

İSTANBUL BİLGİ ÜNİVERSİTESİ
LİSANSÜSTÜ PROGRAMLAR ENSTİTÜSÜ
BİLİŞİM VE TEKNOLOJİ HUKUKU YÜKSEK LİSANS PROGRAMI

ELEKTRİK PİYASASINDA SİBER GÜVENLİK DÜZENLEMELERİ VE
HUKUKİ SORUMLULUK

Esra EYCEOĞLU
119691015

Dr. Öğr. Üyesi Tayfun ACARER

İSTANBUL
2024

Elektrik Piyasasında Siber Güvenlik Düzenlemeleri ve Hukuki Sorumluluk
Cybersecurity Regulation in Electricity Market and Legal Liability

Esra EYCEOĞLU
119691015

Tez Danışmanı : Dr. Öğr. Üyesi Tayfun ACARER
Piri Reis Üniversitesi

Jüri Üyeleri : Prof. Dr. Leyla KESER BERBER
İstanbul Bilgi Üniversitesi

Doç. Dr. Mehmet Bedii KAYA
İstanbul Bilgi Üniversitesi

Tezin Onaylandığı Tarih : 26.04.2024

Toplam Sayfa Sayısı : 187

Anahtar Kelimeler (Türkçe)

- 1) Siber Güvenlik
- 2) Bilgi Güvenliği
- 3) Elektrik Piyasası
- 4) Hukuki Sorumluluk
- 5) Kritik Altyapı

Anahtar Kelimeler (İngilizce)

- 1) Cybersecurity
- 2) Information Security
- 3) Electricity Market
- 4) Legal Liability
- 5) Critical Infrastructure.

İÇİNDEKİLER

İÇİNDEKİLER	iii
KISALTMALAR	v
TABLO LİSTESİ	vii
ŞEKİL LİSTESİ	viii
ÖZET.....	ix
ABSTRACT	x
GİRİŞ	1
I. BÖLÜM: TÜRKİYE ELEKTRİK PİYASASININ HUKUKİ YAPISI VE DÜZENLEMELERİ	3
II. BÖLÜM: ELEKTRİK PİYASASI İÇİN SİBER GÜVENLİĞİN ANLAMI, AMACI VE ÖNEMİ	17
2.1. ELEKTRİK PİYASASINA YÖNELİK SİBER GÜVENLİK KAVRAMLARI	25
2.2. ELEKTRİK PİYASASINDA YAŞANAN SİBER TEHDİTLERİN TÜRLERİ VE ETKİLERİ	36
III. BÖLÜM: ELEKTRİK PİYASASINI ETKİLEYEN SİBER GÜVENLİK DÜZENLEMELERİ VE STANDARTLAR	47
3.1. ULUSAL SİBER GÜVENLİK DÜZENLEMELERİ VE İLGİLİ KURUMLAR.....	48
3.1.1. Ulaştırma ve Altyapı Bakanlığı.....	50
3.1.2. Ulusal Siber Olaylara Müdahale Merkezi Ve Sektörel Olaylara Müdahale Ekibi	63
3.1.3. T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi	68
3.1.4. Bilgi ve İletişim Güvenliği ve Denetim Rehberi	71
3.1.5. Kişisel Verilerin Korunması Kanunu ve İkincil Düzenlemeleri	77
3.1.6. Sermaye Piyasası Kanunu Ve İkincil Düzenlemeleri.....	81
3.1.7. Türk Ceza Kanunu	83
3.1.8. Afet ve Acil Durum Yönetimi Başkanlığı	89
3.1.9. Milli İstihbarat Teşkilatı	95

3.1.10. TÜBİTAK	96
3.2. ULUSLARARASI SİBER GÜVENLİK STANDART VE DÜZENLEMELERİ İLE AB DÜZENLEMLERİ.....	99
3.2.1. ISO/IEC 27001:2022 – ISO/IEC 27001:2022.....	99
3.2.2. Tallinn El Kitabı (Tallinn Manual)	104
3.2.3. Avrupa Konseyi Siber Suç Sözleşmesi (Sanal Ortamda İşlenen Suçlar Sözleşmesi)	106
3.2.4. AB Siber Güvenlik Düzenlemeleri.....	109
3.3. ELEKTRİK PİYASASINA ÖZGÜ SİBER GÜVENLİK DÜZENLEMELERİ	120
3.3.1. Enerji Sektöründe Siber Güvenlik Yetkinlik Modeli Yönetmeliği	120
3.3.2. Enerji Sektöründe Kullanılan Endüstriyel Kontrol Sistemleri için Güvenlik Analiz ve Test Usul ve Esaslar	130
3.3.3. ISO/IEC 27019:2017	132
3.3.4. Türkiye Elektrik İletim Anonim Şirketi Bilgi Güvenliği Politikaları Yönergesi.....	133
IV. BÖLÜM: ELEKTRİK PİYASASINDAKİ HUKUKİ SORUMLULUK VE YAPTIRIMLAR	135
4.1. SİBER SALDIRILAR NEDENİYLE İDARİ OTORİTELERE BAŞVURU İMKANI VE SORUMLULUK.....	138
4.1.1. BTK Nezdinde Sorumluluk.....	141
4.1.2. CDDO Nezdinde Sorumluluk	148
4.1.3. KVKK Nezdinde Sorumluluk	150
4.1.4. EPDK Nezdinde Sorumluluk	154
V. BÖLÜM: SİBER GÜVENLİK YÖNETİMİNE DAİR İYİ UYGULAMALAR VE ÖNERİLER	159
SONUÇ.....	164
KAYNAKÇA	166

KISALTMALAR

AB	:	Avrupa Birliđi
ABD	:	Amerika Birleşik Devletleri
AFAD	:	Afet ve Acil Durum Yönetimi Başkanlığı
AK	:	Avrupa Komisyonu
age	:	Adı Geçen Eser
AR-GE	:	Araştırma Geliştirme
BİG	:	Bilgi ve İletişim Güvenliđi
Bkz.	:	Bakınız
BGYS	:	Bilgi Güvenliđi Yönetim Sistemi Tebliđi
BİLGEM	:	Bilgi Güvenliđi İleri Teknolojiler Araştırma Merkezi
BK	:	Bakanlar Kurulu
BKK	:	Bakanlar Kurulu Kararı
BM	:	Birleşmiş Milletler
BSI	:	British Standard Institute (İngiliz Standartları Enstitüsü)
BTK	:	Bilgi Teknolojileri ve İletişim Kurumu
CCDCoE	:	Müşterek Siber Savunma Mükemmeliyet Merkezi
CDDO	:	Cumhurbaşkanlığı Dijital Donuşum Ofisi
CIA	:	Confidentiality, Integrity, Accessibility (Gizlilik, Bütünlük, Erişilebilirlik)
CSIS	:	Center of Strategic & International Studies (Stratejik ve Uluslararası Çalışmalar Merkezi)
CSIRT	:	Computer Security Incident Response Team (Bilgisayar Güvenliđi Olay Müdahale Ekibi)
EBİS	:	Enerji Piyasası Bildirimleri Sistemi
ENISA	:	European Union Agency for Cybersecurity (Avrupa Birliđi Siber Güvenlik Ajansı)
ENTSO-E	:	European Network of Transmission System Operators for Electricity

		(Avrupa Elektrik İletim Sistemi Operatörleri Ağı)
EPDK	:	Enerji Piyasası Düzenleme Kurumu
EPİAŞ	:	Enerji Piyasası İşletim Anonim Şirketi
EKS	:	Endüstriyel Kontrol Sistemleri
EMS	:	Enerji Yönetim Sistemini
EPCIP	:	European Programme for Critical Infrastructure Protection (Kritik Altyapıların Korunması için Avrupa Programı)
ISO	:	International Standards Organization (Uluslararası Standartlar Örgütü)
IEC	:	International Electrotechnical Commission (Uluslararası Elektroteknik Komisyonu)
KVKK	:	Kişisel Verileri Koruma Kurumu
NATO	:	North Atlantic Treaty Organization (Kuzey Atlantik Antlaşması Örgütü)
NIST	:	National Institute of Standards and Technology (Ulusal Standartlar ve Teknoloji Enstitüsü)
NIS	:	The Network and Information Systems (Ağ ve Bilgi Sistemleri)
s.	:	Sayfa
SOİSS	:	Sanal Ortamda İşlenen Siber Suçlar Sözleşmesi
SOME	:	Sektörel Siber Olaylara Müdahale Ekibi
OECD	:	Organisation for Economic Co-operation and Development (Ekonomik İşbirliği ve Kalkınma Teşkilatı)
OSB	:	Organize Sanayi Bölgesi
USOM	:	Ulusal Siber Olaylara Müdahale Merkezi
TCK	:	Türk Ceza Kanunu
TEİAŞ	:	Türkiye Elektrik
TİB	:	Telekomünikasyon İletişim Başkanlığı
TSE	:	Türk Standartları Enstitüsü

TABLO LİSTESİ

Tablo 1. 1.	Enerji Piyasaları İşletme A.Ş. Esas Sözleşmeye Göre Hissedarlık Yapısı.....	12
Tablo 2. 1.	2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı İçinde Yer Alan “Bilgi Güvenliği” Ve “Siber Güvenlik” Kavramı.....	33
Tablo 3. 1.	5809 sayılı Kanun’da Yapılan Siber Güvenliğe Yönelik Değişikler.....	51
Tablo 3. 2.	5809 sayılı Kanun 5. Madde ve 1 sayılı Cumhurbaşkanlığı Kararnamesi 527/B Maddesi.....	59
Tablo 3. 3.	Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Bilgi ve İletişim Güvenliği Rehberi Varlık Gruplarına Yönelik Güvenlik Tedbirleri	73
Tablo 3. 4.	Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Bilgi ve İletişim Güvenliği Rehberi Uygulama ve Teknoloji Alanlarına Yönelik Güvenlik Tedbirleri.....	74
Tablo 3. 5.	Enerji Sektöründe Siber Güvenlik Yetkinlik Modeli Yönetmeliği Kapsamında Belirlenen Yetkinlik Modeli Kontrol Başlıkları ile Tanımları.....	123
Tablo 3. 6.	Siber Güvenlik Yetkinlik Modeli Uyarınca Sektörel Kritiklik Dereceleri.....	126
Tablo 4. 1.	Bilgi Teknoloji Kurumu İdari Yaptırımlar Yönetmeliği kapsamında bulunan ilgili mevzuat listesi	143

ŞEKİL LİSTESİ

Şekil 2. 1. Altyapı Karşılıklı Bağımlılık Örneği	24
--	----



ÖZET

Siber uzay, tartışmasız şekilde bireyler için güvenliğin sağlanması gereken alanlardan biri haline gelmiştir. Gerek klasik güvenlik anlayışı gerekse toplum yaşamının gerekleri itibariyle de hukuk metinlerinin ve idari otoritelerin bu güvenliği geliştirilmesinde her daim en temel araçlar olarak kabul edildiği görülmektedir. Bu kapsamda, hem fiziksel dünya üzerinde hem de siber uzayda varlığını koruması ve sürdürmesi önem arz eden kritik bir altyapıların da bu korumadan öncelikli yararlanması sağlanmalıdır. Siber güvenliğe ilişkin mevcut hukuki düzenlemelerin taraflara getirdiği pek çok yükümlülük bulunmaktadır. Ancak tanımlarda bir uzlaşma sağlanamamış olması, korunan hukuki değerle orantılı ve ağırlık merkezi siber güvenliğin dışında olmasına rağmen yine de hayatın siber uzaydaki yansıması gereği bu alana ilişkin düzenlemeler içeren çok sayıda hukuki metin ve bu kapsamda görevlendirilmiş kurumun ayrı ayrı bu işin altından gerektiği şekilde kalkması kolay görünmektedir. Bu çalışmada öncelikle elektrik piyasası aktörleri ve birbiri ile olan ilişkileriyle bu piyasada bulunmanın getirdiği yükümlülükleri, ardından ilgili piyasanın geçmişte farklı yerlerde yaşadığı problemlerin etkilerinden, bunun ardından siber güvenlik alanında ilgili piyasayı etkileyen ve sorumluluk ardından bırakan metinler ile idari otoriteler ile kritik altyapı tanımı başta olmak üzere ilgili tanımların içerikleri incelenecektir. İlgili idari otoritelerin ve mevcut hukuk metinlerin getirdiği sorumlulukların siber güvenlik ortamının zarar görmesi halinde nasıl tetikleneceği ve son olarak bu mekanizmaların bireylerin siber uzaydaki güvenliğini sağlamadaki etkinliği tartışılacaktır. Netice itibariyle, ulusal düzeyde ve salt siber güvenliğe özgülenmiş bir yasanın yahut idari otoritenin bulunmadığı ülkemizde, güvenlik ortamının inşası adına atılması gereken adımların neler olabileceği üzerinde durularak çalışmanın amacına ulaşması sağlanacaktır.

Anahtar Kelimeler: Siber Güvenlik, Bilgi Güvenliği, Elektrik Piyasası, Hukuki Sorumluluk, Kritik Altyapı.

ABSTRACT

It is evident that the realm of cyberspace has become a crucial domain where the security of individuals must be guaranteed. It is apparent that legal texts and administrative authorities have consistently been regarded as the most fundamental instruments in the development of this security, both in terms of the conventional understanding of security and the necessities of social life. In this context, it is of paramount importance to ensure that critical infrastructures, which are of paramount importance for the protection and maintenance of their existence in both the physical world and cyberspace, benefit from this protection with priority. The existing legal regulations on cyber security impose a number of obligations on the parties involved. However, despite the lack of consensus on the definitions, the proportionality of the legal value protected and the fact that the centre of gravity is outside of cyber security, it is relatively straightforward for a significant number of legal texts containing regulations related to this field and the institutions assigned within this scope to deal with this task separately due to the reflection of life in cyberspace. This study will initially examine the actors and their relations within the electricity market, as well as the obligations of being in this market. It will then analyse the effects of problems experienced by the relevant market in different places in the past. Furthermore, it will investigate the texts affecting the relevant market in the field of cyber security, and the subsequent responsibility left with administrative authorities. Finally, it will examine the content of the relevant definitions, with a particular focus on the definition of critical infrastructure. This study will examine the manner in which the responsibilities imposed by the relevant administrative authorities and existing legal texts will be triggered in the event of damage to the cyber security environment. It will also assess the effectiveness of these mechanisms in ensuring the security of individuals in cyberspace. Consequently, in our country, where there is no legislation or administrative authority at the national level with a specific remit for cyber security, the

objective of the study will be achieved by focusing on the measures that should be taken to establish a secure environment.

Keywords: Cyber Security, Information Security, Electricity Market, Legal Liability, Critical Infrastructure.



GİRİŞ

İnsanın temel ihtiyaçlardan biri olan güvenliğin sağlanması, artık yalnızca fiziksel olarak can sağlığı ve mal varlıklarının korunması ile değil, dijital dünyada da bir gereksinim haline gelmiştir. Bu dünyanın sınırları ve belirsizliği karşısında edindiği ismin, siber uzay olması da sonsuzluğa doğru genişleme niteliğinin bir getirisi olup, şu satırların yazıldığı ve okunduğu anda dahi gelişen dijital dünyanın uçsuz bucaksızlığına en kolay yoldan açıklamaktadır. Gerçek dünya ile bağı devam ediyor olsa dahi siber uzayda mevcut hukuk kurallarının aynı şekilde uygulanabilirliği yahut yeni baştan kurallara ihtiyaç duyup duymadığı da tartışma konusudur¹. Böyle bir ortamda gerek mahremiyet ihtiyacı gerekse de hayati önemi haiz hizmetlerin kullanılabilirliği adına siber güvenlik, çağın en kritik konularından birine dönüşmüştür. Bu kritik ihtiyacın yansıması olarak Avrupa Konseyi tarafından 2014 yılında yayımlanan Avrupa İnsan Hakları Sözleşmesi ile ilişkili şekilde hazırlanan İnternet Kullanıcıları için İnsan Hakları Rehberi'nde yer verildiği üzere hak ve özgürlüklerin çevrimiçi ortamlarda da varlığını koruduğu ve kullanımlarının desteklenmesi gerektiği belirtilmektedir². Fiziksel hayatın bir uzantısı olan siber uzayda da insan haklarının korunmasına ilişkin yasal çözümlerin oluşturulması ve buna ilişkin başvuru mekanizmalarının kurulması gerektiğinden bahsedilmiştir³. Dijital dünyada yalnızca hak kavramının yalnızca temel insan hakları bağlamında korunması değil, insan hayatının ve yaşamsal faaliyetlerin taşınması sebebiyle bu ortamda gerçekleşen tüm hukuki ilişkiler bağlamında da ele alınması ve bir güvenlik ortamının yaratılmasının aynı oranda önemsenmesi gerekmektedir.

