemek maksadıyla gelişmiş kötücül kod, normal işlemleri kesintiye uğratmaksızın bir müddet dış aktörler tarafından etkinleştirilmeyebilir. Bu bağlamda, bir telekomünikasyon şirketi, güvenilir kabul edilen bir tedarikçiden çekirdek ağ sistemleri yönetim yazılımı satın aldığında; bu tedarikçinin bilgisi dışında ürününde kullandığı bileşenlerden birinin güvenliği kötücül bir kod ile ihlal edilmiş olabilir. Bu durumun yarattığı güvenlik açığı, telekomünikasyon şirketinin çekirdek ağına erişim sağlamak ve diğer saldırı vektörlerine yönelmek için daha büyük bir saldırı zincirinin parçası olarak da istimar edilebilir.[59]

3.2.3. 4G Ağlarından Kalma Güvenlik Riskleri

Teknolojik anlamda karşı karşıya olduğumuz yenileşim ve yenileme rüzgârında, 5G özel ağlarının yalnızca azınlık sayılabilecek bir kısmı sıfırdan inşa edileceği bir gerçekliktir. Bu nedenle, eski teknolojilerin bir kısmının bu sistemde varlığı bir şekilde koruyacağını unutmamak gerekmektedir. Bu bağlamda, yeni nesil 5G ağlarının çoğunun mevcut teknolojiler ve altyapı ile bütünleştirilmesi ve birlikte çalışması gerekeceğinden, işleticilerin %26'sına göre sistem içerisinde eski nesil ağların kullanılmaya devam edilmesinin meydana getirdiği bu durumun bazı zorluklar yaratabileceği değerlendirilmektedir.[60] 5G ağ altyapısının her ne kadar daha güvenli olacak şekilde tasarlandığı ileri sürülse de 4G'nin mirası eski iletişim altyapısından gelen güvenlik özelliklerinin ve protokollerinin çoğunun 5G ağlarında desteklendiği de bilinmektedir. Yeni teknoloji ağında da varlığını sürdüren bu eski iletişim

59 https://media.defense.gov/2021/May/10/2002637751/-1/-1/1/POTENTIAL%20THREAT%20VECTORS%20TO%205G%20INFRASTRUCTURE.PDF, erişim tarihi: 10 Temmuz 2022

60 https://www.trendmicro.com/en_us/research/21/g/with-5g-coming-its-time-to-plug-security-gaps.html, erişim tarihi: 07 Temmuz 2022

altyapısı doğru ele alınmazsa istismara açık güvenlik açıkları oluşabilecektir.[61] Bu çerçevede, başlangıçta önceki nesil mevcut 4G Uzun Vadeli Evrim (LTE) kablosuz ağları üzerine kurulan ve bunlarla entegre edilen 5G altyapısının; söz konusu önceki neslin Signaling System 7 (Sinyalizasyon Sistemi 7/SS7) (Bir telefonun kendi GSM operatörü dışında başka bir operatör ile iletişim kurması için kullanılan uluslararası ağdır.) ve Çap Protokolü (Diameter Protocol) (Bilgisayar ağlarında kimlik doğrulama, yetkilendirme ve muhasebe için kullanılan endüstri standardı bir protokoldür.) gibi potansiyel zafiyet alanlarını da barındırdığından eski güvenlik açıklarını içerebilir ve bunlara yönelik eskiden beri karşılaşılmakta olan istismarlara karşı da savunmasız olabilir. Örneğin, yetkisiz bir dış aktör; erişim sağladığı 5G hücresini 4G yanıltmacası (spoofing) yapmaya izin verecek şekilde yapılandırarak bu hücre üzerinden hizmet alan yakındaki kullanıcıların kullandığı BIT bileşenlerine erişim sağlamak için 5G ağında SS7 içindeki güvenlik açıklarını içeren bir 4G ağ yapılandırmasının işletilmesine yol açabilir. Sonrasında söz konusu dış aktör, bu yolla elde edeceği bilgileri daha güvenli ağlara erişim sağlamak için kullanabileceği ve hassas verilere erişim elde edebileceği değerlendirilmektedir.[62]

3.2.4. Çoklu Erişim Sınır Bilişimine (Multi-Access Edge Computing) İlişkin Riskler

Sınır Bilişim (Edge Computing) kavramındaki sınır (edge) ifadesi, tipik olarak ağ diyagramında trafiğin ağa girdiği veya çıktığı noktayı belirtmek için kullanılmaktadır. Ayrıca sınır (edge), veri aktarımı için temel protokolün değişebileceği noktayı da ifade etmektedir. Sınır Bilişim (Edge Computing) cihazlarında kullanılan işlemciler, daha düşük güç ile işlem yapmak ve daha gelişmiş donanım güvenliği sunmak üzere tasarlanmışlardır. Sınır Bilişim, ağ üzerinde istemci verilerinin mümkün mertebe kaynağına yakın olarak işlendiği dağıtılmış bir bilgi teknolojisi mimarisini tanımlamaktadır.[63] Bu bağlamda, Çoklu Erişim Sınır Bilişimi (Multi-Access Edge Computing/MEC); bazı çekirdek ağ işlevlerini, belki de yüzlerce kilometre uzaktaki merkezi bir konuma bel bağlamak yerine, ağ ucundaki son kullanıcıya yaklaştıra-

61 https://media.defense.gov/2021/May/10/2002637751/-1/-1/1/POTENTIAL%20THREAT%20VECTORS%20TO%205G%20INFRASTRUCTURE.PDF, erişim tarihi: 10 Temmuz 2022

62 https://media.defense.gov/2021/May/10/2002637751/-1/-1/1/POTENTIAL%20THREAT%20VECTORS%20TO%205G%20INFRASTRUCTURE.PDF, erişim tarihi: 10 Temmuz 2022

63 https://www.karel.com.tr/blog/edge-computing-nedir-cloud-computing-ve-fog-computingden-farki-nedir#:~:text=Edge%20Computing%2C%20istemci%20verilerinin%20a%C4%9F%C4%B1n,ba%C4%9Fl%C4%B1%20ayg%C4%B1tlar%C4%B1n%20say%C4%B1s%C4%B1%20taraf%C4%B1ndan%20y%C3%BCr%C3%BCt% C3%BCl%C3%BCr., erişim tarihi: 01 Temmuz 2022

rak verilerin işlenme ve saklanma şeklini dönüştürmektedir.[64] Çok büyük miktarda ham veriyi bir ağ üzerinden uzaktaki bir veri merkezine iletmenin ağ kaynaklarına büyük yük getirdiği düşünüldüğünde, bazı durumlarda, verileri kaynağına yakın bir noktada işlemek ve ağ üzerinden yalnızca değeri olan verileri uzaktaki bir veri merkezine göndermek verimliliği artırmaktadır.[65]

Sınır Bilişim, IoT'ye bağlı cihazlarca yürütülmektedir. Çok sayıda sensörün (duyarganın) entegre edildiği ve bunlardan alınan verilerle çalışan otonom araçlar, akıllı evler ve benzeri cihazların çalışması için gerekli bilgisayar uygulamalarını, merkezi düğümlerden ağın uç noktalarına doğru iterek ağa (veya veri merkezine) sürekli olarak bağlanması gerekliliğini ortadan kaldırmaktadır.[66] Ancak güvenilir olmayan 5G bileşenlerinin bu sisteme eklemlenmesi, çekirdek ağ bileşenlerini; yazılım ve donanım güvenlik açıkları, taklit bileşenler ve yetersiz üretim/bakım süreçlerinin yol açtığı bileşen kusurları kaynaklı risklere maruz bırakabilir.[67] Yapılan bir araştırmada katılımcıların %51'ine göre Çok Erişimli Uç Bilgi İşlem operatör stratejisinin önemli bir parçası olarak görülmekle birlikte, sadece %18'i uç noktalarını veya sınırlarını koruduklarını anlaşılmakta, bu da kurumsal saldırı yüzeyinin başka bir alanını saldırılara maruz bıraktıklarını göstermektedir.[68]

Sınır Bilişim'de; güvenlik, lisanslama ve yapılandırma zorluklarının bulunduğu bilinmektedir. Sınır Bilişim'in dağıtık mimarisi nedeniyle artan saldırı vektörleri bir güvenlik sorunsalıdır. Örneğin, bir sınır kullanıcının sahip

64 https://media.defense.gov/2021/May/10/2002637751/-1/-1/1/POTENTIAL%20THREAT%20VECTORS%20TO%205G%20INFRASTRUCTURE.PDF, erişim tarihi: 10 Temmuz 2022

65 https://www.karel.com.tr/blog/edge-computing-nedir-cloud-computing-ve-fog-computingden-farki-nedir#:~:text=Edge%20Computing%2C%20istemci%20verilerinin%20a%C4%9F%C4%B1n,ba%C4%9Fl%C4%B1 %20ayg%C4%B1tlar%C4%B1n%20say%C4%B1s%C4%B1%20taraf%C4%B1ndan%20y%C3%BCr%C3%BCt%C3%BCl%C3%BCr., erişim tarihi: 01 Temmuz 2022

66 https://www.karel.com.tr/blog/edge-computing-nedir-cloud-computing-ve-fog-computingden-farki-nedir#:~:text=Edge%20Computing%2C%20istemci%20verilerinin%20a%C4%9F%C4%B1n,ba%C4%9Fl%C4%B1%20ayg%C4%B1tlar%C4%B1n%20say%C4%B1s%C4%B1%20taraf%C4%B1ndan%20y%C3%BCr%C3%BCt%C3%BCl%C3%BCr., erişim tarihi: 01 Temmuz 2022

67 https://media.defense.gov/2021/May/10/2002637751/-1/-1/1/POTENTIAL%20THREAT%20VECTORS%20TO%205G%20INFRASTRUCTURE.PDF, erişim tarihi: 10 Temmuz 2022

68 https://www.trendmicro.com/en_us/research/21/g/with-5g-coming-its-time-to-plug-security-gaps.html, erişim tarihi: 07 Temmuz 2022

olduğu daha fazla istihbarat, o kullanıcının sisteminin zafiyeti durumunda kötücül yazılım sızmalarına karşı daha savunmasız kalır ve güvenlik açığı haline gelir. Bir sınır kullanıcının temel sürümü ilk satın alırken düşük bir fiyata mal etse bile, ilerleyen süreçte ihtiyaç duyacağı ek işlevlerin ayrı ayrı lisanslanmasının kullanım maliyetini artırma olasılığı bir lisanslama sorunsalı olarak ifade edilebilir. Ağa bağlı cihazların yönetiminde, sistem merkezi olmadığından her bir sınır aygıtındaki varsayılan parolayı değiştirememek veya yazılımı tutarlı bir şekilde güncelleştirmeyi ihmal etmek yöneticilerin güvenlik açıklarını yanlışlıkla oluşturması yapılandırma sorunsalı olarak tanımlanabilir.[69]

Çoklu Erişim Sınır Bilişimi mimarisi, geleneksel ağ yapılandırmalarının aksine, veri işleme ve depolama gibi temel trafik işlevlerini telekomünikasyon ağlarının uçlarında sunar. Bu sistemde; hipervizörler (hypervisors) [sanal makine monitörü (virtual machine monitor/VMM) olarak da bilinir ve sanal makineler (virtual machines/VM) oluşturan ve çalıştıran yazılımlara verilen isimdir.], işletim sistemleri ve uygulamalar gibi bileşenlerin varlığı, aynı zamanda kritik verileri ele geçirmek, işlemek ve yok etmek için ek saldırı vektörleri de yaratmaktadır. Bu sisteme eklemlenen güvenilir olmayan bileşenler veya kötücül yazılımlar; cihazların klonlanması ve yetkisiz arama yapılması, metin gönderilmesi ile veri kullanımı için son kullanıcıların taklit edilmesi imkânı sağlayarak kullanıcı gizliliğini olumsuz etkileyebilir. Bir şekilde sistemde eklenmiş güvenilir olmayan bileşenler veya kötücül yazılımlar üzerinden yetkisiz erişim sağlanan Çoklu Erişim Sınır Bilişimi ve son kullanıcı bileşenleri, daha geniş Radyo Erişim Ağına (radio access network/RAN) erişim sağlamak için de kullanılabilir. Örneğin; sisteme yetkisiz erişim sağlayan bir aktör, diğer kullanıcıların verilere erişimini engelleyebilir ve 5G teknolojisinin öngördüğü çok düşük gecikme süresini etkileyebilir. Ayrıca, söz konusu yetkisiz aktör tarafından bu suretle hassas sensör ve kullanıcı ekipmanı verilerini çalınabilir, veri akışları değiştirilebilir ve diğer kullanıcıların belirli verilere veya sensör akışlarına erişimi engellenerek ağın gizliliği, bütünlüğü ve kullanılabilirliği olumsuz etkilenebilir. Sonrasında da esasen yetkisiz olan bahse konu aktör RAN'a tam erişim elde etmek için bant genişliğine ulaşıp son kullanıcıların cihazları klonlanabilir.[70]

69 https://www.karel.com.tr/blog/edge-computing-nedir-cloud-computing-ve-fog-computingden-farki-nedir#:~:text=Edge%20Computing%2C%20istemci%20verilerinin%20a%C4%9F%C4%B1n,ba%C4%9Fl%C4%B1%20ayg%C4%B1tlar%C4%B1n%20say%C4%B1s%C4%B1%20taraf%C4%B1ndan%20y%C3%BCr%C3%BCt%C3%BCl%C3%BCr., erişim tarihi: 01 Temmuz 2022

70 https://media.defense.gov/2021/May/10/2002637751/-1/-1/1/POTENTIAL%20THREAT%20VECTORS%20TO%205G%20INFRASTRUCTURE.PDF, erişim tarihi: 10 Temmuz 2022

3.3. 5G Sistem Mimarisiyle İlgili Riskler

Artan veri, kapasite ve iletişim gereksinimlerini karşılamak için tasarlanan ve geliştirilen 5G sistem mimarileri, her ne kadar 5G bileşen üreticileri ve hizmet sağlayıcıları teknoloji iyileştirmeleri yoluyla güvenliği artırmaya çalışsa da hem eski hem de yeni güvenlik açıklarının varlığı istismara açık güvenlik açıklıkları barındırmaktadır. 5G'nin artan kapasitesiyle ağa daha çok sayıda ve potansiyel olarak daha az güvenli cihaz ekleme olanağı yaratan IoT'nin yayılmasındaki kolaylaştırıcılığı sayesinde sistemde artan bileşen çeşitliliğinin; 5G mimarisi içinde karmaşıklığa yol açma ve öngörülemeyen, genel sistem zayıflıkları veya güvenlik açıkları yaratma olasılığı bulunmaktadır.[71]