Günümüz yaşantısının bir parçası olan elektrik hizmetlerinde de siber güvenliğinin sağlanması bu anlamda önemli bir yer kaplamaktadır. Pek çok kurum, ihtiyaç ve aracın sağlıklı bir şekilde çalışabilmesi, elektrik arzının

¹ Duygu Hatipoğlu Aydın, "Siber Alan ve Hukuk", On İki Levha Yayıncılık A. Ş., İstanbul, Mart 2022, s.43.

² Avrupa Konseyi Bakanlar Komitesi, "CM/Rec(2014)6 Sayılı Tavsiye Kararı, İnternet Kullanıcıları için İnsan Hakları Rehberi", 2014, s:6.

³ age. S. 22,24,51.

kesintisiz şekilde devam etmesine bağlıdır. Elektrik piyasasında yer alan aktörlerin, arz güvenliği konusundaki sorumluluğu genel olarak bu hizmetin devamlılığını garanti altına alıyor olsa da, siber güvenliğin sağlanabilmesi ya da sağlanamadığı durumlarda tarafların hukuki taleplerinin ne şekilde karşılanacağı sorusunun yanıtı şuan mevcut mevzuat üzerinden yanıt arıyor olsa da ihtiyaca cevap verip veremediği belirsizdir. İlgili piyasasının pek çok hukuk alanı ile bağlantısı ve yanı sıra siber güvenliğe ilişkin önlemlerin de aynı şekilde farklı amaçlara hizmet eden pek çok mevzuat tarafından bir yükümlülük olarak ele alınmış olması, hukuki taleplerin ne şekilde, kime, nasıl yöneltileceği hususunda kafa karıştırıcı olabilmektedir. Bu çalışma ile öncelikle bir hizmet olarak elektrik piyasası aktörlerinin, siber saldırılar neticesinde arz güvenliğine ilişkin yükümlülükleri yanı sıra müşterilerine yönelik sorumluluğunun ne şekilde tesis edildiği ya da edilmesi gerektiği hususu tartışılacaktır. Ulusal düzeyde bir siber güvenlik yasasının olmayışı ya da enerji piyasasının kritik altyapı olarak kabul ediliyor olmasının da bu sorumluluğa etkisi ayrıca incelenecek konulardır. Bu amaçla öncelikle elektrik piyasasından ve bu piyasada bulunan taraflardan bahsedilecek, siber güvenliğin elektrik piyasası için ne anlama geldiği ve mahiyeti izah edilmeye çalışılacaktır. Çalışmanın devamında siber güvenlik ile bağlantılı kabul edilebilecek ulusal, uluslararası hukuki metinlerin incelenmesinin ardından ayrı bir sektör olarak kritik altyapılardan elektrik piyasasında siber güvenliğin sağlanabilmesi adına yerine getirilmesi beklenen yükümlülükler değerlendirilecektir. Yapılan incelemelerin ardından siber güvenlik ihlallerinin neticesinde meydana gelebilecek zararlar karşısında, mevcut hukuk altyapısı ile sorumluluğun ne şekilde temin edilebileceği araştırılacaktır. Mevcut durumun incelenmesinin ardından, elektrik piyasasında siber güvenlik anlayışının geliştirilmesi ve kişilerin siber saldırılar nedeniyle uğrayacakları zararların en aza indirilmesi ile zararların tazmini adına yapılan iyi uygulama örnekleri ve önerilerden bahsedilerek çalışma tamamlanacaktır.

I. BÖLÜM

TÜRKİYE ELEKTRİK PİYASASININ HUKUKİ YAPISI VE DÜZENLEMELERİ

Uzun yıllar boyunca devlet eliyle görülen elektrik hizmeti yakın sayılabilecek bir tarihte büyük ölçüde özelleştirilmiştir. Elektrik talebinin gün geçtikçe büyümesi ile finansman maliyetlerinin artması⁴ bu politikanın tercihinde en başta gelen nedenler arasında yer almaktadır. Ancak teknolojik gelişmelerin kamu tekeline takip edilememesi sebebiyle yaşanan sıkıntılar, uzmanlaşmış kurumların piyasaya girişi ile verimliliğin, enerji kaybının ve arz güvenliğinin olumlu şekilde etkileneceği yönündeki değerlendirmeler de özelleştirme çalışmasına hız veren faktörlerden olmuştur. Belirtilen nedenlerin neticesinde pek çok sektörde yansımalarını gördüğümüz özelleştirme çalışmaları enerji piyasasında da 80’li yıllardan itibaren ayak sesini duyurmuştur⁵. Ekonomide liberalleşme çalışmalarının da başladığı bu dönemde yapılan yeni yatırımlarda elektrik ihtiyacının karşılanmasında yetersiz kalmıştır⁶.

Özelleştirme ve piyasanın rekabete açılması, karlılık odaklı firmaların hizmetlerinde fark yaratmak amacıyla oluşturacakları katma değer yaratma gayreti ile elektrik piyasasında uzmanlığın öne çıkmasına, kalitenin artırılıp fiyatların azaldığı bir piyasa modeli oluşturulmasına da imkân tanımıştır⁷. Fiyatların tekel bir kurum eliyle düzenlenmesinden hizmet kalitesine bağlı şekilde, rekabetçi bir piyasada faaliyet gösteren piyasa oyuncularına göre piyasa içinde belirleniyor olması ise tüketici nezdinde daha adil bir alışverişin yapılabilmesine de imkân sağlamıştır. Özelleştirme ile piyasanın

⁴ Kaan Mahmut Erdem, Deniz Erdem, “Türkiye’de Elektrik Dağıtımının Özelleştirilmesinin Nedenleri ve Amaçlar Özelleştirmede Tedaş Örneği”, İstanbul Barosu Dergisi, Temmuz-Ağustos, Cilt:91, Sayı:4, 2017, 215-226, s.218.

⁵ Murat Ertılav, Mehmet Aktel, “TEDAŞ (Türkiye Elektrik Dağıtım Anonim Şirketi) Özelleştirmesi”, Uluslararası Alanya İşletme Fakültesi Dergisi, Yıl:2015, C:7, S:2, 95-108, s. 96-97.

⁶ Erol Aslan, “Enerji Sektöründe İmtiyaz Sözleşmesi Çukurova-Kepez Örneği”, (Yüksek Lisans Tezi) Gazi Üniversitesi, 2010, s:32.

⁷ Cem Doğru, “Türkiye’de Elektrik Piyasasının Yeniden Yapılanması Sürecine Bir Bakış”, Sosyal Bilimler Metinleri, Sayı 1, 2010, s.14.

serbestleşmesinin ardındaki amacın tek yönlü olmadığı, hizmeti verenler ile temin eden tüketicilerin de serbestleşmesinin, piyasa modelinin amaçlarından biri olduğu, temelde çift yönlü şekilde ekonomide etkinlik yaratımının yattığı göz önünde bulundurulmalıdır⁸. Bunun yanında mali, toplumsal, sosyal, siyasi ve ideolojik pek çok farklı amacın da özelleştirmenin nedenleri arasında sayılması mümkündür⁹.

Pek çok kurumun yapısının değişimine sebep olan¹⁰ ve uzun yıllar süren özelleştirme çalışmaları neticesinde, elektrik piyasası içinde oluşması beklenen yapı, 6446 sayılı Elektrik Piyasası Kanunu’nun amaç başlıklı 1. Maddesinde de oldukça sarıh bir biçimde açıklanmıştır. İlgili hükme göre ilgili piyasanın “*Bu Kanunun amacı; elektriğin yeterli, kaliteli, sürekli, düşük maliyetli ve çevreyle uyumlu bir şekilde tüketicilerin kullanımına sunulması için, rekabet ortamında özel hukuk hükümlerine göre faaliyet gösteren, mali açıdan güçlü, istikrarlı ve şeffaf bir elektrik enerjisi piyasasının oluşturulması ve bu piyasada bağımsız bir düzenleme ve denetimin yapılmasının sağlanmasıdır.*” Şeklindeki amacı haiz bir kanun üzerine şekillenmesi beklentisi bulunmaktadır.

İlgili hükümden de açıkça görüleceği üzere, piyasanın yalnızca rekabetçi bir yapıya kavuşması değil aynı zamanda bu yapı içinde verilen hizmetlerin “yeterli, kaliteli, sürekli, düşük maliyetli ve çevreye uyumlu” bir şekilde sunuluyor olması da önem arz etmektedir. Bu amaçlar, özelleştirme çalışmalarına katılmış ve piyasada faaliyet gösteren şirketlere bir yükümlülük olarak aktarılmış durumdadır.

Bunun yanında,

⁸ Enerji Piyasası Düzenleme Kurulu, “Elektrik Piyasasında Uygulama El Kitabı”, 2003 s.2.

⁹ Ertılav, Aktel, s. 96-98.

¹⁰ Hakan Çetintaş, İbrahim Murat Bicil, “Elektrik Piyasalarında Yeniden Yapılanma ve Türkiye Elektrik Piyasasında Yapısal Dönüşüm”, Optimum Ekonomi ve Yönetim Bilimleri Dergisi,2015, 2(2),1-15, s.10-12.

- Elektrik enerjisi piyasasında verimliliği artırmak ve maliyetleri azaltmak için rekabetin sağlanması,
- Enerji sektörünün mali açıdan sürdürülebilirliğinin temin edilmesi için maliyetleri yansıtan fiyatların oluşturulması,
- Arz güvenliğinin sağlanması ¹¹ piyasanın özelleştirilmesi neticesinde piyasayı düzenlemekle görevlendirilmiş regülatif bir kurum olan Enerji Piyasası Düzenleme Kurumu tarafından da elde edilmesi beklenen hedefler arasındadır. Aynı zamanda, bu hedeflerin rekabetçi bir piyasanın içinde yer alan özel şirketlerin hizmet yarışında öne geçmek için kullanacağı basamakların da listesine karşılık geldiği söylenebilir.

Belirtilen amaçları yerine getirmek üzere çalışan elektrik piyasasındaki modern elektrik güç sistemlerinin teknik olarak üretim, iletim, dağıtım gibi üç temel teknik ünitelerden oluşmakta ve bu sistemlerin tüketici ile buluşturulduğu satış faaliyeti ile birlikte aynı zamanda bu süreçler temel hizmetler olarak kabul edilmektedir¹². Temel hizmetlerin yanı sıra günümüzde gelişen teknolojiler ve kaynakların tüketim hızının verdiği tahribatın giderilmesi adına artık yenilebilir enerji hizmetleri ile elektriğin depolanması da elektrik piyasasında adı geçen hizmetlerden olmuştur. Hem devletlerin hem de özel kuruluşların gündeminde önemli bir başlık olarak yer alan iklim krizinin yarattığı ve yaratacağı sonuçların bertaraf edilmesi adına yenilebilir enerji kaynaklarının çoğalmasına yönelik pek çok düzenleme yapılmıştır. Elektriğin üretildiği an tüketilmesi gereken bir kaynak olması da arz ve talep ekonomisi içinde değişen bir dinamik yaratmaktadır. Kaynak israfının önüne geçilebilecek, bunun yanında maliyetlere de çok önemli bir kazanç olarak kaydedilecek depolama faaliyeti 2022 yılında yapılan yasa değişikliği ile lisansa tabi kılınarak piyasaya dahil olmuştur.

Sonuç olarak 6446 sayılı Elektrik Piyasası Kanunu’nu içinde piyasadaki

¹¹ EPDK, “Elektrik Piyasasında Uygulama El Kitabı” s.2.

¹² Hasan Ayrancı, “Enerji Sözleşmeleri”, Yetkin Yayınları, 2000, s.49.

faaliyetlere yönelik olarak,

- Üretim faaliyeti
- İletim faaliyeti
- Dağıtım faaliyeti
- Toptan satış faaliyeti
- Perakende satış faaliyeti
- Piyasa işletim faaliyeti
- İthalat ve ihracat faaliyeti
- İhracat faaliyeti
- Toplayıcılık faaliyeti

İle ilişkin düzenlemelere yer verilmiştir. İlgili başlıklar aynı zamanda lisansa tabi kılınmış faaliyetlerin listesi olarak mevzuatta yer almakta olup bunun dışında lisanssız üretim faaliyetleri, depolama faaliyeti ile şarj hizmetleri de 6446 sayılı Kanun'nun düzenleme yaptığı alanlar arasında yer almaktadır. Belirtilen tüm faaliyetlerin elektrik piyasasında yer aldığı ve birbiriyle ilişkili olduğu biliniyor olduğundan her birini elektrik piyasası içinde ancak farklı uzmanlıklarıyla hizmet veren bir oyuncu olarak kabul etmekte fayda bulunmaktadır. Bu kısmın devamında anlatılacak olan, elektrik üretim sisteminin araçları olarak kabul edilecek lisanslar ve faaliyetlerine ilişkin detayların tamamı 6446 sayılı Elektrik Piyasası Kanunu'nda yer verildiği ölçüde ve sınırlı şekilde izah edilecektir.

Elektrik piyasası içinde bulunan tarafları, görev ve yükümlülükleriyle birlikte ele almak gerekirse, üretim şirketlerinden başlamak, elektriğin ürün olarak da tabiatına uygun olacaktır. Elektrik üretimi, en bilinen yöntemlerden olan barajlar aracılığıyla hidroelektrik enerjiden faydalanılarak gerçekleştirilebileceği

gibi rüzgâr, güneş enerjisi, biyokütle, jeotermal ya da termal kaynaklardan faydalanılarak da yahut günümüzde tartışmalara da konu olan nükleer enerji ile üretilmektedir. Üretim yapacakları her bir tesis için ön lisans başvurusu yapması gereken üretim şirketlerinin teminat mektubu teslim etmesi, tesisin kurulumu için belirlenen sahanın zilyetliğini temin etmesi, saha için çevresel etki değerlendirmesinin yapılması, altyapı kurulumu, iletim hattına bağlantı anlaşması yapılması gibi işlemleri tamamlamalarının ardından üretim lisansı teslim edilir. Özel şirketlerin yanı sıra kamunun¹³ ve organize sanayi bölgelerinin de elektrik üretimi yapabilme imkânı bulunmaktadır. Ayrıca lisanssız şekilde yenilebilir enerjilerden elektrik üretimi yapılabilmesi imkânı da koşulları karşılayan herkes tarafından faydalanılabilecek bir elektrik üretim şeklidir. Yenilebilir enerji kaynaklarından lisanssız üretim yapmanın, lisanslı elektrik üretiminden farklı koşulları olmakla birlikte, lisansa tabi şekilde elektrik üretimi yapan şirketlerin bir yıl içindeki elektrik üretimleri bir önceki yıl Türkiye’de üretilmiş elektriğin en fazla %20’si ile sınırlı olmak durumundadır. Üretim şirketleri üretmiş oldukları elektriği tedarik şirketlerine satabildikleri gibi serbest tüketici¹⁴ vasfına sahip taraflara da doğrudan elektrik satabilme imkanına sahiptirler. Bunun yanında lisanslarında belirlenen elektrik üretim miktarını aşmamak koşuluyla ve kendi tüketimleri hariç olmak üzere elektrik alımı da yapabilen üretim şirketlerinin tedarik şirketleri, serbest tüketiciler, iletim şirketi, zaman zaman dağıtım şirketleri

¹³ Türkiye Elektrik Üretim-İletim A.Ş. (TEAŞ) Genel Müdürlüğünün, 02.03.2001 tarih ve 24334 sayılı Resmi Gazetede yayımlanan 05.02.2001 tarih ve 2001/2026 sayılı Bakanlar Kurulu Kararı ile Elektrik Üretim A.Ş. (EÜAŞ)’ın da dahil olduğu, Türkiye Elektrik İletim A.Ş. (TEİAŞ), ve Türkiye Elektrik Ticaret ve Taahhüt A.Ş. (TETAŞ) unvanlı üç ayrı anonim şirket olarak teşkilatlandırılmış şirketlerden biri olarak ve 4628 sayılı Elektrik Piyasası Kanunu çerçevesinde faaliyette bulunmak üzere yapılandırılmış bir kamu kuruluşudur.

¹⁴ Serbest tüketici, Elektrik Piyasası Tüketici Hizmetleri Yönetmeliği’nin 4. Maddesinin 4. bendine göre “Serbest tüketici: Kurul tarafından belirlenen elektrik enerjisi miktarından daha fazla tüketimde bulunması veya iletim sistemine doğrudan bağlı olması veya organize sanayi bölgesi tüzel kişiliğini haiz olduğu için tedarikçisini seçme hakkına sahip gerçek veya tüzel kişiyi,” ifade etmektedir. Serbest tüketici, Enerji Piyasası Düzenleme Kurumu’nun resmi internet sayfasında aynı zamanda “Tüketiciler, serbest tüketici olup/olmadıklarını görevli tedarik şirketi tarafından gönderilen/bırakılan ödeme bildirimi veya faturalarda görebilirler. Ödeme bildirimi veya faturalarda; aboneliğe ait cari yıl ile bir önceki takvim yılı tüketim miktarları yer alır. Bu miktar o yıl için Kurul tarafından belirlen serbest tüketici limitini geçiyorsa serbest tüketici olma hakkına sahipsiniz demektir. ” şeklinde açıklanmıştır. 2024 yılı için belirlenen ve Resmi Gazete’de yayımlanan serbest tüketici limiti 950 kWh olarak belirlenmiştir.

ve diğ er üretim şirketleri gibi farklı taraflarla ilişkili bir piyasa oyuncusu olduđu söylenebilir.

Elektrik üretimi, genel itibariyle yerleşmenin olmadığı ya da üretim yapılacak kaynağa yakın alanlarda, kapsamlı tesislere ihtiyaç duyan bir faaliyet olduğundan, üretim aşamasından sonra şehirleşmenin olduğu alanlara taşınması amacıyla iletim hatlarına ihtiyaç duymaktadır. İnsan yerleşiminin başladığı bölgelerde trafolarla gerilimi düşürölüp dağıtım şebekesine aktarılan elektriğ in uzun mesafelerce yüksek frekansta iletilmesine aracılık eden bu makro şebeke, elektrik piyasası içinde özelleştirilmemiş ancak lisansa tabi ve yönetimi Türkiye Elektrik İletim Anonim Şirketi'ne ait olarak gerçekleştirilen bir hizmettir. İletim işletmesinin münhasıran TEİAŞ'a bırakılmış olmasının en önemli sebebi olarak batık maliyeti gösterilebilir. Bir kamu iktisadi devlet teşekkülü¹⁵ olarak faaliyet gösteren TEİAŞ'ın 02.07.2021 tarihli ve 4222 sayılı Cumhurbaşkanlığı Kararı ile özelleştirme kapsamına alındığı ve özelleştirme hazırlık işlemlerinin 31/12/2022 tarihine kadar tamamlanmasının öngörölldüğü kaydedilmiş olsa da konu ile alakalı bu tarihe kadar farklı bir gelişme yaşanmamıştır.

İletim faaliyeti gereğı, üretim hattından dağıtıma kadar elektriğ in yük dağıtımı ile frekansının kontrollü şekilde aktarılması, iletimin güvenli şekilde yapılması, bağlantı anlaşmasına uygun şekilde tarafların eşit şartlarda iletim hizmetinden faylanması gibi teknik görevlerinin yanında TEİAŞ'ın idari görevleri de bulunmaktadır. İletim hattına ilişkin yatırım ve iletim hattı kapasite arttırım planlarının yapılması ile elektrik piyasasında yan hizmet¹⁶ olarak geçen, elektrik sistemlerinin güvenilir şekilde işletimi ile iletişimi, elektriğ in gerekli kalite koşullarında hizmete sunulması konusunda belirlenen yükümlölüklerin takibi

¹⁵ TEİAŞ, 18.06.1984 tarih, 18435 sayılı Resmi Gazete'de yayımlanan 233 sayılı Kamu İktisadi Teşebbüsleri Hakkında Kanun Hükmünde Kararnameye tabi iktisadi devlet teşekkülü olup, Enerji ve Tabii Kaynaklar Bakanlığının ilgili kuruluşu olarak faaliyet göstermektedir.

¹⁶ Elektrik Piyasası Yan Hizmetler Yönetmeliğ i'nin Tanımlar başlıklı 3. Maddesinin 1. Fıkrasının III. Bendi uyarınca yan hizmet "Bu Yönetmelik uyarınca iletim sistemine veya dağıtım sistemine bağı lı ilgili tüzel kişilerce sağlanacak olan, iletim veya dağıtım sisteminin güvenilir şekilde işletimini ve elektriğ in gerekli kalite koşullarında hizmete sunulmasını sağlamak üzere bu Yönetmelik ve Elektrik Şebeke Yönetmeliğ inde ayrıntılı olarak tanımlanan hizmetleri," olarak tanımlanmıştır.

aslen TEİAŞ'a aittir. Bununla birlikte elektrik piyasasında üretim ve tüketim kalemlerine ilişkin ticaretin düzenli şekilde ilerlemesi ile sistemlerin sürekli işler kalabilmesine hizmet eden gerçek zamanlı sistem güvenliğinin kontrolünü yapmak, dengeleme ve uzlaştırma ile şebeke konularına ilişkin taraflara getirilen düzenlemelerin uygulamasını izlemek de TEİAŞ'ın görevleri arasındadır. Elektriğin uluslararası alanda alım satımına imkân sağlayan enterkonneksiyon sistemlerine¹⁷ ilişkin çalışmaları da yine TEİAŞ takip etmektedir. Kısaca üretilen elektrik ile tüketime sunulan elektriğin dengelenerek, sağlıklı bir şekilde sistemlerin işlerliğinin devam etmesi, frekansının düzenlenmesi ve sistemlerin frekans eşitsizliklerinden kaynaklanacak bir sebeple işlerliğini yitirmesinin önüne geçilmesi şeklindeki görev ve sorumluluğun TEİAŞ'a ait olduğu söylenebilir.

Dağıtım şirketleri, iletim hattından gelen elektriğin nihai tüketiciler tarafından kullanımı için gerekli gerilim seviyesinin ayarlanması, enerji akışını kontrol etmek, güç aktarımını sağlamak, hatların izolasyonunu gerçekleştirmek, gerilim seviyelerini değiştirmek, koruma ve kontrol ekipmanlarını barındırmak gibi elektriğin son tüketiciler tarafından kullanımına kadar devam eden teknik işlevleri yerine getirir. Özelleştirme çalışmaları neticesinde Türkiye 21 adet dağıtım bölgesine¹⁸ ayrılmış ve her bir dağıtım bölgesinde hizmet veren şirketler ihaleye katılarak ilgili bölgede 49 yıllığına ve mevzuatta belirlenen yükümlülöklere uygun şekilde hizmet vermeyi taahhüt etmişlerdir. İlgili dağıtım şirketleri görevli oldukları bölgede, enerji kaynaklarından gelen yüksek gerilimli

¹⁷ Enterkonneksiyon sistemi, farklı bölge veyahut ölkelerde bulunan enerji sistemlerinin veya elektrik şebekelerinin birbirine bağlanması, bu bağlantılar sayesinde, enerji ticareti yapılabilmesi, enerji kullanımına ilişkin arz ve talep dengesinin sağlanması, şebekenin güvenli şekilde dağıtımı, maliyetlerin optimize edilmesini sağlamaktadır.

¹⁸ Türkiye'de bulunan dağıtım ilgili şirketleri; Akdeniz Elektrik Dağıtım Anonim Şirketi, Akedaş Elektrik Dağıtım Anonim Şirketi, Aras Elektrik Dağıtım Anonim Şirketi, Adm Elektrik Dağıtım Anonim Şirketi,

Başkent Elektrik Dağıtım Anonim Şirketi, Boğaziçi Elektrik Dağıtım Anonim Şirketi, Çoruh Elektrik Dağıtım Anonim Şirketi, Dicle Elektrik Dağıtım Anonim Şirketi, Çamlıbel Elektrik Dağıtım Anonim Şirketi, Fırat Elektrik Dağıtım Anonim Şirketi, Gdz Elektrik Dağıtım Anonim Şirketi, İstanbul Anadolu Yakası Elektrik Dağıtım Anonim Şirketi, Kayseri Ve Civarı Elektrik Türk Anonim Şirketi, Meram Elektrik Dağıtım Anonim Şirketi, Osmangazi Elektrik Dağıtım Anonim Şirketi, Sakarya Elektrik Dağıtım Anonim Şirketi, Toroslar Elektrik Dağıtım Anonim Şirketi, Trakya Elektrik Dağıtım Anonim Şirketi, Uludağ Elektrik Dağıtım Anonim Şirketi, Vangölü Elektrik Dağıtım Anonim Şirketi, Yeşilırmak Elektrik Dağıtım Anonim Şirketi.

elektriğin düşük gerilime dönüştürülmesi, enerji ölçümlemesi ve koruma sistemleri gibi işlemler gerçekleştirerek güvenli bir enerji akışının teminini sağlar.

Dağıtım şirketleri, görevli oldukları bölgede, sayaçların okunması, bakımı ve işletiminden, yerleşim alanlardaki genel aydınlatma hizmetinden, teknik ve teknik olmayan kayıpların karşılanması amacıyla elektrik temin etmekten sorumlu tutulmuşlardır. Belirlenen faaliyetlerin gerçekleştirilmesi için Enerji Piyasası Düzenleme Kurulu onayı ile dağıtım tesisleri için dağıtım kapasite ikamesi ve/veya arttırımı yapılması, ilgili çalışmaların, yatırımlarının gerçekleştirilmesi gibi görevleri de yerine getirmektedir. Dağıtım şirketleri tarafından gerçekleştirilen dağıtım sistemlerine yönelik yatırımların mülkiyeti kamuya ait olduğundan, yeni dağıtım sistemi, sistem iyileştirilmesi, kapasite arttırımı gibi çalışmaların tamamında Kurul'dan onay alınması zorunlu olup aksi hal idari yaptırım uygulanmasını gerektirmektedir. Dağıtım şirketlerinin, elektriğin aktarımına yönelik görevlerinin yanında, elektriğin kullanımında optimizasyonu sağlayabilmek adına da görevleri bulunmaktadır. Örneğin dengeleme için talep tahmini yapmak ve TEİAŞ'a bildirme optimizasyon görevinin bir parçasıdır. Elektrik hizmetlerinde özelleştirmenin temel amacı olan liberalleşme ile serbest tüketiciler her ne kadar bulundukları bölgedeki dağıtım şirketinden elektrik dağıtım hizmeti almak dışında bir seçeneğe sahip değillerse de (organize sanayi bölgeleri hariç olmak üzere) ürün olarak elektriği temin edecekleri tedarik şirketini seçme hakları bulunmaktadır. Dağıtım şirketlerinin ise tedarikçisi kim olursa olsun tüketicilere elektrik dağıtım, sayaç okuma, genel aydınlatma ve belirlenen hizmetlerde eşit yaklaşım yükümlülüğü ve yanı sıra mevzuatta belirlenenler dışında elektrik piyasasında farklı herhangi bir faaliyet ile iştigal etmeme yükümlülüğü bulunmaktadır.

Tüketicilerin elektriği ürün olarak satın aldığı şirketler ise piyasadaki elektriğin toptan ve perakende satış faaliyetini gerçekleştiren tedarik şirketleridir. Elektrik tedarikçisi olarak anılan ilgili şirketlerin ayrımında, dağıtım bölgesinde görevli olup olmamalarına göre bir fark bulunmaktadır. Esasen dağıtım şirketi tarafından ve görevli olduğu bölgede gerçekleştirilmesi beklenen elektriğin

perakende satış faaliyeti “görevli tedarik şirketleri” tarafından icra edilmektedir. Görevli tedarik şirketleri farklı bölgelerdeki serbest tüketicilere de elektrik satabilmelerinin yanında görevli oldukları ilgili bölgede serbest tüketici olmayan tüketicilere regüle edilmiş tarife üzerinden yahut serbest tüketici olmasına karşılık tedarikçi seçmeyen tüketicilere son kaynak tedarikçisi sıfatıyla ve son kaynak tarifesi üzerinden elektrik temin etmektedirler. Bunun dışında kalan bağımsız tedarik şirketleri ise bölge kısıtlaması olmaksızın serbest tüketici sıfatını sahip herkese elektrik enerjisi temin edebilmekte ancak serbest tüketici sıfatına sahip olmayan tarafların tedarikçisi olamamaktadırlar. Belirtilen şekilde nihai tüketiciye elektrik satabilmek için tedarik lisansına sahip şirketlerin, satacağı elektriği temin edebilmek için üretim şirketlerinden elektrik alımı yapabilmenin yanında ithalat şirketlerinden veyahut yenilebilir enerji üreticilerinden de elektrik alabilme imkânı bulunmaktadır. Her halükârda tedarik şirketlerinin satın alabilecekleri ve nihai tüketiciye satabilecekleri elektriğin miktarı Türkiye’de bir yıl içinde tüketilen elektriğin %20’sini geçemez.

Elektriğin üretildiği an tüketilmesi gereken bir kaynak olması piyasada gerçekleştirilen alım satımların da düzenlenmesini ve kontrol edilmesini gerekli kılmıştır. Özelleştirme öncesinde üretim maliyetleri ile tüketim maliyetleri arasında farkın ölçümlenmesinde kamunun tekel gücünün kullanılıyor olması kayıp kaçak oranının Organisation for Economic Co-Operation and Development ortalama rakamlarına göre yüksek bir noktada seyretmesi¹⁹ toleransını geliştirmiş, bu durum piyasada maliyet artışına sebep olmuştur. Elektrik hizmetinin satış, dağıtım, iletim, üretim bacağında farklı şirketlerin faaliyet gösteriyor ve buna göre bütçeler çalışıyor olması gibi sebeplerin tamamı birlikte değerlendirildiğinde, piyasada şeffaflığın sağlanması ile maliyetlerin net bir şekilde ortaya konması hususu öncesinden daha büyük bir önemi haiz olmuştur.

Belirtilen amaçların sağlıklı şekilde yürütümü, elektrik piyasasının bağımsız bir şekilde işlemesi, elektrik üreticileri, tedarikçileri ve tüketicileri

¹⁹ Ertılav, s. 100.

arasında enerji alım satımı, dengeleme ile piyasa takas işlemlerinin gerçekleştirilmesi, etkili, şeffaf ve güvenilir bir yapının oluşturulması ile işletimin yapılması da ayrı bir lisansa tabi iş olarak belirlenmiştir. Bu görevleri yüklenmiş olan işletim lisansı sahibi Enerji Piyasaları İşletme A.Ş. (bundan sonra EPIAŞ olarak anılacaktır) özel hukuk hükümlerine göre kurulmuş bir şirkettir. Esas sözleşmesinde gösterilen hissedarlık yapısı²⁰;

Tablo 1. 1. Enerji Piyasaları İşletme A.Ş. Esas Sözleşmeye Göre Hissedarlık Yapısı:

Pay Sahibi	Grubu	Oranı
TEİAŞ	A	%30
Borsa İstanbul A.Ş.	B	%30
Piyasa Katılımcıları	C	%40

Kaynak : Enerji Piyasaları İşletme Anonim Şirketi, “Esas Sözleşmesi”, link: https://www.epias.com.tr/images/dokuman/Ek-1_1_EPIAS_Esas_Sozlesme.pdf (Son erişim tarihi:22.06.2024)

Şeklinde olup, C grubu hisseye sahip 94 özel sektör katılımcısının sahip olduğu pay %39,17 ortaklık şeklindedir. TEİAŞ’ın da bir kamu iktisadi teşebbüsü olduğu göz önünde bulundurulduğunda EPIAŞ’ın hissedar yapısının özel hukuk kişileri ile ve kamu iktisadi teşebbüsünden oluşan karma bir niteliği haiz olduğu görülmektedir. Yayımlanan son faaliyet raporuna göre de ortaklık yapısının korunduğu görülmektedir²¹.