Önceki nesile ait iletişim altyapısıyla bütünleştirilmiş yeni nesil ağ sisteminin, eskinin sadece kullanılabilir teknolojisini değil sorunlarını, diğer bir deyişle eski nesil ağın istismara açık yönlerini de miras olarak devralacağı aşikârdır. İlaveten, yeni nesil kablosuz ağlarda kullanılmak üzere geliştirilen yeni bileşenler ve teknolojiler kullanılıp yayıldıkça sistemde yeni yeni zayıflıklar keşfedileceği de öngörülmektedir. Bununla birlikte, önceki nesil kablosuz ağlara göre daha fazla ve gittikçe artan sayıda BIT bileşeni kullanması öngörülen 5G ağlarının bu yapısının, sistem üzerinde işlem gören kritik verileri ele geçirmek, manipüle etmek, bozmak ve yok etmek için yeni vektörlerin ortaya çıkma ihtimalini artırdığı da değerlendirilmektedir. Yazılım Tanımlı Ağ İletişimi (SDN), Ağ Dilimleme (Network Slicing), Sınır Bilişim (Edge Computing) gibi 5G sistem mimarisine ilişkin yaklaşımlar, sistemin işlevselliğini ve güvenliğini artırmaya çabalarken aynı

71 https://media.defense.gov/2021/May/10/2002637751/-1/-1/1/POTENTIAL%20THREAT%20VECTORS%20TO%205G%20INFRASTRUCTURE.PDF, erişim tarihi: 10 Temmuz 2022

zamanda yapısal özellikleri nedeniyle artan bir saldırı zemini yaratma potansiyeli de taşımaktadır. 5G tehdit vektörlerine odaklı ve zayıflıkların erken tespit edilmesi yönünde çabalar süreklilik arz etmezse ağa bağlı cihazlar üzerinden kuruluşları ve kullanıcıları olumsuz yönde etkileme potansiyeli taşıyan ve 5G sistem mimarisiyle gelen söz konusu tehditler ve güvenlik açıkları istismar edildiğinde siber olayların etkisinin de artış göstermesi beklendik bir durumdur.[72]

72 https://media.defense.gov/2021/May/10/2002637751/-1/-1/1/POTENTIAL%20THREAT%20VECTORS%20TO%205G%20INFRASTRUCTURE.PDF, erişim tarihi: 10 Temmuz 2022

4.

5G Güvenlik Endişeleri

4. 5G Güvenlik Endişeleri

5G ağlarında güvenlik endişelerinin[73] bir kısmı ağın kendisinden kaynaklanırken diğer bir kısmı da ağa bağlanan cihazlardan kaynaklanmaktadır. 5G ağları hizmet sağlayıcılar ve kullanıcıları için hem hız hem de hacim bakımından kapasite artışı sağlarken aynı zamanda siber saldırganların eylem kapasitesinin de artışına neden olacaktır. Genişletilmiş 5G ağının kullanıcılara sağladığı faydaların aynı zamanda bu ağ yapısının ve bağlılarının siber güvenliğine zarar verme olasılığı da bulunmaktadır. Bu bağlamda, siber saldırıların giderek yaygınlaşmasının ve artmasının yarattığı riskli ortam nedeniyle 5G ağlarında siber güvenliğin sağlanması için önemli iyileştirmeler yapılması ihtiyacını da doğurmaktadır. Bu doğrultuda 5G teknolojisine yönelik başlıca siber güvenlik endişeleri şu şekilde özetlenebilir:[74]

4.1. Merkezi Olmayan Güvenliğin Olası Olumsuz Etkileri

5G ağlarının dinamik yazılım tabanlı sistemlerinin çok daha fazla trafik yönlendirme noktasına sahip olması güvenlik kontrollerini ve izlemeyi zorlaştırdığından

73 https://www.kaspersky.com/resource-center/threats/5g-pros-and-cons, erişim tarihi: 01 Temmuz 2022

74 https://www.kaspersky.com/resource-center/threats/5g-pros-and-cons, erişim tarihi: 01 Temmuz

güvenli olmayan alanların ortaya çıkması ağın geri kalan bölümlerini tehlikeye atması da muhtemeldir.[75]

4.2. Artan Bant Genişliğinin Mevcut Güvenlik Denetimlerini Zorlaştırması

5G teknolojisinin mümkün kıldığı daha fazla bant genişliği veri trafiğinde artan hız ve hacim, servis sağlayıcıların güvenliği gerçek zamanlı olarak güvenlik izlemesini olumsuz etkilemesi ve güvenliğin sağlanması için yeni yöntemler geliştirilmesi ihtiyacını artırması beklenmektedir.[76]

4.3. Nesnelerin İnterneti (Iot) Cihazlarının Üretim Kaynaklı Güvenlik Eksiklikleri

5G teknolojisi daha fazla cihazın ağa bağlanması anlamına geldiğinden, söz konusu ağlara bağlı çok farklı IoT cihazları (buzdolapları, akıllı televizyonlar, kapı kilitleri, hoparlörler vs.) için genel geçer güvenlik standartlarının olmaması nedeniyle farklı güvenlik seviyelerinde üretilen bu cihazların içinde siber güvenlik eksikliği olanların ağın tamamı için bir risk yaratması da beklendiktir. Farklı güvenlik seviyelerindeki milyarlarca cihaz, ağ zayıflığına yol açan milyarlarca olası ihlal noktası yaratarak ağ ihlallerinin ve siber saldırıların artmasına neden olabilir.[77]

4.4. Bağlantı Kurarken İlk Aşamadaki Şifreleme Eksikliği Kaynaklı Muhtemel Zafiyet

Bağlantı sürecinin başındaki şifreleme eksikliği ağa bağlı cihaz bilgilerini açığa çıkaracağından, söz konusu cihazlara yönelik siber saldırılarda saldırganların, ağa hangi cihazların bağlı olduğunu ve bu cihazların türü ve işletim sistemi gibi ayrıntıları öğrenmelerine ve bu ayrıntılardan hareketle de o cihazların zafiyetlerini istismar ederek saldırılarını daha hassas bir şekilde planlayıp gerçekleştirmelerine imkân tanıması beklendiktir. 5G ağındaki siber güvenlik açıkları çok çeşitli siber saldırılar için istismar edilebilmekle birlikte, en temel siber tehditler olarak Botnet, Dağıtık Hizmet Engelleme (Distributed Denial-of-Service/DDoS) ve Ortadaki Adam (Man-in-the-Middle/MiTM) saldırıları ile konum izleme ve çağrı durdurma/dinlemeye maruz kalınabilir.[78]

75 https://www.kaspersky.com/resource-center/threats/5g-pros-and-cons, erişim tarihi: 01 Temmuz 2022

76 https://www.kaspersky.com/resource-center/threats/5g-pros-and-cons, erişim tarihi: 01 Temmuz 2022

77 https://www.kaspersky.com/resource-center/threats/5g-pros-and-cons, erişim tarihi: 01 Temmuz 2022

78 https://www.kaspersky.com/resource-center/threats/5g-pros-and-cons, erişim tarihi: 01 Temmuz 2022

JANDARMA VE SAHİL GÜVENLİK AKADEMİSİ
İÇİŞLERİ BAKANLIĞI
1904

5.