18 Mart 2015 yılında kurulmuş EPIAŞ’ın görev ve sorumluluğunda olan

²⁰ Enerji Piyasaları İşletme Anonim Şirketi, “Esas Sözleşmesi”, link: https://www.epias.com.tr/images/dokuman/Ek-1_1_EPIAS_Esas_Sozlesme.pdf (Son erişim tarihi:22.06.2024)

²¹ Enerji Piyasaları İşletme Anonim Şirketi, “Faaliyet Raporu 2022”, 14 Şubat 2023, s.24 link: <https://www.epias.com.tr/wp-content/uploads/2023/02/EPIAS-2022-Yili-Faaliyet-Raporu-2023.pdf>, (son erişim tarihi 22.06.2024)

Şeffaflık Platformu, özetle elektrik kullanımları neticesinde gereken dengeleme ve elektrik alım satımlarına ilişkin uzlaştırma faaliyetlerinin gerçekleştirildiği, katılımcıları elektrik üreticileri ile tedarikçilerinden oluşan bir nevi elektrik borsası olarak faaliyet göstermektedir. EPİAŞ, kontrolünü sağladığı Şeffaflık Platformu ile sistem içinde elektriğin anlık üretiminde belirlenen maliyeti ile tedarik şirketleri tarafından satın alım talebi, talep karşısında değişen fiyatlama gibi parametrelerden oluşan yapıyı işletmektedir. Elektrik ticareti yapan tarafların, kayıtlı olmak durumunda olduğu ve Sermaye Piyasaları Kanunu hükümlerine göre türev araç kabul edilen elektrik sözleşmelerinin işlem gördüğü, borsa ile benzeş özellikler gösteren dinamik platform sayesinde elektrik piyasası herkese açık bir şekilde takip edebilmektedir. Platformun içinde Gün Öncesi Piyasası, Gün İçi Piyasası, Vadeli Elektrik Piyasası işlemleri yapılmakta olup Şeffaflık Platformunun faaliyete başlaması ile EPDK tarafından elektrik piyasası reformu adına öngörülen “Piyasa Günü”²² başlamış ve elektrik ticareti tam anlamıyla bağımsızlığına kavuşmuştur. İşletim lisansına sahip EPİAŞ’ın görev ve sorumlulukları arasında toptan organize elektrik piyasasına ilişkin uluslararası enerji piyasaları işlemlerini yürütmek, dağıtım, taşıma, tedarik, piyasa işletimi ve son kullanıcılara yönelik tarifelerin belirlenmesi, organize elektrik piyasasında faaliyet gösteren taraflara yönelik mali uzlaştırmanın sağlanması, piyasa katılımcılarından alınacak teminatların kontrol ve yönetimi gibi hususlar yer almaktadır.

Elektrik piyasası içindeki ithalat ve ihracata ilişkin işlemler ise Kurul onayı doğrultusunda tedarik ve üretim lisansı sahibi şirketler tarafından gerçekleştirilebilmektedir. Türkiye, elektrik iletimine hizmet eden Avrupa enterkoneksiyon sisteminin işletmesinden sorumlu Avrupa Elektrik İletim Sistemi İşleticileri Birliği’ne (European Network of Transmission System Operators for Electricity) 2016²³ yılında dahil olmuş ve uluslararası elektrik ticareti yapabilen bir

²² EPDK, 2003 s.3

²³ European Network of Transmission System Operators for Electricity, Turkish grid operator, TEIAS, joins ENTSO-E as observer member, 15 Ocak 2016, link: <https://www.entsoe.eu/news/2016/01/15/teias-member/> (Son erişim tarihi 22.06.2024)

konuma gelmiştir.

6446 sayılı Kanun'da belirtilen tedarik, dağıtım, iletim, üretim lisanslarının ve iştiğal ettikleri alanların dışında ayrıca belirli şartları sağlaması halinde lisansız elektrik üretme hakkının tesisi de söz konusudur. Kendi tesislerinde kullanmak üzere sanayi ve ticari işletmeler, seralar, tarım arazileri veya hayvan çiftlikleri gibi alanlar için tarımsal işletmeler, bireysel ihtiyaçları için konut sahipleri ya da kooperatifler lisans almaksızın elektrik üretebilmektedir. Bu alanda sıklıkla öne çıkan yöntemler, çatı üstü güneş enerjisi sistemleri, rüzgâr türbinleri, güneş enerjisi panelleri, biyogaz tesisleri veya mini rüzgâr türbinleri gibi yöntemlerdir. Lisanssız üreticiler, belirlenen tarife üzerinden üretmiş oldukları fazla enerjiyi şebekeye de satabilmekte ve gelir elde etmektedir. Genellikle yenilebilir enerji kaynaklarına dayanan lisansız elektrik üretimi düşük maliyetli ve çevre dostu olmaları nedeniyle teşvik edilmektedir. Bu şekilde, enerji üretiminde çeşitlilik, enerji tasarrufu sağlanmakta ve enerji arz güvenliği artırılmaktadır.

Elektrik Piyasası Kanunu gereği verilen lisanslar ile her bir lisans sahibinin hak ve yükümlülükleri düzenlenmiş durumdadır. Elektriğin santrallerde üretilmesinden sonra, evlerimizde bastığımız açma/kapama tuşuna kadar ki yolculuğu aslında hayli meşakkatli ve pek çok tarafın birlikte gerçekleştirdiği bir hizmetler bütünüdür. Bu yolculuğun içinde lisansa tabi üretim şirketleri tarafından üretilen elektrik, kullanımına imkân sağlayacak şekilde regüle edilerek şehir şebekesine iletişim şirketi TEİAŞ sayesinde ulaşır, iletim santrallerinden alınan elektrik de şebekeden kullanılabilecek şekilde dağıtım şirketleri sayesinde yayılır. Şehir şebekesine ulaşan elektriğin satışı ile doğrudan tüketicilerin kullanımına aracılık eden perakende tedarik şirketleri ise elektriğin satış faaliyetini gerçekleştirerek tüketici ile buluşturur. Bunun yanında elektrik piyasasının takibi konusunda çalışmalar yapan EPIAŞ başta olmak üzere TEDAŞ, EPDK, Enerji ve Tabi Kaynaklar Bakanlığı gibi pek çok kurumun etkisinden de bahsetmek gerekir. Ayrıca lisansız üretim yaparak üretim noktasından elektrik şebekesine katılan yenilebilir enerji üreticileri ile artık üretimden gelen elektriğin depolanması ile satışına aracılık eden depolama lisansı sahibi şirketler de

yolculuğun içindeki diğer aktörlerdir.

Oldukça kapsamlı ve önem arz eden bir iş olan elektrik hizmetlerinin, 2001 yılından bu yana 6446 sayılı Kanun'da belirtilen amaca uygun şekilde temin edilebilmesi için EPDK'da çalışmaya devam etmektedir. Özelleştirilmiş bir hizmet olarak anılıyor olsa da elektrik hizmetlerinin kontrolü, şirketlerin tekel gücünü kötüye kullanmaması, verilen hizmetin devamlılığı için takip edilecek usulü belirleyip düzenleyerek, aynı zamanda ilgili piyasanın takipçisi ve denetleyicisi olarak EPDK'da varlığını sürdürmektedir²⁴. EPDK'ya Enerji Piyasası Düzenleme Kurumunun Teşkilat ve Görevleri Hakkında Kanun ile verilmiş görevler:

- Lisansların temini,
- İşletme devir hakkı sözleşmelerinin düzenlenmesi,
- Lisans verilmiş ilgili şirketlerin performansının izlenmesi,
- Performans parametrelerinin belirlenmesi,
- İlgili düzenleyici yasal metinlerin oluşturulması, tadili ve uygulanması ile uyumluluğun denetlemesi,
- Piyasada uygulanacak tarifelerin belirlenmesi ile uyarlanması²⁵ şeklinde sayılabilir.

Kısaca, lisans sahibi olsalar da elektrik piyasasındaki tüm şirketler imtiyaz sözleşmelerinde belirlenmiş yükümlülüklerini yerine getirirken, Kurul kararlarıyla bağlı olup, denetimine tabi durumdadırlar.

Görüleceği üzere, elektrik piyasası, enerji üretiminden dağıtımına kadar birçok paydaşı içeren karmaşık bir yapıdır. Bu paydaşlar arasında özel enerji

²⁴ Doğru, 2010, s. 10.

²⁵ Enerji Piyasası Düzenleme Kurumunun Teşkilat ve Görevleri Hakkında Kanun, Resmî Gazete Nu: 28603, Yayımlı Tarihi:30.03.2013, Kanun Nu:6446, 4. Madde.

şirketleri, kamu kurumları, tedarikçiler, ve tüketici grupları bulunmaktadır. Elektrik piyasasında faaliyet gösteren şirketler ve kamu kurumları, enerji üretimi, iletimi ve tüketimi için birbirlerine bağlı olup, enerji arzının sürekliliği amacıyla sık sık işbirliği yapmaktadır. Pek çok firma bu işbirliği ve sistemlerin entegrasyonu için manuel araçların yanı sıra bilişim sistemlerini de kullanır vaziyettedir. Bu birbirine bağlılık ve birleşik yapının etkisiyle siber güvenlik olayları elektrik piyasası ve hizmetin kendisi için de bir domino etkisi yaratmaktadır. Siber güvenliğin bu bakış açısıyla önemi ile elektrik piyasası için ne anlama geldiği, piyasadaki oyuncuların bu husustaki sorumlulukları metnin devamında detaylandırılarak izah edilecektir.

II. BÖLÜM

ELEKTRİK PİYASASI İÇİN SİBER GÜVENLİĞİN ANLAMI, AMACI VE ÖNEMİ

Elektrik piyasası mevzuatına bakıldığında görüleceği üzere, piyasanın oyuncuları pek çok hukuki sorumluluk ve yetki ile donatılmış durumdadır. Pek çok teknik gerekliliğin yerine getirilmesi beklenen ve oldukça katmanlı bir yapısı bulunan²⁶ ilgili sektörün sorumlu olduğu ve aslında ulusal anlamda önemi haiz arz güvenliğinin kritik bir alanını oluşturan siber güvenlik de hem teknik hem de kendine has özelliklere sahip, farklı disiplinlerin de konusuna giren bir alan olarak anılmaya başlamış başlamıştır²⁷.

Siber güvenlik alanında hukuki bir metin yazılması ve tarafların sorumlulukları ile yetkilerinin tespit edilmesi, hiç şüphesiz ilgili alanın temel kavramlarını haiz olmayı gerektirmektedir. Bu nedenle konunun teorik kısmına ve kompleks yapısına ilişkin değerlendirmelere girilmeden, önem arz ettiği düşünülen tanımların yapılması ile başlamak, konuyu kavramak açısından gerekli görünmektedir. Metnin bundan sonraki ilk başlığında, üzerinde hali hazırda bir uzlaşma olmaması ve yer aldığı metinlere göre farklılık gösteriyor olsa da belirli tanımlar üzerinde durulacaktır. Bunun öncesinde ise siber güvenlik bakış açısıyla elektrik piyasasının konumundan bahsetmek gerekmektedir. Bu kapsamda kritik altyapı tanımı, elektrik piyasası için bakımından öncelikle anlaşılmalıdır.

Dönemin Ulaştırma Bakanlığı²⁸ tarafından hazırlanan ve 25.03.2013 tarihinde Bakanlar Kurulu tarafından kabul edilen Ulusal Siber Güvenlik Stratejisi

²⁶ Mustafa Meral, “Siber Güvenlik Kapsamında Kritik Altyapıların Korunmasının Önemi”, (Yüksek Lisans Tezi), Harp Akademileri Stratejik Araştırmalar Enstitüsü, 2015 S.44.

²⁷ Soner Çelik, “Siber Uzay Ve Siber Güvenliğe Multidisipliner Bir Yaklaşım”, Academic Review of Humanities and Social Sciences, 2018, 1(2): 110-119, s. 118.

²⁸ 2024 yılı itibarıyla Ulaştırma ve Altyapı Bakanlığı adıyla hizmet vermeye devam eden ilgili Bakanlığın, 2011’den 2018 tarihine kadar devam eden hizmet döneminde ismi Ulaştırma, Denizcilik ve Haberleşme Bakanlığı olarak anılmış olup, bazı mevzuat hükümlerinde isminin bu şekilde yer aldığı görülmektedir. 2011’den evvel Ulaştırma Bakanlığı olarak anılan kurumun 5809 sayılı Kanun’da da isminin aynı şekilde yer alıyor olması ve metinde karışıklığın önünde geçilmesi adına bundan sonra Ulaştırma Bakanlığı olarak anılacaktır.

ve 2013-2014 Eylem Planı'nda kritik alt yapılara ilişkin “*Kritik altyapılar: İşlediği bilginin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda,*

- *Can kaybına,*
- *Büyük ölçekli ekonomik zarara,*
- *Ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapıları,”* şeklinde bir tanım yapılmıştır.

Aynı tanım 2016-2019 tarihleri ve 2020-2023 tarihleri için hazırlanan Ulusal Siber Güvenlik Stratejisi ve Eylem Planı belgelerinde de aynı şekilde yerini almıştır²⁹. Bu tanım, kritik alt yapı kabul edilen ilgili sektörleri doğrudan belli etmiyor olsa da 2013-2014 Eylem Planı metninin giriş kısmında “*Kamu kurumlarına ilave olarak enerji, haberleşme, su kaynakları, tarım, sağlık, ulaşım, eğitim ve finansal hizmetler gibi kritik altyapı sektörlerinde faaliyet gösteren kurum ve kuruluşlar da bilgi ve iletişim sistemlerini yoğun olarak kullanmaktadır.*” Denilmek suretiyle bu sektörlerin neler olabileceği konusunda yön gösterilmiştir.

2016-2019 Eylem Planı'nda ise “*Kritik altyapı sektörleri: 20/06/2013 tarih, 2 sayılı Siber Güvenlik Kurulu kararı uyarınca kritik altyapıları barındırmakta olan “Elektronik Haberleşme”, “Enerji”, “Su Yönetimi”, “Kritik Kamu Hizmetleri”, “Ulaştırma” ve “Bankacılık ve Finans” sektörlerini, ... ifade eder.*” şeklindeki tanımı ile 2020-2023 Eylem Planı'nda ise “*Kritik Altyapı Sektörleri: Mülga Siber Güvenlik Kurulu'nun 20 Haziran 2013 tarihli ve 2 sayılı kararı uyarınca kritik altyapıları barındırmakta olan “Elektronik Haberleşme”, “Enerji”, “Finans”, “Ulaştırma”, “Su Yönetimi” ve “Kritik Kamu Hizmetleri” sektörleri.*” denilerek, ilgili sektörler sayılmıştır.

²⁹ Ulaştırma ve Altyapı Bakanlığı, “2020-2023 Siber Güvenlik Stratejisi” s.9, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, “2016-2019 Ulusal Siber Güvenlik Stratejisi”, 2016, s.8.

İlk eylem planında bahsi geçen eğitim, sağlık, tarım gibi sektörlerin 2016-2019 tarihli ve sonraki metinde yer almadığı, bunların yerine ise kritik kamu hizmetlerinin eklendiği görülmektedir. 2016-2019 tarihli metinde yer alan “Bankacılık ve Finans” sektörü ise 2020-2023 tarihli metinde yalnızca “Finans” olarak anılmıştır.