Ağ Koruması ve Denetim

5. Ağ Koruması ve Denetimi

5.1. 5G'de Siber Güvenlik için Sağlanması Gereken Temel Şartlar[79]

5.1.1. Ağlarda 5G Güvenlik Temellerinin Oluşturulması

Veri merkezli bir kurumsal ağ örüntüsü olarak 5G sisteminin BT'de önemli değişiklikler yaratacağı ve IoT'ye sahip işletmeler için bünyelerine tamamen yeni yönetim varlıkları katacağı beklentisiyle, "bağlantılı" bir dünyada gerçekleşen bilgi alışverişinde yeni teknolojilerin geliştiricilerini/dağıtıcılarını ve bunların son kullanıcılarını koruyarak siber ortamda güvenliği sağlamak daha da fazla önem kazanmaktadır. Bu bağlamda, özel 5G bağlantısından beklenen faydayı sağlayabilmek için sistemin kullanıcısı kuruluşlar/işletmeler; bulutta yerel uygulamalar, sanallaştırma gibi teknolojik yenileşimler ve bunlara karşılık gelen güvenlik isteklerini karşılamak için yerleşik bir alım ve uyumlandırma sürecine de sahip olmalıdır.80 Teknolojik anlamda yeni bir gerçekliğe geçiş yaparken 5G teknolojisi altyapısının ve bileşenlerinin kullanıma sunumu hız kazandıkça ve kullanım modellemeleri geliştirildikçe, bekle gör tarzında veya tepkisel bir yaklaşım yeni nesil kablosuz ağların ve bunlara bağlı cihazların güvenliğinin sağlanması açısından uygun bir güvenlik anlayışı olmadığı değerlendirilmektedir. Bu bağlamda proaktif, diğer bir deyişle ön alıcı yaklaşım sergilenmesinin, sürdürülebilirlik ve sistemin kullanıcılarının beklentilerinin karşılanması bakımından daha uygun bir güvenlik yönetimi anlayışı olacağı düşünülmektedir. Her ne kadar 5G sistem mimarisinin, geliştirme sürecinin başlangıcından itibaren güvenlik ön planda tutularak tasarlanmış olduğu ileri sürülmekte olsa da tamamen güvenli olmadığı da bilinmektedir. Bu çerçevede, söz konusu mimaride ideal bir siber güvenlik çözümü, tüm kurumsal ağlarda uçtan uca güvenlik isteğini karşılamayı hedeflemektedir.81 Teknoloji geliştiricilerinin, bahse konu yeni gerçeklik ortamında ulusal mobil ağlardaki yaygın zayıflıkları gidermek üzere 5G sisteminin güvenliğini sağlamak için öncelik vermesi gerekmektedir. Bu bağlamda, evvela ağlarda 5G güvenlik temellerinin saptanması bir gereklilik olarak ortaya çıkmaktadır. Bu minvalde, ağ işleticilerinin; 5G sisteminin taşıdığı kendine has riskleri karşılamak için yazılım merkezli koruma yöntemlerine odaklanmaya başlayacakları ve şifreleme çözümleri, ağ izleme, vesair işlemi geliştirmek için gayret göstermeleri gerekeceği öngörülmektedir.[82]

79 https://www.kaspersky.com/resource-center/threats/5g-pros-and-cons, erişim tarihi: 01 Temmuz 2022

80 https://www.trendmicro.com/en_us/business/solutions/iot/enterprise-5g-iot.html, erişim tarihi: 07 Temmuz 2022

81 https://www.trendmicro.com/en_us/business/solutions/iot/enterprise-5g-iot.html, erişim tarihi: 07 Temmuz 2022

82 https://www.kaspersky.com/resource-center/threats/5g-pros-and-cons, erişim tarihi: 01 Temmuz 2022

Kaynak: Trend Micro
*https://www.trendmicro.com/en_us/business/solutions/iot/enterprise-5g-iot.html

Şekil 1: Kurumsal 5G'de Uçtan Uca Güvenlik

5.1.2. Üreticilerin Güvenlik Çabalarını Artırmak İçin Teşvik Edilmesi

5G sisteminin güvenliğini değerlendirirken, bu yapının; yalnızca bağlı cihazların oluşturduğu zincirin en zayıf halkası kadar güçlü olduğunu unutmamak gerekir. Ticarî rekabet ortamında, özellikle tüketicilerin satın alırken göz önünde bulundurduğu kıstaslar arasında kaliteyi daha geri planda tutabildiği ürünler bağlamında, aynı tür ürünü üreten diğer rakip firmalara göre piyasadaki en ucuz ürünü sağlama motivasyonu düşünüldüğünde, üreticiler açısından güvenli teknoloji geliştirme ve uygulama maliyetleri; üretim süreçlerinde dikkate alınan kriterler sıralamasında, ağa bağlanacak bileşenlerin güvenlik özellikleri ve tüketicinin dijital korunması aleyhine, daha öncelikli olacağı değerlendirilmektedir. Bu bağlamda, kar maksimizasyonu odaklı bir serbest piyasa mekanizmasında, 5G sistemine eklemlenmek üzere üretilen ağ bileşenlerinin üreticilerinin, güvenlikli bir siber ortam oluşturma yönünde göstermeleri beklenen çabayı artırmak maksadıyla, motive edilmeleri de bir gereklilik olarak önümüze çıkmaktadır. Bunun da üreticiler için güvenli teknoloji geliştirmeyi bir kıstas olarak önceleyecek ekonomik faydalar sağlamaktan geçeceği düşünülmektedir.[83]

83 https://www.kaspersky.com/resource-center/threats/5g-pros-and-cons, erişim tarihi: 01 Temmuz 2022

5.1.3. Nesnelerin İnterneti (IoT) Siber Güvenliği Hakkında Tüketici Farkındalığının Artırılması

Güvenlikle ilişkili tüm tedbirlerde olduğu gibi farkındalık yaratmak IoT siber güvenliği bakımından da hayatî bir konumdadır. Ne tedbir alınırsa alınsın, kurulan sistemlerin en nihayetinde insanların kullanımına sunulacağı ve onların güvenlik tedbirlerini zafiyete uğratacak bilinçli veya bilinçsiz tutumlarının siber ekosistemde yaşayan tüm varlıkları bir şekilde olumsuz etkileyeceği değerlendirilmektedir. Bu nedenle IoT'de siber güvenlik konusunda tüketicilerin farkındalıklarını artırıcı eğitimler verilmesi önem arz etmektedir. Kullanıcıların, güvenlik kalitesi uygun ürünler kullanmaları ve ağa bağlı tüm cihazlarının yazılım güncellemelerinin doğru ve zamanında yapılmasının önemi hakkında bilinçlendirilmesi de faydalıdır. Bileşen üreticilerinin piyasaya sunduğu cihazlar bakımından güvenlik kalitesindeki geniş çeşitlilik arz etmektedir. Bu çeşitlilik nedeniyle; hâlihazırda sıradan kullanıcıların talip oldukları IoT cihazlarının ne kadar güvenli olduğunu kolayca anlayabilmeleri pek de mümkün olmadığından, akıllı teknolojilerin üreticilerinin bu zafiyeti giderecek güvenlik tanımlaması içeren standart bir etiket sistemi kullanmaktan sorumlu tutulabileceği değerlendirilmektedir. Güvenli olması için tasarlanan 5G sisteminin devreye alınması bunun için geliştirilen güvenliği artırma çabalarıyla da eş zamanlı yürümektedir. Ancak her teknolojide olduğu gibi yeni güvenlik zafiyetleri hem cihazların hem de kullanıcıların birbirleriyle etkileşimi sonucu ortaya çıkabilmektedir. Bu bağlamda, 5G sisteminde tasarlanan tedbirleri/korumaları iyileştirmek için gerçek dünyadan uygulama sonuçlarına ihtiyaç duyulduğundan, 5G devreye alındıktan çok sonra da daha güvenlikli bir ortam yaratma yönünde çalışmaların devam etmesi beklendik bir durumdur.[84]

Bu çalışmada ortaya konan anlatı bağlamında peki o zaman kullanıcılar olarak 5G teknolojisine nasıl hazırlanmalıyız? sorusu da cevaplanması gereken husus olarak gündeme gelmektedir. Mevcut durumda bazı alanlarda teknolojik yükseltmelerin ortaya çıkmaya başladığının gözlemlenmesine rağmen, 5G'nin küresel ölçekte ve tüm sektörlerde tam anlamıyla kullanıma sunulmasının sanılandan daha uzun bir zaman alabileceği öngörülmektedir. Ancak, her hâlükârda hazırlıksız yakalanmamak önemlidir. Bu çalışmada betimlenen dijital ortamda kullanıcıların kendi kişisel

84 https://www.kaspersky.com/resource-center/threats/5g-pros-and-cons, erişim tarihi: 01 Temmuz 2022

güvenliğini ve gizliliğini mümkün olduğunca kendi inisiyatifinde tutmak için ihtiyatlı olmaları gerektiği değerlendirilmektedir. Bu bağlamda pek çok tedbirin yanı sıra aşağıda bahsedilen çözümlerden de faydalanılabilir:[85]

5.1.3.1. Anti-Virüs Çözümü Kullanımı

Bilgisayar sistemlerinde kötücül yazılımların tespit edilmesine, engellenmesine ve işlevsizleştirilmesine yönelik üretilmiş bilgisayar programları olarak tanımlanan anti-virüs yazılımları,[86] temel olarak tarama (scanning), temizleme (cleaning), kurtarma (recovery) ve koruma (protection) gibi işlevler görmektedir.[87] Bu bağlamda tüm bilgi işlem özellikli cihazlarınıza bir anti-virüs çözümü yüklemek, sınırlılıklarıyla birlikte önleyici bir tedbir olarak virüs bulaşını engelleme çabasında bir ölçüde yardımcı olacaktır.[88] Ancak, kökset (rootkit) ve ön yükleme seti (bootkit) saldırılarının da varlığı düşünüldüğünde, anti-virüs yazılımlarının yanında, casus yazılım önleme yazılımları (antispyware) için bile belli zorluklar bulunmaktadır. Bütün bu tedbirler bir bütün olarak düşünüldüğünde, anti-virüs yazılımlarını sistemde yüklü ve güncel bulundurulmasının ve programların uyarılarının dikkate alınarak görü-

85 https://www.kaspersky.com/resource-center/threats/5g-pros-and-cons, erişim tarihi: 01 Temmuz 2022

86 https://bitdefender.com.tr/antivirus-nedir/, erişim tarihi: 07 Temmuz 2022

87 https://veb.com.tr/kurumsal-antivirus-cozumleri/urun/29-kurumsal-antivirus-cozumleri.html, erişim tarihi: 07 Temmuz 2022

88 https://www.kaspersky.com/resource-center/threats/5g-pros-and-cons, erişim tarihi: 01 Temmuz 2022

nüşte zararsız olan bir dosyanın bile kaynağı doğrulanamıyorsa bilinçsizce açılması yerinde bir davranış olarak değerlendirilmektedir.

5.1.3.2. Sanal Özel Ağ (Virtual Private Network/VPN) Kullanımı

Sanal Özel Ağ (Virtual Private Network/VPN), kullanıcıyı fiziksel olarak bulunmadığı bir yerdeki fiziksel bir ağa, örneğin bir şirketin yerel ağına, sanki oradaymış gibi uzaktan bağlayan bir teknoloji olarak tanımlanabilir. Ancak VPN; kullanıcıların ülkede erişim kısıtlaması uygulanan internet sitelerine, diğer bir deyişle yasaklı sitelere, girmek için kullanabildiği Opera Tarayıcısı çalıştırmak, Google Translate'den yararlanmak veya DNS değiştirmek gibi birçok farklı yöntem arasında başvurduğu bir çözüm olarak da bilinmektedir. VPN çözümleri; bilgi işlem cihazına kurulu özelleşmiş bir ağ sürücüsü vasıtasıyla sanal bir ağ bağdaştırıcısı gibi davranarak hedef ağdan bir IP numarası alıp o ağda izin verilen uygulamalara veya yerel adreslere erişim imkânı tanımaktadır. Esasen VPN, kullanıcının bilgisayarının fiziksel

olarak bulunduğu yerden hedef ağa yeterli bir güvenlik seviyesi kullanılması durumunda içinden geçen veri trafiğinin içeriğinin dışarıdan okunmasını engelleyen şifreli (kriptolu) bir bağlantı tüneli açmaktadır.[89] Kullanıcının, dış aktörlerin kendi verilerine izinsiz olarak erişmesini ve çevrimiçi etkinliğini gözetlemesini engellemek için bir VPN çözümü kullanması veri güvenliği açısından uygun bir davranış olarak değerlendirilmektedir.[90]

5.1.3.3. Parola Güvenliği Çözümleri

Kullanıcıların sistem üzerindeki hesaplarına erişim için parola kullanımı ve parolaların güçlü hale getirilmesi önem arz etmektedir. Ancak, kullanıcıların tahmin edilmesi zor parolalar üretebilmesini engellediği savıyla harf, sayı ve özel karakter kombinasyonuyla karmaşık parola oluşturulmasını şart koşmanın artık tek başına bir güvenlik tedbiri olarak görülmediği ileri sürülmektedir. Kullanıcının belirli sürelerde parolasını yenilemesine, diğer bir deyişle periyodik şifre değişimine, yönelik uygulamanın şifre güvenliğini güçlendirmekten ziyade kötüleştirdiği de iddia edilmektedir. Bu doğrultuda, the National Institute of Standards and Technology'nin

89 https://www.karel.com.tr/blog/5-soruda-vpn-nedir-nasil-calisir, erişim tarihi: 07 Temmuz 2022

90 https://www.kaspersky.com/resource-center/threats/5g-pros-and-cons, erişim tarihi: 01 Temmuz 2022