Bunun yanında, enerji sektörünün içinde doğal gaz, petrol, elektrik ve günümüz Türkiye’si için artık nükleer enerji de olduğu ve bu ana enerji kaynaklarına ilişkin Boru Hatları ile Petrol Taşıma Anonim Şirketi, EPIAŞ, üretim şirketleri, iletim şirketleri, perakende şirketleri, dağıtım şirketleri, kullanıcı birlikleri, taşıyıcılar, dolum tesisleri, ihrakiye teslim şirketleri ve bayileri, LPG bayileri, lisanslı depolama faaliyeti yürütenler, madeni yağ üreticileri gibi ve sayılanların dışında da pek çok taraf ve şirketin bulunduğunu da belirtmek gerekir. Bahsi geçen işletmelerin tamamının kritik alt yapı sektörüne özgü oyuncular olamayacağı ortada olduğu gibi kimlere bu kapsamda bir sorumluluk atfedileceğinin çerçevesinin çizilmemiş olması da bir belirsizlik yaratmaktadır. Bu belirsizlikten lafzi yorum ile çıkma gayreti ile çalışması için bir altyapı sistemine ihtiyaç duyan işletmelerin bu kapsamda değerlendirilebileceği gibi bir çerçeve yaratılabilecekse de yeterli olamayacağı ortadadır. Kritik altyapıların belirlenmesi görevinin tamamlanmamış olduğunu gösteren bu sektör listesi ve ileride bahsedilecek pek çok mevzuat hükmü de bu belirsizliğin önüne geçilmesi gerektiğini işaret etmektedir.

AB nezdinde de kritik altyapıların güvenliğini sağlayabilmek adına öncelikle bu yapıların tespiti ve buna ilişkin somut bir metodolojisi geliştirilmesi gerektiği görülmüştür. Bu tespit çalışmasının yarattığı zorluğu aşabilmek adına AB’de öncelikle 2008/114/EC sayılı bir direktif yayımlanmıştır³⁰. Yayımlanan Direktif ile Avrupa’da kritik altyapıların korunmasına yönelik başlatılmış olan EPCIP programı ve devamında gelen programların etkinliğini arttırabilmek, yanı sıra kritik altyapıların korunmasına ilişkin çalışmaların tüm Avrupa genelinde

³⁰ AB Konseyi, 2008/114/EC Sayılı Direktif, “on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection”, 2008.

arttırılması ile paydaşlar arasında işbirliği ile iletişim sağlanmasını da amaçlanmıştır. 2008/114/EC sayılı Direktif'ten evvel AB Komisyonu tarafından yayımlanan, 2004/702 Sayılı Rapor'da da kritik altyapıların tespitine ilişkin, kapsam, büyüklük ve zaman etkisinin göz önünde bulundurulması önerilmiştir³¹. Sonrasında gelen 2008/114/EC sayılı Direktif ise kritik altyapıların tanımlanması adına, 2004/702 sayılı Rapor ile paralel şekilde ancak enerji³² ve ulaşım sektörlerinin alt sektörleri önceliklendirilerek³³ tüm sektörün ne şekilde ele alınıp kritik altyapıların ve önem derecelerinin nasıl tespit edileceğine ilişkin somut bir metodoloji ortaya koymuştur. 2008/114 sayılı Direktif'in 3. Maddesinde belirlenen parametreler ve sonrasında EK 2'ye yapılan atıf ile bir AB ülkesinde bir kuruluşun kritik altyapı olup olmadığının belirlenmesine ilişkin olarak yapılacak değerlendirmede,

1. Kayıp kriteri (potansiyel ölüm veya yaralanma sayısı olarak değerlendirilir)
2. Ekonomik etki kriteri (ekonomik kaybın ve/veya ürünlerin veya hizmetlerin bozulmasının önemi olarak değerlendirilir; potansiyel çevresel etkiler de dahil)
3. Kamu etkisi kriteri (halkın güvenine, fiziksel acıya ve günlük yaşamın kesintisine etki olarak değerlendirilir; temel hizmetlerin kaybı da dahil).

³¹ AB Komisyonu, 2004/702 Sayılı Rapor, "Critical Infrastructure Protection in the fight against terrorism", 2004, s.5 "Potansiyel kritik altyapıyı tanımlamak için üç faktör önerilebilir: • Kapsam - Bir kritik altyapı unsurunun kaybı veya kullanılamaz hale gelmesi, etkilenen coğrafi alanın boyutuna göre değerlendirilir - uluslararası, ulusal, bölgesel / yerel. • Büyüklük - Etkinin veya kaybın derecesi Hiçbiri, Minimal, Orta veya Büyük olarak değerlendirilebilir. Potansiyel büyüklüğü değerlendirmek için kullanılabilecek kriterler arasında: (a) Kamu etkisi (etkilenen nüfus miktarı, can kaybı, tıbbi hastalık, ciddi yaralanma, tahliye); (b) Ekonomik (GSYİH etkisi, ekonomik kaybın önemi ve / veya ürünlerin veya hizmetlerin bozulması); (c) Çevresel (halka ve çevredeki konuma etkisi); ve (d) Karşılıklı bağımlılık (diğer kritik altyapı unsurları arasında). (e) Siyasi (hükümetin yeteneklerine olan güven); • Zaman etkileri - Bu kriter, bir unsurun kaybının ne zaman ciddi bir etkiye sahip olabileceğini belirler (yani, anlık, 24-48 saat, bir hafta, diğer)."

³² AB Konseyi, 2008/114/EC Sayılı Direktif, Ek 1'e göre enerji sektöründe yer alan elektrik, doğal gaz ve petrol kurumları bu kapsamda sayılmıştır.

³³ AB Konseyi, 2008/114/EC Sayılı Direktif, Gerekçe (Recital) 5.

4. Kritik altyapı sektörünün öznel özelliklerinin

Göz önünde bulundurulması gerekmektedir. Sektörlerin sahip olduğu özelliklerden ve verdikleri hizmet ile sattıkları ürünlerden bağımsız şekilde tespit yapılması amaçlandığından, ilk üç kriter her bir kuruluş nezdinde belirlenebilir özelliklere sahip çapraz kesen kriterler olarak anılmıştır. 2008/114/EC sayılı Direktif ile bu parametrelere ilişkin AB üyesi ülkelerinin iç hukukunda etkili yönergeler çıkarılıp eşikler belirleyebileceği, bu hususta bir bağlayıcılık olmadığı ancak kriterlere yönelik eşikler ve kritik altyapılara yönelik olarak AB Komisyonu'na raporlama yükümlülüğü getirilmiştir. Ek 2'de yer alan prosedüre göre ise kritik altyapıların belirlenmesine ilişkin Üye Devletlerin,

1. Sektör özelinde değerlendirme yapması,
2. Adımda belirledikleri sektörün, toplumsal işlevlerin sürdürülmesi, insanların sağlığı, emniyeti, güvenliği, ekonomik veya sosyal refahı adına değeri ve verdiği ürün ve hizmetin kesintiye uğraması halinde önemli bir etkinin oluşup oluşmayacağı ile alternatiflerine yönelik bir değerlendirme yapması,
3. Adımda etkili olduğu belirlenen sektörün zarar görmesi halinde en az iki Üye Devlet üzerinde madde 3'te belirtilen zayıat, ekonomik etki, kamu etkisi bağlamında etkisi ve bu sektörün zarar görmesi durumunda alternatiflerinin varlığı, düzeltilmesinde geçecek zamanı dikkate alınarak önemini değerlendirme,
4. Adımı da geçen sektör için zayıat, ekonomik etki, kamu etkisi bağlamında etkisini ve bu sektörün zarar görmesi durumunda alternatiflerinin varlığını, düzeltilmesinde geçecek zamanı dikkate alarak önemini değerlendirme,

Aşamalarını tamamlayarak kritik altyapı tespitini gerçekleştirmesi beklenmektedir. İzah edilen adımların kendi içlerinde de birbirilerine bağılılığı

görülmekle birlikte prosedür, bir adımın dahi değerlendirmeyi geçemiyor olması halini, bu sektörün kritik altyapı olamayacağı şeklindeki yorumlamayı gerektirmektedir. Her ne kadar yasal düzenleme ile kritik altyapıların belirlenmesine yönelik AB için değerli bir adım atılmışsa da bu tespitin yapılmasının zorluğu görülmektedir. Ancak bu yolda genel geçer parametrelerin oluşturulması ve bunların gelişen teknoloji karşısında da sürdürülebilir olabilmesi, her halükarda öznel değerlendirmelerin yerine nesnel gerekçelere indirgenmesi önemlidir. Türkiye’de de kritik altyapıların sektör ve alt sektör bazlı belirlenmesinin, gerek güvenliklerinin geliştirilmesi gerekse de sorumlulukların tasnifi açısından oldukça önemli bir konu olarak gündeme alınması gerekmektedir. Bu hususta hazırlanan Bilgi ve İletişim Güvenliği Rehberi, varlık gruplarına yönelik olarak kritiklik derecesinin nasıl belirlenebileceği yönünde bir metodoloji geliştirmiş olsa da yeterli görünmemektedir. Zira bir adım öncesinde, bir şirketin enerji sektöründe olsa dahi, ilgili rehberde yer alan sorumluluğun tarafı ve kritik altyapı olarak kabul edilip edilmediği muğlak görülmektedir.

Her halükârda enerji ve ardı sıra elektrik piyasasının kritik altyapılar arasında kabul edildiği, dağıtım, üretim ve iletim gibi lisans sahibi şirketlerin gerek hizmetlerini sunmak için ihtiyaç duydukları sistem gereklilikleri gerekse de vermiş oldukları hizmet itibarıyla kritik altyapı oldukları şeklindeki bir yorumun ilgili strateji belgeleri ve mülga Siber Güvenlik Kurulu’nun 20 Haziran 2013 tarihli ve 2 sayılı kararı uyarınca kabul edilmesi gerekir. Zira bahsedilen lisans sahibi şirketlerin bilgi altyapılarının gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda, can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek nitelikte olması, yaptıkları işin doğasından kaynaklanmaktadır. Ancak elektrik piyasasında yer alan ve ilgili mevzuat ile düzenlenmiş sorumluluklara sahip hangi kuruluşların kritik altyapı olarak kabul edildiğinin tespiti hali hazırdaki hukuki metinler aracılığı ile mümkün görünmemektedir.

Kritik altyapıları belirlemekle görevlendirilmiş olan Ulaştırma Bakanlığı nezdinde kurulmuş Ulusal Siber Olaylara Mühadale Merkezi tarafından

yayımlanan Sektörel SOME Kurulum ve Yönetim Rehberi içinde, enerji sektörü için kritik altyapıların belirlenmesine yönelik olarak “Sistemlerin ürettiği, depoladığı, ilettiği, dağıttığı veya satışına aracılık ettiği enerji miktarı”na bakılarak bir tespit yapılabileceği EPDK’ya önerilmişse de henüz bu hususta bir düzenleme yapılmamıştır. Detaylarına daha sonra değinilecek olan güncel mevzuata göre Ulaştırma Bakanlığı ve Cumhurbaşkanlığı Dijital Dönüşüm Ofisi de bu hususta yetkili konumdadır. Bu nedenle bu hususta yapılacak bir düzenlemenin getirilmesine kadar yapılan bir kuruluşun kritik altyapı olarak kabulünün mümkün görünmemektedir. Hali hazırda var olan bu belirsizlik içinden çıkabilmek adına metnin bundan sonrasında, gerekmesi halinde istisnai durumlardan bahsedilerek elektrik piyasasının tamamından kritik altyapı olarak bahsedilecektir.

Kritik altyapı olarak kabul edilen elektrik piyasasında siber güvenliğin ise ayrı ve özel bir önemi bulunmaktadır. Her ne kadar kritik altyapılar ülkelerin önceliklerine göre farklılık gösterebilir de³⁴ hangi sektörde olursa olsun kritik altyapı olarak kabul edilen kuruluşların birbirleriyle olan ilişkisinde elektrik piyasası, etkisi ve günümüz çalışma koşullarının temelini oluşturan teknolojinin işleyişi gereği merkezi bir konumu bulunmaktadır. Literatürde karşılığı, altyapı karşılıklı bağımlılıkları olan bu durum, bir altyapının durumunun, diğerinin durumunu doğrudan veya dolaylı olarak etkilediği farklı altyapılar arasındaki bağlantıları ve ilişkileri ifade eder. Bu karşılıklı bağımlılıklar fiziksel, siber, coğrafi veya mantıksal nitelikte olabileceği gibi çeşitli mekansal ve zamansal ölçeklerde ortaya çıkabilir. Altyapıların karşılıklı bağımlılıklarının dikkate alınması önemlidir çünkü bir altyapıdaki aksaklıklar veya arızalar diğer altyapılar üzerinde dalgalanma etkileri yaratabilir, geniş coğrafi bölgeleri etkileyebilir ve potansiyel olarak ulusal ve küresel ekonomide aksamalara neden olabilir. Özellikle siber uzayda bu bağımlılık her ne kadar yeni de olsa altyapıların otomasyonu ve şebeke kontrollerinin SCADA sistemleriyle yapılması gibi

³⁴ Mustafa Ünver, Cafer Canbay, Hüseyin Burhan Özkan, “Kritik Altyapıların Korunması”, Bilgi Teknolojileri Ve İletişim Kurumu, 1. Basım, Nisan 2011, S.4-7.

kesintisinin 60 milyon dolar zarara neden olduđu, aktörlerinin Rusya olduğundan şüphelenilen siber saldırılarla elektrik altyapısı zarar gören Ukrayna’da ise bu nedenle alınan önlemler ile yapılan çalışmaların, ekonomiye her gün 200 milyon dolardan fazla maliyete sebep olduğu söylemektedir³⁸.

Her bir sektörü, tüm kurum ve kuruluşların işleyişini, insanların sosyal hayatını ve hatta psikolojilerini etkileyebilecek nitelikte, hayati önem sahip elektrik alt yapısının sağlıklı ve kesintisiz çalışabilmesi hiç şüphesiz, fiziksel ve siber saldırılardan güçlü bir savunma mekanizması ile korunmasına bağlıdır. Çalışmanın bundan sonraki kısmında, öncelikle siber güvenliğe ilişkin önemli kavramlara ve elektrik piyasandaki yansımalarına ardından da elektrik piyasasında yaşanmış somut olaylar üzerinden etkilerine yer verilerek siber güvenliğin piyasa için öneminden bahsedilecektir.

2.1. ELEKTRİK PİYASASINA YÖNELİK SİBER GÜVENLİK KAVRAMLARI

Siber güvenlik uygulaması itibarıyla pek çok mühendislik bilgisini bünyesine dahil eden ve teknik bir alan olduğundan hakkında yapılan araştırmalarda da bu teknik altyapının izlerini barındırmaktadır. Bunun yanı sıra, fiziksel bir alanda sağlanması beklenen güvenlik ile birden çok boyutu olan siber uzayda³⁹ sağlanması beklenen güvenliğin yöntemleri de haliyle ayrı bir alan olarak uzmanlaşılmasını gerekli kılmaktadır. Elektrik piyasası operasyonları ve bu operasyonlarda kullanılan sistemler de aynı şekilde mühendislik birikimi üzerine inşa edilmiş olduğundan, iki alanın kesişiminin anlatımı karmaşık bir izaha sebep olabilmektedir. Her ne kadar bu alanların uygulamaları nedeniyle fen bilimlerinin araştırmalarına konu edilmesi doğasındansa da bu gelişimin getirdiği faydaların ve korunması gereken unsurların beşeri bilimlerce de konu edilmesi o

³⁸ Peleschuk, Dan, “Blackouts hit Ukraine's small businesses, and wider economy, hard”, link: <https://www.reuters.com/world/europe/blackouts-hit-ukraines-small-businesses-wider-economy-hard-2022-11-18/> (Son erişim tarihi 22.06.2024)

³⁹ Muhammet Oğuz, “Stratejiden Yasaya Avrupa Birliği Siber Güvenlik Politikası”, (Yüksek Lisans Tezi) Marmara Üniversitesi, 2021, s.15.

kadar gerekli olmuştur. Bu nedenle hakkında yazılan sosyal alana ilişkin metinler de bu teknik dili potası içinde eritmek durumunda kalmıştır. Yine de pek çok tanım üzerinde hatta siber güvenlik tanımı üzerinde dahi bir uzlaşma yahut kesinlik olduğunu, doğrudan bu konuda hazırlanmış yasalara bakarak bile bahsetmek mümkün görünmektedir⁴⁰.

Bu kapsamda, metinde faydalı olacağı öngörüldüğünden tanımların gruplandırılması ve sonrasında açıklamalarına hukuki yorum yapılabilecek derinlikte ve gereklilikte, dolayısıyla genel itibariyle değinilmesinin, teknik detaylara girilerek yanlış anlatımların önüne geçmesi, en azından kısıtlanması amaçlanmaktadır.

Siber güvenlik alanındaki yaklaşımlar ile yaşanan sorunlara çözüm arayışını konu alan metinlerin yalnızca mühendislik bilgisi ile çözüme kavuşamayacağı⁴¹ bu nedenle konunun teknik boyutu ve yönetişimine yönelik olarak ikiye ayrıldığını söylemek, oldukça fazla ve farklı alana temas eden bir alan olması sebebiyle tam bir bölünme için doğru olmayacaksa da çatı olarak kabul edilebilir⁴². Bu alanda çalışan insanların da kolaylıkla görebileceği üzere süreçlerin teknik olarak hazırlığının yapılması ve üstten bir bakış ile bir strateji ve plan hazırlanmasını gerektiren yönetişim kısmı birbirinin içinde ancak birbirinden ayrı profesyonellikler gerektiren hususlardır. Teknik kavramların bütün unsurları ile yönetişim metinlerinde yer alması mümkün olmayacaksa da bu kavramların temel ve ayırıcı özelliklerinin belirlenmesi ve anlaşılması şeklinde ilerlemek faydalı, aynı zamanda da kolaylaştırıcı olacaktır.

Teknik olarak tüm eylemlerin savunma ve saldırı başlıkları altında, bunların gerçekleştiği alana ise siber uzayda yer alan her bir katman olarak bir ayrıma gitmek en basit anlatım olarak kabul edilebilecektir. Katman kavramının, bu

⁴⁰ Jeff Kossef, "Defining Cybersecurity Law", Iowa Law Review, Cilt 103, No. 985, 2018, 985-1031, s. 986.

⁴¹ Salih Bıçakçı, "NATO'nun Gelişen Tehdit Algısı: 21.Yüzyılda Siber Güvenlik", Uluslararası İlişkiler Dergisi, Cilt: 10 Sayı: 40, 100 - 130, 01.03.2014, 102.

⁴² Çelik, 2018, s. 111.

satırların yazıldığı esnada gelinen son noktada bilinebilecek düzeydeki siber uzay mekanları, bahsedilen saldırıların, ya da saldırılardan koruma yöntemlerinin uygulandığı ortamlar olduğu söylenebilir. Bu kavramları hukuki olarak korunması arzu edilenler olarak kabul etmek de mümkündür. Saldırı ve savunma başlıkları ise kelimelerin temel anlamlarıyla ancak siber alanlarda yer alan halleriyle ele alındığında yapılacak gruplamaya ilişkindir. Netice itibarıyla tanımların anlaşılabilmesi ve gerekli şekilde kümelenebilmesi için her şeyden evvel siber güvenlik kavramının açıklanması ve ardından bu alana yönelik kavramların, zaman zaman birbiriyle yer değiştirse ve birbirinin içine geçse de savunma ile saldırı olarak kümelenmesinin faydalı olabileceği düşünülmüştür.

Siber güvenlik tanımı, internetin hayatımıza bu kadar sirayet etmediği ve dünyanın farklı yerlerindeki kişiler ile etkileşimin mümkün olmadığı 1980'lere kadar bilgisayar güvenliği olarak anılacak şekilde ve ancak dışarıdan bir müdahalenin verebileceği bir zarardan korunma yöntemi olarak var olmuştur⁴³. Dolayısıyla bu dönemde siber güvenlik yöntemleri de dışarıdan gelebilecek bir saldırının verebileceği zararlardan korunulabilmesine yönelik olacak şekilde kısıtlı bir gelişim göstermiştir. Siber güvenliğin, saldırı yöntemlerinin sınırlılığı nedeniyle gösterdiği kısıtlı gelişimin benzer şekilde saldırılar bakımından da ilk dönemlerde kısıtlı olduğunu söylemek yanlış olmayacaktır. 2000'li yılların başlaması ile internetin gelişimi ve yaygınlaşması saldırı yöntemlerinin ve dolayısıyla siber güvenlik risklerinin de değişimi ile gelişimine sebep olmuştur⁴⁴.

Açıklandığı üzere, internetin yaygın bir kullanım hacmine ulaşması ve artık insanların, kurumların, iletişimin ve birbiriyle etkileşimin doğal bir parçası haline gelmesi, bu alandan gelebilecek kazanımların yanında tehlikeleri de dönüştürmüştür. Bu nedenle, bilgi ve bilgi güvenliği ile veri ve siber güvenlik kavramlarının da derinleştirilmesi ve açıklanması değerlidir. Çoğu zaman aynı

⁴³ Bıçakcı, 2014, s. 106.

⁴⁴ Adish K. and Venkatesh, "A Review Paper on Cyber Security", International Journal of Advanced Research in Science, Communication and Technology (IJARSCT) 2. Kitap 2. Sayı, Mart 2022 s: 528.

anlama gelecek şekilde kullanılıyorlarsa da bilgi güvenliği ve siber güvenlik kavramları da birebir olarak aynı anlamları ifade etmemektedir.

Bu iki kavram arasındaki farkın incelenmesi adına, öncelikle veri ve bilgi kavramları ile işe başlanabilir. En temel haliyle veri, anlamlandırılmamış ve karar vermekte kullanılabilecek komut, olgu, sinyal, rakam ya da olay yığını olarak tanımlanabilir⁴⁵. Türk Dil Kurumu tarafından yapılan ve bilişim alanına özgülen tanımı ile ise veri “*Olgu, kavram veya komutların, iletişim, yorum ve işlem için elverişli biçimli gösterimi*”⁴⁶ anlamına gelmektedir. Verinin bilişim sistemleri ve dolayısıyla bilgisayarlar aracılığı ile depolanan birimler olduğu söylenmekteyse de⁴⁷ aksi şekilde bilişim sistemlerinin dışında yer alan sanat eserlerinin, bir bitkinin genomunun ya da bir şişe içeceğin dahi veri olarak kabul edileceği şeklinde farklı görüşler de mevcuttur⁴⁸. Bu husustaki tartışmalara girmeksizin, metaforik olarak verilerin dağınık halde bulunan kelimeler olduğunu söylemek de kavramı somutlaştırmak adına uygun olabilir.

Bilgi ise verinin anlamlandırılmış, karar vermekte kullanılabilir, olaylar ya da olgular arasında tutarlı ve kabul edilebilir ilişkiler kurulmuş haline verilecek isimdir⁴⁹. Yine Türk Dil Kurumu tarafından yapılan tanımı ile bilgi “*Verinin anlam kazanmış biçimi*”⁵⁰ olarak ifade edilmektedir. Veri ile alakalı verilen metafor üzerinden gidilecek olursa, bilginin, anlamlı bir şekilde sıralanmış kelimeler ile yapılan cümleler olduğunu söyleyebiliriz.

⁴⁵ Şeref Sağıroğlu, “Siber Güvenlik Ve Savunma: Önem, Tanımlar, Unsurlar Ve Önlemler, Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık”, 1. Baskı, Ankara, 2018, s: 22.

⁴⁶ Türk Dil Kurumu, <https://sozluk.gov.tr/>, (Son erişim tarihi : 20.04.2024)

⁴⁷ data **noun** : information, especially facts or numbers, collected to be examined and considered and used help decision making, or information in an electronic form that can be stored and used by a computer: The data was/were collected by various researchers. Now the data is/are being transferred from magnetic tape to hard disk, Link: <https://dictionary.cambridge.org/dictionary/english/data>. (Son erişim tarihi: 22.06.2024)

⁴⁸ University of York, “Data: a Practical Guide, What is data?” link: <https://subjectguides.york.ac.uk/data/lore> (Son erişim tarihi: 22.06.2024)

⁴⁹ Sağıroğlu, 2018, s. 22

⁵⁰ Türk Dil Kurumu, <https://sozluk.gov.tr/>, (Son erişim tarihi 22.06.2024)

Bilgi ve veri ile alakalı yapılan tanımların üzerine ise bilgi güvenliği ve siber güvenliği izah etmek daha kolay olacaktır. ENISA tarafından klasik bilgi güvenliği modelinin içinde bu gizlilik, bütünlük ve erişebilirlik kavramlarının yer alması gerektiği ve bilgi güvenliğinin siber güvenliğin bir alt kümesi olduğu işaret edilmiştir⁵¹. Bu değerlendirmede yer alan CIA üçlüsü olarak adlandırılan gizlilik, bütünlük ve erişebilirlik kavramlarının dışında, bilginin varlık olarak korunması amacıyla yapılan önlem girişimleri olarak anıldığı tanımlar da mevcuttur⁵². Neticesi itibariyle her iki tanım da aynı amaca hizmet ediyor olsa da, bilginin korunması beklenen varlık olarak ayrıca anılması ve daha somut bir ifade biçimi olması yönüyle birbirlerinden ayrılmaktadır. Kısaca bilgi güvenliğinin, bilişim sistemlerinde bulunan ve bilgilerin erişilebilir olması, gizli kalabilmesi ve bütünlüğünün korunması için alınan önlemler olduğu söylenebilir. Siber güvenlik konusunda ise ENISA'nın takip ettiği içerik siber olayların önlenmesi, tahmin edilmesi, tolerans gösterilmesi, tespit edilmesi, hafifletilmesi, ortadan kaldırılması, analiz edilmesi ve soruşturulmasının tüm yönlerini kapsamaktadır. Aynı zamanda siber güvenliğin bilgi güvenliğinin içeriklerinin de dahil olduğu kullanılabilirlik, güvenilirlik, emniyet, gizlilik, bütünlük, sürdürülebilirlik (somut sistemler, bilgiler ve ağlar için) sağlamlık, hayatta kalabilirlik, esneklik (siber alanın dinamikliğini desteklemek için), hesap verebilirlik, orijinallik ve inkar edilemezlik (bilgi güvenliğini desteklemek için) niteliklerini de taşıması gerektiği belirtilmiştir⁵³. ITU tarafından yapılan tanımında ise siber güvenlik pek çok aracı bulunan ve korunması amaçlanan araçların güvenliğinin sürdürülmesine ilişkin bir tanım yapmaktadır. İlgili tanıma göre siber güvenlik, siber ortamı⁵⁴ ve kuruluş ile kullanıcı varlıklarını korumak için kullanılabilecek araçlar, politikalar, güvenlik kavramları, güvenlik önlemleri, kılavuzlar, risk yönetimi yaklaşımları, eylemler, eğitimler, iyi uygulamalar örnekleri ile sağlanan güvence ve teknolojiler

⁵¹ ENISA, “Overview of cybersecurity and related terminology”, Versiyon 1, 2017, s.6.

⁵² Şeref Sağıroğlu, “Siber Güvenlik Ve Savunma Farkındalık ve Caydırıcılık”, Grafiker Yayınları, Ankara, 2018, s.26.

⁵³ ENISA, 2017, s.6.

⁵⁴ Uluslararası Telekomünikasyon Birliği tanımı ile siber Ortam: Kullanıcılar, ağlar, cihazlar, tüm yazılımlar ve süreçler dahildir, depolanan veya aktarılan bilgiler, uygulamalar, hizmetler ve doğrudan bağlanabilen sistemler veya dolaylı olarak ağları ifade etmektedir.

bütünü olup, varlıkların, bilgi işlem cihazlarının, kuruluşların personelinin, altyapısının, uygulamalarının, hizmetlerinin, telekomünikasyon sistemlerini ve siber ortamda iletilen ve/veya depolanan bilgilerin bütünü, ilgili güvenlik risklerine karşı bunların güvenliğinin devamlılığını sağlama çalışması olarak ifade edilmiştir. Bunun yanında siber güvenliğin güvenlik hedefleri, erişilebilirlik, gizlilik ve bütünlük olarak sayılmıştır⁵⁵. Aslında siber güvenliğin, korumakla yükümlü olabileceği sistemler, veri üretilebilmesi, depolayabilmesi ya da kullanabilmesi mümkün sistem sayısı kadar geniş bir alanda var olabileceğini ve bu alanlardan birinin de en temel ve yaygın veri işleme aracı olan bilgisayar ya da benzeri şekilde bilgi üretimi, kullanımı ya da depolanmasına imkân tanıyan bilişim aracını içerir bir üst kavram olduğunu söylemek mümkündür. Bilgiyi var eden veriyi koruma ve güvenliğini sağlama amacı güden siber güvenlik doğası gereği veriden üretilmiş bilgiyi de koruyan bir çerçeveye sahiptir.

2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar, Türkiye’de yapılan ve siber güvenlik kavramının konu edildiği önemli metinlerden biridir. İlgili Kararın, Tanımlar ve Kısaltmalar başlıklı 2. Maddesinin c bendinde yer aldığı hali ile *“Ulusal Siber Güvenlik: Bilgi ve iletişim teknolojileri vasıtasıyla sağlanan her türlü hizmet, işlem ve veri ile bunların sunumunda yer alan sistemlerin güvenliğini, ifade eder.”* Şeklinde dir. Bu metnin sonrasında yapılan çalışmalar neticesinde Ulaştırma Bakanlığı tarafından hazırlanan Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı’nda “siber ortam, ulusal siber ortam, siber güvenlik ve ulusal siber güvenliğin” de dahil olduğu konuya ilişkin tanımlar yapılmıştır. İlgili metinde,

“Siber ortam: Tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan ortamı,

⁵⁵ Uluslararası Telekomünikasyon Birliği , “ITU-T X-Series Recommendations: Data Networks, Open System Communications And Security, Telecommunication security, Overview of cybersecurity”, 2008, s.6.

Ulusal siber ortam: Kamu bilişim sistemleri ile gerçek ve tüzel kişilere ait bilişim sistemlerinden oluşan ortamı,

Siber güvenlik: Siber ortamı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilginin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber güvenlik olaylarının tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesini,

Ulusal siber güvenlik: Ulusal siber ortamda bilgi ve iletişim teknolojileri vasıtasıyla sağlanan her türlü hizmet, işlem ve verinin ve bunların sunumunda yer alan sistemlerin siber güvenliğini,” şeklinde tanımlanmıştır. Bir sonraki dönem olan 2016-2019 yıllarına ilişkin hazırlanmış düzenlenen Ulusal Siber Güvenlik Stratejisi ve Eylem Planı’nda ise önceki Eylem Planı’nda yer alan siber ortam tanımı “siber uzay” olacak şekilde, ulusal siber ortam tanımı ise “ulusal siber uzay” olarak yer almış ancak tanımlara ilişkin açıklamalar aynı şekilde kalmıştır.

2013-2014 yılı Eylem Planı’nda yer alan siber güvenlik tanımı ile ulusal siber güvenlik tanımı ise 2016-2019 Eylem Planı içinde daha farklı şekilde yer bulmuştur. 2016-2019 Eylem Planı’nda siber güvenlik tanımı “*Siber güvenlik: Siber uzayı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilgi/verinin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber güvenlik olaylarının tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesini*” şeklinde yer almıştır. İlk etapta büyük bir farklılık olmadığı düşünülecekse de gizlilik, bütünlük ve erişilebilirliğinin korunması beklenen varlık, yeni metinde yalnızca bilgi değil bilgi ve veri şeklinde belirlenmiştir. Ulusal siber güvenlik tanımı da 2016-2019 tarihli Eylem Planı’nda “*Ulusal siber güvenlik: Ulusal siber uzayı oluşturan bilgi ve iletişim teknolojileri vasıtasıyla sağlanan her türlü hizmet, işlem, bilgi/verinin ve bunların sunumunda yer alan*

donanım ve yazılım sistemlerinin ulusal ölçekte sağlanan siber güvenliğini” ifade edecek şekilde yer almıştır. Öncelikle ulusal siber güvenlik tanımında, siber ortam yerine siber uzay kavramı dahil edilmiş ve siber güvenlik ile paralel şekilde yalnızca bilginin değil bilgi ile verinin de ulusal siber güvenliğe dahil edilmesi sağlanmıştır.