(ABD Ulusal Standartlar ve Teknoloji Enstitüsü/NIST) yayınladığı bir raporda periyodik şifre değişimi kuralının kaldırılmasının önerildiği bilinmektedir. Bunun yerine, yeni oluşturulan parolaların; zorunlu olarak çok sık kullanılan, kolay tahmin edilebilen veya çalınmış parolalardan oluşan bir listeyle karşılaştırılması suretiyle şifre geçerliliğinin denetlenmesi önerilmektedir. Ayrıca, iki faktörlü kimlik doğrulaması (two-factor authentication/2FA) ve çok faktörlü kimlik doğrulaması (multi factor authentication/MFA) parola güvenliğinde kullanılan teknolojiler olarak öne çıkmaktadır. İki faktörlü kimlik doğrulaması; kullanıcının, hem parolasını hem de şifrematiğini/akıllı telefonunu kullanılıp kimliğinin doğrulanarak sisteme giriş yapmasına dayanan iki aşamalı bir süreç olarak tasarlanmıştır. Bu süreçte, kullanıcının ilk doğrulama aşamasında kendisi tarafından belirlenmiş olan parolasını girdikten sonra ikinci doğrulama aşamasında ya kendisine tahsisi edilen şifrematik tarafından üretilen ya da sisteme tanımlı numarası üzerinden akıllı telefonuna gönderilen tek kullanımlık doğrulama kodunu girmesi istenmektedir. Çok faktörlü kimlik doğrulaması ise iki faktörlü kimlik doğrulamasında kullanılan parola ile şifrematik/akıllı cep telefonu donanımı üzerinden tek kullanımlık şifre gibi uygulamalara ek olarak parmak izi ve iris tarama gibi biyometrik veriler de kullanılmaktadır.[91] Ancak, sisteme giriş için akıllı cep telefonu üzerinden alınan bir kodun kimlik doğrulama için kullanması açısından, SS7 ağı üzerinden kullanıcının cep telefonuna gitmesi gereken SMS trafiğini başka bir numaraya yönlendirebilmesinin mümkün olması nedeniyle, SS7'nin diğer açıklarının yanında ağ iletişiminde güvenlik için potansiyel bir zafiyet alanı oluşturduğu da bilinmektedir.[92] Bu nedenle, kullanılan parola güvenliği çözümlerinin potansiyel güvenlik açıklarının da farkında olmak önem arz etmektedir. Kullanıcılar açısından tüm IoT cihazlarının "yönetici/şifre" ("admin/password") tarzı kimlik bilgilerinin ve bu bağlamda, veri tabanı yazılımının işleyişini tanımlayan arka uç (backend) şifrelerinin fabrika çıkışı varsayılan durumdan farklılaştırılarak güncellenmesi önerilmektedir.[93] En nihayetinde, güçlü parola güvenliği uygulanması veri güvenliği açısından uygun bir davranış olarak değerlendirilmektedir.[94]

91 https://www.beyaz.net/tr/guvenlik/makaleler/sifre_guvenligi.html, erişim tarihi: 07 Temmuz 2022

92 https://arkakapidergi.com/ss7-protokolu-ve-gsm-aglarindaki-potansiyel-tehlikeler/

93 https://www.kaspersky.com/resource-center/threats/5g-pros-and-cons, erişim tarihi: 01 Temmuz 2022

94 https://www.kaspersky.com/resource-center/threats/5g-pros-and-cons, erişim tarihi: 01 Temmuz 2022

5.1.3.4. Güncel Güvenlik Yamalarının Uygulanması

Kullanıcılar tarafından tüm IoT cihazlarının (Ağa bağlanan kişisel bilgisayarlar, akıllı cep telefonları, akıllı ev aletleri, arabaların bilgi-eğlence sistemleri dâhil) güvenlik yamalarının uygulanarak güncel halde tutulması da bir önem arz etmektedir. İnternet, Bluetooth veya diğer kablosuz veri iletim kanallarına bağlanan tüm cihazlar için (uygulamalar, işletim sistemi vb.) güvenilir kabul edilen üreticilerin yayımladığı en son güncellemelerin yapılması veri güvenliği açısından uygun bir davranış olarak değerlendirilmektedir.[95]

5.1.3.5. Sıfır Güven Ağ Erişimi (Zero-Trust Network Access) Çözümleri

Sıfır Güven Ağ Erişimi (Zero-Trust Network Access) uygulamasında, kurum içindeki uygulamalara erişimi güvenli hale getirmek için öncelikle kullanıcılar kurumdaki ağ erişiminden, uygulamalar da internetten yalıtılmaktadır. Bu uygulamada, esasen, tüm uygulamaların kurumsal ağa bağlanması ve internete açılması yerine, yalnızca kullanılan uygulamaların genel ağ trafiğinden yalıtılmış bir ortamda birbirleriyle iletişim kurması sağlanmaktadır. Böylelikle, kullanıcıların; genel ağa maruz bırakılmaksızın, kurum içinde kullanılan uygulamalara güvenli ve kesintisiz bir şekilde bağlanması sağlanmaktadır. Sıfır Güven Ağ Erişimi uygulaması; bir kurumun ağ cihazlarına ait IP adreslerinin internete maruz kalmasını önlemekte ve sadece "giden" bağlantılar kurmak suretiyle, uygulama ve ağ altyapısının yetkisiz kullanıcılara görünmez olmasını sağlamaktadır. Ayrıca, Sıfır Güven Ağ Erişimi uygulamasında, ayrıntılı uygulama erişim politikaları kullanılarak, kullanıcıların kurum ağına tam erişim sağlaması yerine yalnızca yetkilendirildikleri uygulamalara bire bir erişimine imkân tanınmakta, kullanıcı faaliyetleri de gerçek zamanlı olarak denetlenebilmektedir. Sonuç olarak, Sıfır Güven Ağ Erişimi, dış aktörlerin kurum ağına asla erişememesini ve yalnızca yetkili kullanıcıların izin verilen uygulamalara erişebilmesini sağlayarak güvenliği ihlal edilmiş cihazların kurum ağında oluşturabileceği riskler minimize edilmeye, üçüncü taraf kullanıcı zafiyetleri de kontrol altına alınmaya çalışılmaktadır.[96]

95 https://www.kaspersky.com/resource-center/threats/5g-pros-and-cons, erişim tarihi: 01 Temmuz 2022

96 https://cyberartspro.com/sifir-guven-ag-erisimi-zero-trust-network-access/, erişim tarihi: 04 Temmuz 2022

SONUÇ

SONUÇ

Bilgisayar kullanıcılarının küresel anlamda artan internet erişimi ve ağ tabanlı etkileşimi; olumlu yönleriyle birlikte, siber kaynakların siber suçlar ve diğer kötücül kullanımlarla istismar potansiyeli de göz önünde bulundurulduğunda, nispeten mesafenin önemsizleştiği ve sınırların bulanıklaştığı artan tehdit ortamının bir işaretçisi ve internet ortamını kullanan toplumun büyük kesiminin risk altında olması anlamına da gelmektedir.[97]