Ulaştırma Bakanlığı tarafından yayımlanan Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023 Tanımlar kısmında ise diğer Eylem Planlarından farklı olarak *“Bilgi Güvenliği: Bilişim sistemlerinin ve bilgilerin izinsiz kullanımını, yetkisiz kişilerce erişilmesini ve ifşa edilmesini, silinmesini, değiştirilmesini ve zarar görmesini, engellemek, bu sistem ve bilgilere yetkili kişiler ve işlemlerin ihtiyaç duyulan zamanda ve kalitede erişilmesini sağlamak için yürütülen faaliyetler bütünü.”* Şeklinde bilgi güvenliği ve ayrıca *“Siber Güvenlik: Siber uzayı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilginin/verinin gizliliği, bütünlüğü ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber olayların tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber olay öncesi durumlarına geri döndürülmesini kapsayan faaliyetler bütünü.”* Şeklinde siber güvenlik tanımı ayrı ayrı yer almıştır. Yapılan bu son düzenleme ile de siber güvenlik ile bilgi güvenliğinin farkı da ortaya konulmuştur.

İlgili tanımlardan da görüleceği üzere bilgi güvenliği ve siber güvenlik farklı amaçlara hizmet eden ancak birbiriyle etkileşim içinde olan ve birbirlerini kapsayan-kapsanan olarak tamamlanabilecek kavramlardır. 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı içinde yer alan halleriyle ele alındığını aşağıdaki tabloda ilgili kavramların içeriği daha net bir şekilde ortaya konulmaktadır.

Tablo 2. 1. 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı İçinde Yer Alan “Bilgi Güvenliği” Ve “Siber Güvenlik” Kavramı

	Bilgi Güvenliği	Siber Güvenlik
Konusu	<i>Bilişim sistemlerinin ve bilgilerin</i>	<i>Siber uzayı oluşturan bilişim sistemlerinin</i>
Amacı	<i>yetkisiz kişilerce erişilmesini ve ifşa edilmesini, silinmesini, değiştirilmesini ve zarar görmesini, engellemek, bu sistem ve bilgilere yetkili kişiler ve işlemlerin ihtiyaç duyulan zamanda ve kalitede erişebilmesini sağlamak için</i>	<i>Saldırılardan korunmasını, bu ortamda işlenen bilginin/verinin gizliliği, bütünlüğü ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber olayların tespit edilmesini,</i>
Yöntemi	<i>yürütülen faaliyetler bütünü.</i>	<i>bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber olay öncesi durumlarına geri döndürülmesini kapsayan faaliyetler bütünü.</i>

Görüleceği üzere siber güvenlik, bilgi güvenliğini de bünyesine dahil etmiş ve kapsayıcı bir yaklaşımla bilişim sistemlerinin kurulması amacının dışında herhangi bir etki yaratacak, sistemlerin içeriklerini herhangi bir şekilde ve amacı dışında dışarıya taşıyabilecek ya da bütünlüğünü bozabilecek her türlü etkiden korunmasını ve eğer bunun aksi bir olay yaşanırsa, sistemin en baştaki çalışma prensibine uygun şekilde eski haline dönmesini amaçlar şekilde tanımlanmıştır. Tanımın içeriğinde de görüleceği üzere siber güvenlik doğası gereği bir saldırı ve buna karşı geliştirilen bir savunmanın bileşim kümesi olarak varlık göstermektedir. Siber savunmanın, siber güvenlikten ayrılan ve bir alt başlık olarak alınmasına sebep olan yönünün herhangi bir saldırı ortaya çıktığında ve barış şartları altında değilken etkinlik kazanan tedbirler olması⁵⁶, siber saldırının ise belirli bir varlığın bütünlüğünü korumak için değil kendinden başkaca bir hedefe⁵⁷ yönelik planlanıyor ve zarar verme motivasyonu içeriyor olması gösterilebilir. Bu kavramlara nelerin dahil edildiğini biliyor olmak da teknik bir olay karşısında eylemin ve sorumluluğun tespiti bakımından önem arz edebilecektir. Bu hususta her bir kavramın tanım olarak açıklamalarından ziyade ilgili kavramların listelenmesi ile yetinilip, kategorisinin anlaşılması adına sıralanması uygun olacaktır.

Siber savunma yöntemleri

Ağ Bölümlendirme	Zafiyet Taraması	Yığın İleti Engelleme Sistemi (Anti Spam)
Güvenlik Duvarı	Steganografi	İçerik Filtreleme Sistemi
Veri Kaçağı Önleme	Penetrasyon Testi	Hava Boşluğu Sistemi
Yük Dengeleme	Ağ Erişim Kontrolü	Uç Nokta Güvenliği Sistemi
Balküpu	Güvenlik Bilgi ve Olay Yönetimi Sistemleri	Şifreleme (Kriptografi)

⁵⁶ Barış Çeliktaş, “Siber Güvenlik Kavramının Gelişimi Ve Türkiye Özelinde Bir Değerlendirme” (Yüksek Lisans Tezi) Karadeniz Teknik Üniversitesi, 2016, s. 22.

⁵⁷ Tayfun Acarer, “ Ülke Güvenliğimizde Alınabilecek Makro Siber Güvenlik Önlemleri”, Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, Cilt:6, No:2, S:61-71, 2020, s.62.

Antivirüs	Çoklu Faktörlü Kimlik Doğrulama	Elektronik İmza - Sayısal İmza
Uç Nokta Güvenliği	Zaafiyet tarama araçları	Elektromanyetik Güvenlik

Siber saldırı yöntemleri

Yetki Arttırımı	Zaafiyet Tarama Araçları	İstem dışı yığın ileti
Mantık Bombası	Sosyal Mühendislik	Arka kapı kullanımı
Solucanlar	Spam mail	IP Gizleme
Botnetler	Şebeke T trafiğinin Dinlenmesi	Açık mikrofon dinleme
Truva Atı	Kriptografik Saldırıları	Oturum çalma
Virüsler	Casus Yazılımı	Sıfır gün saldırısı
Kök Kullanıcı Takımı (Rootkit)	Reklam Yazılımı	Yemleme/Oltalama
DDoS Saldırıları	Ortakdaki Adam Saldırıları	

Sayılanların yanında da pek çok yöntem bulunmakta olup ilgili saldırı ve savunma yöntemleri dışında siber ile başlayan pek çok kavram bulunmaktadır. Siber hijyen, siber tehdit, siber esneklik, siber savaş, siber terörizm, siber suç, siber casusluk/istihbarat, siber etik gibi kavramlar saldırı ve savunma yöntemlerinin dışında ancak daha farklı dinamiklere sahip kavramlar olarak kabul edilebilir. Siber uzayın yayılması ve bünyesinde barındırdığı ilişkilerin çeşitlenmesiyle birlikte ortaya çıkan sorunlar, çözüm yöntemleri yanı sıra ortaya çıkan ihtiyaçlar, hakkında yapılan çalışmalar ve değerlendirmeler de gelişmekte, dolayısıyla üretilen kavramlar da kavramlar da artış göstermektedir.

Siber uzayda gelişen olaylara ilişkin kavramların görece yeni olması, gelişen teknoloji ile siber ortama taşınan hizmet ürün sayısının artması ile çoğalan hukuki ilişkiler neticesinde saldırı ve savunma çeşitlerinin de gelişim gösteriyor olması ilgili yükümlülükler ve sorumluluğun belirlenmesinde kafa karıştırıcı

olmaktadır. Bu açıdan her ne kadar zor olsa da özellikle hukuki olarak siber güvenlik tanımının yapılması hem hukuki ilişkilerin tespitinde hem de bu ilişkilere yönelik sorumluluğun belirlenmesinde yardımcı olacaktır. Farklı disiplinlerdeki odak noktasına ve farklı ihtiyaçlara göre şekillenen tanımların yerine siber güvenlik ile neyin güvenliğinin, nerede ve kimin güvenliğinin, ne şekilde, ne zaman ve neden güvence altına alındığının belirlenmesi kavramın içinin doldurulmasına da yardımcı olabilecektir⁵⁸.

2.2. ELEKTRİK PİYASASINDA YAŞANAN SİBER TEHDİTLERİN TÜRLERİ VE ETKİLERİ

Güvenlik denildiğinde tehlikelerin gelebileceği tarafın hep dışarıdan olduğunu düşünür ve bu girişleri engellemek üzere sistemleri geliştirmeye çabalarız. Siber güvenlik anlayışında da bu durum Stuxnet saldırısına⁵⁹ kadar aynı şekilde devam etmiştir. Ancak bu tecrübeden de edinilen deneyim neticesinde görüleceği üzere, siber uzayda var olan etkileşim ve erişim noktası kadar saldırıya açık alan ve dolayısıyla güvenlik ihtiyacını karşılayacak savunma yöntemine ihtiyaç bulunmaktadır. Bu olayın da gösterdiği üzere dış dünya ile bağı olsun olmasın, sistem ve hatta bağlantı sayısı kadar siber saldırıya açık kapı ve dolayısıyla savunulması gereken alan bulunmaktadır. Elektrik piyasasının merkezi konumu ve etkileşim içinde olduğu tarafların fazlalığı düşünüldüğünde ise hem saldırıya açıklık hem de etki alanı itibarıyla oldukça hassas bir noktada durduğu söylenebilir.

⁵⁸ Kossef, 2018, s.994.

⁵⁹ Stuxnet saldırısı, İran'ın nükleer programını hedef alan bir siber saldırı olarak 2005-2010 yılları arasında geliştirilmiş olup, ilk kez 2009'un sonlarında keşfedilmiştir. Bu karmaşık saldırının etkisi ise 2010 yılında anlaşılmıştır. Saldırı yöntemleri arasında, USB bellek yoluyla yayılma, yerel ağ sızması, sistemleri hedef alma ve kontrol etme, yapılandırılmış kod yürütme gibi teknikler kullanılan saldırının kapalı devre bilgisayar sistemlerine USB bellekler aracılığıyla sızdığı, yerel ağa yerleştikten sonra hedef sistemlere bulaştığı bilinmektedir. Endüstriyel kontrol sistemlerini hedef alarak nükleer santrifüjleri etkileyen saldırı sayesinde endüstriyel ekipmanlarının, yetkili kullanıcı komutlarından farklı ve istenmeyen şekilde kontrol edebilmesine imkan sağlamıştır. Stuxnet saldırısı, gerek kapalı devre sistemlere giriş yapmış olması gerekse de endüstriyel kontrol sistemlerini hedef almasıyla siber güvenlikte yeni bir dönemin başlangıcını işaret eden ve uluslararası politika, endüstriyel güvenlik ve siber savunma stratejileri üzerinde önemli etkileri olan bir olaydır.

Günümüz dünyasında elektrik, kullanım alanı itibariyle modern toplumun yaşamından çıkarmayı düşünemeyeceği kadar yerleşik ve hayati bir meta olarak varlığını sürdürmektedir. Kritik alt yapı olduğu kabul edilen, finans, sağlık, kamu hizmetleri, elektronik haberleşme, su yönetimi gibi sektörlerin, asgari düzeyde dahi çalışmalarına devam edebilmesi açısından elektrik vazgeçilmez bir unsurdur. İletişim, ulaşım ve beslenme gibi en temel ihtiyaçların da günümüz yaşam koşulları gereği elektrik olmaksızın mümkün olamayacağını, en azından büyük ölçüde sekteye uğrayacağını öngörmek zor olmayacaktır. Evrensel hizmet tanımı içinde yer alan faaliyetler⁶⁰ de dahil olmak üzere pek çok hizmet ve ürünün elektrik olmaksızın sağlanabilmesi mümkün değildir. Bu etki ve önemi göz önünde bulundurularak elektrik de dahil olmak üzere enerjiye erişim kavramının, temel insan hakkı şeklinde kabulüne ilişkin tartışmalar da hukuk dünyasındaki önemli gündem konularından biridir⁶¹. Enerji ve bir adım ilerisinde elektriğe erişimin önemi ve bu alanda yaşanan aksaklıkların yarattığı etki incelendiğinde, temel insan hakkı olmasına sebep tartışmaların kaynağı çok daha kolay bir şekilde anlaşılabilir.

2012 yılında Hindistan’da, aynı anda etkilenen insan sayısı itibariyle zamanına kadar yaşanan en büyük kabul edilen elektrik kesinti nedeniyle ortaya çıkan zarar, sosyal ve ekonomik olarak bir kaosla eşdeğer olmuştur. 30 Temmuz 2012 tarihinde Hindistan’da ayrı alt yapılar olarak faaliyet gösteren, 5 elektrik bölgesinden biri olan kuzey bölgesinde yaşanan elektrik kesintisinin, en basit anlatımıyla arzın aşırı talep karşısında dengelemeyi yapamamış olmasından

⁶⁰ 5369 Evrensel Hizmet Kanunu, Evrensel hizmetin kapsamı Madde 5 Evrensel hizmet;

a) Sabit telefon hizmetlerini,

b) Ankesörlü telefon hizmetlerini,

c) Basılı veya elektronik ortamda sunulacak telefon rehber hizmetlerini,

d) Acil yardım çağrıları hizmetlerini,

e) İnternet hizmetlerini,

f) Ulaşımı deniz yoluyla sağlanabilen yerleşim alanlarına yolcu taşıma hizmetlerini,

g) Deniz haberleşmesi ve seyir güvenliği haberleşme hizmetlerini,

Kapsar.. Evrensel hizmetin kapsamı; ülkenin sosyal, kültürel, ekonomik ve teknolojik şartları da göz önünde bulundurularak, üç yılı aşmamak üzere belirli aralıklarla, Cumhurbaşkanınca yeniden belirlenebilir.

⁶¹ Pınar Aksakal Aydın, “İnsan Hakları Açısından Enerjiye Erişim Kavramı, Birleşmiş Milletler ve Bölgesel Düzenlemeler Açısından Enerjiye Erişim Kavramı”, (Yüksek Lisans Tezi) İstanbul Bilgi Üniversitesi, 2020, S:53.

kaynaklandığı tespitinde bulunulmuştur⁶². Yaşanan kesintinin giderildiği düşünülürken, bir gün sonra yani 31 Temmuz 2012 tarihinde gerçekleşen ikinci kesinti ile birlikte Hindistan'da dünya nüfusunun yaklaşık % 10'una karşılık gelecek 680⁶³ milyon insan elektriğe erişim sıkıntısı yaşamıştır. Etkilenen insan sayısı tespiti, bölgede yaşayan insan sayısına göre yapılmış olup, kesintiden elektrik aboneleri yani müşteri olarak etkilenen insanların yarısına yakınının (323 milyon) elektrik aboneliği olmadığı belirtilmiştir⁶⁴. Yayımlanan haberlere göre uzmanlar, kesintinin temel nedeninin yetersiz yatırımlardan, ülke yönetiminin hatalı enerji politikalarından kaynaklandığını belirterek, yaşanan olayın belirtilerinin yıllardır ihmal edildiğini vurgulamışlardır. Olay sonrasında hazırlanan rapor içerisinde de uzman görüşleri ile paralel hususlar yer almaktadır. Akıllara Hindistan'a zarar vermeyi amaçlayan bir siber saldırı ihtimali hemen gelse de aynı raporda nedenler arasında siber saldırı ihtimalinin kesinlikle yer almadığı özellikle vurgulanmıştır⁶⁵.

Hindistan'ın 28 eyaletinin 20'sini kapsayan kesintinin gerçekleşmesiyle birlikte tren seferleri durmuş, madenlerde çalışanlar mahsur kalmış, pek çok hastane ve tesis hizmet veremez hale gelmiştir. Su tesisatının işlemesine kaynaklık eden elektriğin de kesilmesi ile günlük yaşantıda temel ihtiyaçların giderilmesine yönelik olarak önemli sorunlar yaşanmıştır. Büyük sanayi şirketleri ve havaalanları sahip oldukları jeneratörler sayesinde işlevlerini kısıtlı olarak sürdürebilmişlerse de jeneratörü olmayan ulaşım araçları ile ticari işletmelerin çalışması kesintiye uğramıştır⁶⁶.