"Doğrudan ya da dolaylı olarak internete, elektronik haberleşme ve bilgisayar ağlarına bağlı olan tüm sistem ve hizmetler" olarak tanımlanan siber uzayda güvenlik alanına yönelik faaliyetler Türkiye'de yürürlükte bulunan "Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023" belgesi çerçevesinde sürdürülmektedir.[98] 2020-2023 dönemi için "ülke ekonomisinin geliştirilmesini, toplumsal yaşamın korunmasını ve milli güvenliğin sağlanmasını desteklemek için; ülkemizde güvenli biçimde işleyen bir siber ortama sahip olmak ve siber güvenlikte uluslararası alanda marka haline gelmek" şeklinde ifade edilen 2023 vizyonunun gerçekleşmesi ve bunun sonrasına güvenle yol alınması amacıyla belirlenen stratejik amaçlar arasında "Yeni Nesil Teknolojilerin Güvenliği" de yer almaktadır. Küresel gelişmelere koşut Türkiye'de de birçok uygulamayla birlikte, toplumsal hayatın merkezinde yer edinmeye başlayan yeni nesil teknolojilerden nesnelerin interneti, bulut bilişim ve yakın zamanda hayata geçmesi beklenen 5G gibi teknolojilerin güvenli kullanımının sürdürülebilir ulusal ekonomik kalkınmayı destekleyecek unsurlar arasında görüldüğü 2020-2023 strateji belgesinde açıkça belirtilmektedir.[99]

Verilerin üretilmesinin yanı sıra nasıl değerlendirildiği de önem taşımaktadır. 5G teknolojisiyle artan bağlantı hızıyla birlikte artan veri trafiği hacmi içerisinde, doğru verinin doğru zamanda doğru yere güvenli bir biçimde iletilebilmesinde 5G kablosuz ağ bağlantısı altyapısı ve bileşenlerine ilişkin sektörlere özgü belli standartların geliştirilmesinin, faydalı bilginin üretilmesi ve güvenli kullanım kapasitesinin artırılması için önemli olduğu değerlendirilmektedir. Bu bakımdan siber

97 http://www.tid.web.tr/kurumlar/tid.web.tr/isd/203/alperbilgic.pdf, erişim tarihi: 04 Temmuz 2022

98 https://hgm.uab.gov.tr//uploads/pages/siber-guvenlik/ulusal-siber-guvenlik-stratejisi-ep-2020-2023.pdf, erişim tarihi: 04 Temmuz 2022

99 https://hgm.uab.gov.tr//uploads/pages/siber-guvenlik/ulusal-siber-guvenlik-stratejisi-ep-2020-2023.pdf, erişim tarihi: 04 Temmuz 2022

güvenlik kavramı yeni teknolojiler bakımından ayrı bir önem kazanmaktadır. Bu bağlamda, siber tehditlerle mücadele ön alıcı bir yaklaşımı gerektirmektedir. Ancak hatırda tutulması gereken nokta şudur ki; siber tehditlerle mücadele topyekûn bir savaşım alanıdır. Bu nedenle, toplumdaki tüm kurum/kuruluşların yanı sıra tüm bireylerin de bu mücadelenin bir parçası haline getirilmesi gerekmektedir.[100] Sonuç olarak, bu anlayış çerçevesinde, 5G teknolojisi ve bunun altyapısına yönelik risklerin ve güvenlik açıklarının değerlendirilmesi için 5G'ye yönelik stratejilerin sektörel standartları da kapsayacak şekilde gözden geçirilmesi ve güncel tutulması önem kazanmaktadır.

Her zaman ve her yerde kullanılabilecek yüksek hız, artırılmış bant genişliği ve bilgiye düşük maliyetli erişim sağlayabilecek kablosuz ağlara yönelik küresel talep artış göstermektedir. Daha 5G'ye tam bir geçiş gerçekleşmemiş olmasına rağmen, 2030'lu yılların başlarında, yetenekleri henüz tam olarak ortaya konmamış ve uygulamasına ilişkin yeterli teknik ilerleme olgunlaşmamış olmakla birlikte, mobil kablosuz ağlarda altıncı nesil (6G) teknolojisine geçişle ilgili düşünceler dillendirilmekte hatta yedinci nesil (7G) ve ötesine geçişle ilgili öngörüler paylaşılmaktadır. Bu bağlamda, 6G kablosuz mobil iletişim ağlarında uyduların küresel kapsama sağlamak için kullanılması tasarlanmakta olduğu bilinmektedir. Kullanıcılara daha önce benzeri görülmemiş seviyede mobilite sağlaması beklenen ve uydu işlevleriyle daha gelişmiş 7G kablosuz mobil iletişim ağlarıyla da uzay dolaşımı (space roaming) elde edilmesi hedeflendiği anlaşılmaktadır. 7G'den sonraki teknolojinin de 7.5G veya 8G olarak adlandırılabileceği değerlendirilmektedir. Ancak, söz konusu teknolojilerin hayata geçirilebilmesi için gerekli protokollerin ve standartların geliştirilmesine ilişkin ortak bir anlayışın henüz bulunmadığı değerlendirilmektedir.[101]

Önemli bilgisayar korsanlığı (hacker) konferanslarından birisi olan ve her yıl Las Vegas, Nevada'da düzenlenen DEFCON'un 2022 yılında icra edilen toplantısında, Shadytel adlı grubun; faydalı ekonomik ömrünü tamamladığından daha uzak bir yörüngeye gönderilmeyi bekleyen, jeostatik yörüngedeki (yer sabit yörüngedeki) hizmet dışı bırakılmış Anik F1R uydusunun kontrolünü 300 $'lik yazılım ta-

100 http://www.tid.web.tr/kurumlar/tid.web.tr/isd/203/alperbilgic.pdf, erişim tarihi: 04 Temmuz 2022

101 https://ijstm.inarah.co.id/index.php/ijstm/article/view/379/344, erişim tarihi: 16 Eylül 2022

nımlı telsiz yayın donanımı olan HackRF kullanarak "onunla biraz eğlenmek için" ele geçirmeyi ve onu 2021 yılında San Diego'da icra edilen ToorCon bilgisayar korsanlığı konferansının konuşmaları ile WarGames gibi klasik bilgisayar korsanı filmlerini yayınlamak için kullandıklarını açıklamıştır.[102] Bu durumda uyduya dayalı iletişim ağları da dahil olmak üzere mesafenin önemsizleştiği siber ortamda güvenlikleştirmenin kazandığı önem bir kez daha vurgulanmalıdır.

102 https://www.vice.com/en/article/y3pwqx/hackers-took-over-a-commercial-satellite-to-broadcast-hacker-movies, erişim tarihi: 16 Eylül 2022

JANDARMA VE SAHİL GÜVENLİK AKADEMİSİ
İÇİŞLERİ BAKANLIĞI
1904

KAYNAKÇA

ABD Savunma Bakanlığı (2021). Potential Threat Vectors to 5G Infrastructure. https://media.defense.gov/2021/May/10/2002637751/-1/-1/1/POTENTIAL%20THREAT%20VECTORS%20TO%205G%20INFRASTRUCTURE.PDF adresinden 10 Temmuz 2022 tarihinde alınmıştır.

BeyazNet (2022). Şifre Güvenliği. https://www.beyaz.net/tr/guvenlik/makaleler/sifre_guvenligi.html adresinden 07 Temmuz 2022 tarihinde alınmıştır.

Bilgiç, A. (2021). Siber Vatan ve Siber Güvenlik: Siber Tehditlerle Mücadele Örgütlenmesinde Türkiye Örneği. http://www.tid.web.tr/kurumlar/tid.web.tr/isd/203/alperbilgic.pdf adresinden 04 Temmuz 2022 tarihinde alınmıştır.

Bitdefender (2022). Antivirüs Nedir?. https://bitdefender.com.tr/antivirus-nedir/ adresinden 07 Temmuz 2022 tarihinde alınmıştır.

Cabrera, E. (2021). With 5G coming, it's time to plug security gaps. https://www.trendmicro.com/en_us/research/21/g/with-5g-coming-its-time-to-plug-security-gaps.html, erişim tarihi: 07 Temmuz 2022 tarihinde alınmıştır.

CNBC LLC. (2022). Verizon, AT&T agree to delay some 5G deployment until mid-2023. https://www.cnbc.com/2022/06/17/verizon-att-agree-to-delay-some-5g-deployment-until-mid-2023.html adresinden 01 Temmuz 2022 tarihinde alınmıştır.

CyberArts Bilişim A.Ş. (2022). Sıfır Güven Ağ Erişimi (Zero-Trust Network Access). https://cyberartspro.com/sifir-guven-ag-erisimi-zero-trust-network-access/ adresinden 04 Temmuz 2022 tarihinde alınmıştır.

Demirel, F. (2013). GSMA Intelligence: Dünyanın mobil sektör bilgileri tek çatı altında. https://webrazzi.com/2013/06/14/gsma-intelligence/ adresinden 01 Temmuz 2022 tarihinde alınmıştır.

e-Dönüşüm Türkiye Projesi: Birlikte Çalışabilirlik Esasları Rehberi Sürüm 2.1. (2012). http://www.bilgitoplumu.gov.tr/wp-content/uploads/2014/04/Birlikte_Calisabilirlik_Esaslari_Rehberi_2.1.pdf adresinden 10 Temmuz 2022 tarihinde alınmıştır.

Ergin, Y. (2016). SDN ve NFV Nedir? Aralarındaki Farklar Nelerdir?. https://www.karel.com.tr/blog/sdn-ve-nfv-nedir-aralarindaki-farklar-nelerdir adresinden 10 Temmuz 2022 tarihinde alınmıştır.

Franceschı-Bıcchıeraı, L. (2022). Hackers Took Over a Commercial Satellite to Broadcast Hacker Movies. https://www.vice.com/en/article/y3pwqx/hackers-took-over-a-commercial-satellite-to-broadcast-hacker-movies adresinden 16 Eylül 2022 tarihinde alınmıştır.

Gtech (2021). Nesnelerin İnterneti (IoT) Nedir. https://www.gtech.com.tr/nesnelerin-interneti-iot-nedir/ adresinden 01 Temmuz 2022 tarihinde alınmıştır.

Haverans, R. (2021). From 1G to 5G: A Brief History of the Evolution of Mobile Standards. https://www.brainbridge.be/en/blog/1g-5g-brief-history-evolution-mobile-standards adresinden 01 Temmuz 2022 tarihinde alınmıştır.

IBM (2022). What is supply chain management?. https://www.ibm.com/topics/supply-chain-management adresinden 07 Temmuz 2022 tarihinde alınmıştır.

Karel (2015). 5 Soruda VPN Nedir, Nasıl Çalışır ve Nasıl Kurulur?. https://www.karel.com.tr/blog/5-soruda-vpn-nedir-nasil-calisir adresinden 07 Temmuz 2022 tarihinde alınmıştır.

Kaspersky (2022). Is 5G Technology Dangerous? - Pros and Cons of 5G Network. https://www.kaspersky.com/resource-center/threats/5g-pros-and-cons adresinden 01 Temmuz 2022 tarihinde alınmıştır.

Lynch, K. (2015). 1973: First Mobile Phone Call. https://www.guinnessworldrecords.com/news/60at60/2015/8/1973-first-mobile-phone-call-392969 adresinden 01 Temmuz 2022 tarihinde alınmıştır.

Opensignal Limited (2020). Turkey: Mobile Network Experience Report. https://www.opensignal.com/reports/2020/06/turkey/mobile-network-experience adresinden 01 Temmuz 2022 tarihinde alınmıştır.

Şişman, M. (2018). SS7 Protokolü ve Gsm Ağlarındaki Potansiyel Tehlikeler. https://arkakapidergi.com/ss7-protokolu-ve-gsm-aglarindaki-potansiyel-tehlikeler/ adresinden erişim tarihi: 07 Temmuz 2022 tarihinde alınmıştır.

T.C. Avrupa Birliği Bakanlığı Sosyal, Bölgesel ve Yenilikçi Politikalar Başkanlığı (2018). Sanayi 4.0 Bilgi Notu. https://www.ab.gov.tr/siteimages/resimler/Sanayi%204_0%20web.pdf adresinden 01 Temmuz 2022 tarihinde alınmıştır.

T.C. Çevre ve Şehircilik Bakanlığı (2019). 2020-2023 Ulusal Akıllı Şehirler Stratejisi ve Eylem Planı. https://www.akillisehirler.gov.tr/wp-content/uploads/EylemPlani.pdf adresinden 01 Temmuz 2022 tarihinde alınmıştır.

T.C. Ulaştırma ve Altyapı Bakanlığı (2019). Ulusal Siber Güvenlik Stratejisi ve Eylem Planı: 2020-2023. https://hgm.uab.gov.tr//uploads/pages/siber-guvenlik/ulusal-siber-guvenlik-stratejisi-ep-2020-2023.pdf adresinden 04 Temmuz 2022 tarihinde alınmıştır.

Trend Micro Incorporated (2021). 5G Security for Enterprises: Security platform for end-to-end enterprise connectivity. https://www.trendmicro.com/en_us/business/solutions/iot/enterprise-5g-iot.html adresinden 07 Temmuz 2022 tarihinde alınmıştır.

TÜSİAD (2016). Türkiye'nin Küresel Rekabetçiliği İçin Bir Gereklilik Olarak Sanayi 4.0: Gelişmekte Olan Ekonomi Perspektifi. https://tusiad.org/tr/yayinlar/raporlar/item/download/7494_67a3aa94bcfce900229f42280fa1ba68 adresinden 01 Temmuz 2022 tarihinde alınmıştır.

Vaıgandla, K.k., Azmı, N., Ramya, P., & Karne, R. (2021). A Survey On Wireless Communications: 6G and 7G. International Journal of Science, Technology & Management, 2(6), 2018-2025. https://ijstm.inarah.co.id/index.php/ijstm/article/view/379/344 adresinden 16 Eylül 2022 tarihinde alınmıştır.

Veb Bilgi İşlem Otomasyon (2018). Kurumsal Antivirüs Çözümleri. https://veb.com.tr/kurumsal-antivirus-cozumleri/urun/29-kurumsal-antivirus-cozumleri.html adresinden 07 Temmuz 2022 tarihinde alınmıştır.

Yetimler, E. (2022). Edge Computing Nedir? Cloud Computing ve Fog Computing'den Farkı Nedir? https://www.karel.com.tr/blog/edge-computing-nedir-cloud-computing-ve-fog-computingden-farki-nedir#:~:text=Edge%20Computing%2C%20istemci%20verilerinin%20a%C4%9F%C4%B1n,ba%C4%9Fl%C4%B1%20ayg%C4%B1tlar%C4%B1n%20say%C4%B1s%C4%B1%20taraf%C4%B1ndan%20y%C3%BCr%C3%BCt%C3%BCl%C3%BCr. adresinden 01 Temmuz 2022 tarihinde alınmıştır.

NOTLAR

NOTLAR

NOTLAR

jsgaedutr

www.jsga.edu.tr