⁶² The theme of this issue is India's major electricity supply outage that occurred in July 2012, ESI Bulletin on Energy Trends and Development (Volume 5 / Issue 4 • March 2013)

⁶³ Helen Pidd, India blackouts leave 700 million without power, The Guardian link: <https://www.theguardian.com/world/2012/jul/31/india-blackout-electricity-power-cuts> (Son erişim tarihi: 22.06.2024)

⁶⁴ Power Technology, 2015

⁶⁵ Penna Electric, Top 5 Of The World's Biggest Power Outages, Link: <https://www.pennaelectric.com/top-5-of-the-worlds-biggest-power-outages/> (Son erişim tarihi: 22.06.2024)

⁶⁶ Roger Cormier, The 12 Biggest Blackouts In History, link: <https://www.mentalfloss.com/article/57769/12-biggest-electrical-blackouts-history> (Son erişim tarihi: 22.06.2024)

Kesintiden sonra yapılan tespitlere göre kesintinin gerçekleştiği dönemde, bölgenin hava şartları için önemli bir etken sayılabilecek muson yağmurlarının, normal iklim koşullarına uygun olacak şekilde bir yağış grafiği izlememiş olmasının hava sıcaklığını arttırdığı, bunun sonucunda artan soğutma sistemleri kullanımı nedeniyle Kuzey Eyaletleri tarafından aşırı elektrik talebinin, Batı Eyaletleri tarafından aşırı elektrik arzı ile gidilerilmesine çalışırken bakım, yatırım eksiklikleri gibi faktörlerin birleşip hali hazırda yetersiz olan elektrik şebekesinin çökmesine neden olduğu tespitinde bulunulmuştur ⁶⁷ . Doğal nedenler kaynaklanıyor olsa bile gerek ülke içinde gerekse ülke dışında etkileri olan bu durum, Hindistan'nın uluslararası ekonomide kredibilitesine dahi zarar vermiş⁶⁸, hakkında olumsuz görüşlerin oluşmasına sebep olmuştur. Her ne kadar tarihte en fazla insanı etkileyen elektrik kesintisi olarak anılsa da sık sık kesintilerin yaşadığı ülkede, devamlı hale gelen bu durumun, belirli sektörlerin çalışmalarına olan etkileri üzerinden yapılan hesaplamalarda, ülkenin gayi safi milli yurt içi hasılasının %5'i⁶⁹ oranında bir zarar verdiği espit edilmiştir. Hızlı nüfus artışının yani sıra sanayileşme konusunda önemli adımlar atan ülkelerden biri olarak ,yaşanan elektrik kesintilerini önlemek adına adımların atılması gerektiği açıkça görülmektedir.

Elektrik arzının kesintiye uğramasının arkasında pek çok etken bulunuyor olsa da siber güvenlik son dönemlerde kaçınılması en önemli tehditlerden biri haline gelmiştir. Zira, bu denli önemli bir varlığın, zarar görmesi ya da erişilemez hale gelmesinin etkileri de kullanım alanı ile orantılı şekilde hayli tahrip edici olabilmektedir.

⁶⁷ Anubhav Ratha, "India's Blackouts of July 2012: What Happened and Why?", Ulusal Singapur Üniversitesi, Enerji Araştırmaları Enstitüsü, Enerji Trendleri ve Gelişmeleri Bülteni, Cilt 5, Sayı 4, Mart 2013, 2-5, s.3-4.

⁶⁸ The Economic Times Industry, Power outages have negative impact on Indian economy: Moody's link: <https://economictimes.indiatimes.com/industry/energy/power/power-outages-have-negative-impact-on-indian-economy-moodys/articleshow/15328536.cms> (Son erişim tarihi: 22.06.2024)

⁶⁹ Anwar Shahzad Siddiqui, Abrar Ahmad, Ahraz Athar, Economic Impact Of Power Outage on GDP of India, International Journal of Engineering Technology, Management and Applied Sciences, 2015, Mart syf: 162

Birleşmiş Milletler'in, Uluslararası Telekomünikasyon Birliği (International Telecommunication Union) tarafından 2020 yılı için hazırlanmış Global Siber Güvenlik İndeksi'nde, siber güvenlik stratejileri açısından net bir çerçeveye ihtiyaç duyan kritik alt yapılara yönelik herhangi bir riskin gerçekleşmesi halinde ortaya çıkacak zarar, ülke için oldukça büyük olacağından kritik altyapılarda olabilecek bir siber saldırının, olasılığının dahi düşürülmesi gerektiğinin altı çizilmiştir⁷⁰. Sürdürülebilir Kalkınma Hederlerinden insana yakışır iş ve ekonomik büyüme, sanayi, yenilikçilik ve altyapı, eşitsizliklerin azaltması bağlamında da⁷¹ siber güvenlik kapasitesinin geliştirilmesi gerektiğini belirten Global Siber Güvenlik İndeksi'nde, bu kapasitenin gelişmişliğini ölçmek için hazırlanmış soruların bir kısmı yasal olgunluk düzeyini tespit etmeye yöneliktir⁷². Bu minvalde, gerek devletlerin siber güvenlik alanına ilişkin sorumluluklarının belirlenmesi, gerekse de siber saldırılar nedeniyle zarar görenlerin haklarının korunması açısından yasal düzenlemelerin eksiksiz ve kapsayıcı bir şekilde yapılması, ertelenmemesi gereken bir görevdir. Ülkeler arasında dahi bir üstünlük ve tahakküm altına alma yöntemi olarak kullanılan siber saldırıların yarattığı etkilere ilişkin önemli örneklerden biri de Ukrayna'da gözlemlenmiştir.

2014 yılından bu yana devam eden Rusya ve Ukrayna arasında yaşanan gerilimler ve siber uzaya da yansımış düzensiz misillemeler devam etmektedir. Arkasında Rusya'nın olduğu kesin şekilde ispatlanamış olsa dahi Ukrayna'ya oldukça zarar veren misillemelerden bir tanesi ise 2015 yılının aralık ayında gerçekleşmiştir. Ukrayna'da yaklaşık 225.000 kişiyi etkilemiş, bazı bölgelerde 1, bazılarında 6 saate kadar uzayan elektrik kesintilerine sebep olmuş siber saldırının arkasında, Rusya'nın askeri siber istihbarat teşkilatına bağlı olarak çalışan Sandworm isimli grup tarafından gerçekleştirildiğine inanan kesimler

⁷⁰ International Telecommunication Union, Global Cybersecurity Index 2020, s: 9.

⁷¹ age, s: 24.

⁷² age, s: 138.

bulunmaktadır⁷³. Zamanına kadar resmi olarak elektrik altyapısına yapılan ilk siber saldırı olma özelliğini taşıyan bu olayda⁷⁴, hackerlerin Black Energy 3 adıyla anılan zararlı bir yazılım aracılığıyla ve hayli karmaşık yöntemler kullanarak elektrik altyapısına zarar vermiş olduğu, ABD Siber Güvenlik ve Altyapı Güvenliği Ajansı yetkililikleri tarafından yapılan duyuruda açıklanmıştır⁷⁵.

İlgili siber saldırıdan sonra yapılan incelemeye göre, oldukça kapsamlı bir şekilde saldırının kurgulandığı⁷⁶ ortaya çıkmış olup, lokasyon, aksiyon, zaman, dilimi, cihaz/uygulama, altyapı içindeki rolü, sömürü metodu, etkisini tespit ederek saldırının incelenmesi neticesinde, aşağıda verilen 17 adımın takip edildiği ve oldukça detaylı bir planın ürünü olduğu görülmektedir. Saldırının ilk aşamalarının, 2014 yılının mayıs ayından da öncesine dayandığını belirten rapora göre izlenen adımlar aşağıdaki gibidir.

1. Keşif ve istihbarat toplanması; açık kaynaklar üzerinden sistem ve kullanıcıları hakkında bilgi toplama ve hazırlık yapma anlamına gelmektedir.
2. Kötü amaçlı yazılım geliştirme ve silahlandırma; keşif aşamasında temin edilen bilgilere uygun şekilde, Black Energy 3 adı verilen zararlı yazılımın ve uzaktan erişim araçlarının geliştirmesi aşamasıdır.
3. Zararlı uzaktan erişim yazılımlarının (Remote Access Trojan-RAT) iletilmesi; şirket içinde kullanılan ve daha evvel istihbaratı yapılmış e-posta adreslerine oltalama e-postaları ile Microsoft uygulaması

⁷³ John Hultquist, “Sandworm Team And The Ukrainian Power Authority Attacks”, Link: <https://www.mandiant.com/resources/blog/ukraine-and-sandworm-team> (Son erişim tarihi 22.06.2024).

⁷⁴ Brazilya’da 2012 yılında yaşanan elektrik kesintisinin ilk etapta siber saldırı kaynaklı olduğu belirtilmişse de sonrasında bu iddianın doğru olmadığına yönelik açıklamalar da yapılmıştır.

⁷⁵ Cybersecurity & Infrastructure Security Agency, “Cyber-Attack Against Ukrainian Critical Infrastructure”, 2021, link : <https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01> (Son erişim tarihi: 22.06.2024)

⁷⁶ Booz Allen Hamilton, “When the Lights Went Out – A comprehensive review of the 2015 cyber on the Ukrainian critical infrastructure” 2016, s:3

dosyalarına gizlenmiş uzaktan erişim imkânı veren zararlı yazılımların iletilmesidir.

4. Zararlı uzaktan erişim yazılımlarının kurulması; çalışanların bilgisayarlarında Microsoft uygulamalarını kullanmaları sayesinde, zararlı yazılımlar içeren Microsoft dosyaları aracılığı ile Black Energy 3 isimli zararlı yazılımın sistemlere kurulmasıdır.
5. Komuta ve kontrol sunucusunun kurulması; kötü amaçlı yazılımı hazırlayanların, erişmiş olduğu cihazlarla iletişim kurarak saldırganlara kontrol ve erişim sağlaması ve bu sunucu sayesinde saldırganların kötü amaçlı yazılımı güncellemelerini, yeni talimatlar vermesini veya çalınan bilgileri almasını sağlar.
6. Kötü amaçlı yazılıma eklentilerin iletilmesi; sistemlerde bulunan Black Energy 3'un işlevlerine ek olarak kimlik bilgisi toplama ve dahili ağ keşfi sağlayacak nitelikteki yazılımların aktarılmasını tesis eder.
7. Kimlik bilgilerinin toplanması; sistem yöneticisi olarak giriş sağlayan kişilerin klavye hareketlerinin kaydı gibi yöntemlerle sistem içindeki kullanıcı bilgilerinin temin edilmesi ile sonrasında sistemlere giriş yapmak üzere saklanmasıdır.
8. Kurumsal ağ üzerinde potansiyel hedefleri keşfetme; kesintisiz güç kaynağı, veri merkezine ait sunucular, telefon hizmetleri merkezi gibi kritik ve zarar verilmesi hedeflenen kurumsal sistemlerinin keşfedilmesi aşamasıdır.
9. Endüstriyel Kontrol Sistemleri- EKS (Industrial Control System-ICS) ağında keşif ve hedef belirleme; endüstriyel işletmelerde üretim ve işletme süreçlerini otomatikleştirmek, izleme ve kontrol etme için kullanılan bir dizi bilgisayarlı sistem ve cihazlar bütünü olan EKS ve bağlı bulunan

HMI, DMS, RTU, UPS⁷⁷ gibi yerler üzerinde incelemeler yaparak kritik alanların ve saldırının yönteminin belirlenmesi amacıyla bilgi toplanmasıdır.

10. Kötü amaçlı aygıt yazılımı geliştirme; ilgili sistemlere giriş kanallarının keşfinden sonra sistemlere zarar vermek ya da tahrip etmek, dışarıdan komutlar vererek beklenmedik kötücül etkiler yaratmak üzere zararlı yazılımların sistem içinde hedeflenen ağlardaki etkinliğini geliştirme sürecidir.
11. Veri imhası için kötü amaçlı yazılımları yüklemek; sistem işleyişine erişim ile veri silinmesine ilişkin komutların hazırlanması ve bu verilere dayalı çalışan sistemlerin çalışamaz hale gelmesine sebep verilmesidir.
12. Kesintisiz güç kaynağı kesintisinin planlanması; Endüstriyel kontrol sistemlerinin devamlı ve kesintisiz çalışabilmesi müşterileri ile gerekli koordinasyon ekipleriyle iletişimini de mümkün kulan telekomünikasyon sistemleri ile veri sunucularına bağlı bulunan kesintisiz güç kaynaklarının işlevsiz hale getirilmesidir.
13. Açma-kapama şalterlerine müdahale; elektrik devrelerinde aşırı akım veya kısa devre gibi tehlikeli durumları algılayarak takip eden, elektrik akımını kesen ve böylece güvenliği sağlayan koruyucu cihazların devreden çıkarılmasıdır.
14. Saha cihazlarıyla bağlantıyı kesme; açma-kapama sistemlerine yapılan müdahalenin giderilebilmesi için saha ile yapılan iletişimi kuran sistemlerle iletişimin kesilmesidir.

⁷⁷ HMI (Human-Machine Interface) İnsan-Makine Arayüzü: Human Machine Interface / Makine ile İnsan Arasında Bilgi Aktarımı Sağlayan Arayüz, DMS (Distribution Management System) Dağıtım Yönetim Sistemi, RTU (Remote Terminal Unit) Uzak Terminal Ünitesi, UPS (Uninterruptible Power Supply) Kesintisiz Güç Kaynağı, Bilgi ve İletim Rehberi, s.6.

15. Telekomünikasyon hizmeti engelleme saldırısı; müşterilerin şirkete ulaşması ve bildirimlerde bulunabilmesinin engellenmesidir.
16. Kesintisiz güç kaynağı ile sistemin ayağa kaldırılmasının engellenmesi; daha evvel planlanan kesintisiz güç kaynaklarının sistemi yeniden ayağa kaldırabilmesi için bağlanmasının engellenmesi sürecidir.
17. Kritik sistem verilerinin yok edilmesi; sistemlerin eski haline döndürülebilme için ihtiyaç duyulan yedek veri setlerinin yok edilmesidir.

Ukrayna’da bulunan ve elektrik altyapısının kontrolü ile işletilmesinde kullanılan endüstriyel altyapı sistemine büyük zarar vermiş siber saldırının, sistemli ve uzun bir süre çeşitli aksiyonların alınması şeklinde bir plan üzerine inşa edilmiş olduğu görülmektedir. Birden fazla yöntemin adım adım işletilmesi sonucu büyük bir kitleyi etkileyen ve günün büyük bir kısmında elektrik kesintisi yaratan bu saldırıdan pek çok kişi ve işletme zarar görmüştür. Saldırının tespit edilmesinden ve elektrik altyapısının ayağa kaldırılmasından sonra dahi, endüstriyel kontrol operatörleri tarafından önceye nazaran çok daha sık pek çok yeni saldırı bildiriminde de bulunulmuştur⁷⁸.

Bu kapsamlı ve etkili siber saldırının, enterkoneksiyon nedeniyle Avrupa yahut farklı ülkeleri etkilemesinden de ayrıca endişe edilmiştir. Bu endişeler yersiz olmamakla birlikte, önlenbilmesi adına gerçekçi ve bütüncül adımların atılması da bir gerekliliktir. Özellikle elektrik şebekelerinin enterkoneksiyon sistemleri ile birbirlerine bağlantılı hale gelmiş olması tehlikenin boyutlarının de genişlemesine kaynaklık etmektedir. Farklı coğrafi bölgelerdeki elektrik şebekeleri arasında güç paylaşımı yaratmak, elektrik kesintileri esnasında bir bölgenin elektrik talebinin diğer bölgelerden gelen fazla güçle karşılanmasının sağlanması, enerji ticareti gerçekleştirmek ve daha geniş bölgelerde arz talep dengesini verimli şekilde dengeleyebilmek, acil durumlarda veya ani talep artışlarında ek kapasite sağlanmasında kolaylık yaratmak, yenilenebilir enerjinin

⁷⁸ Booz Allen Hamilton, 2016 s.3

verimli kullanımını desteklemek gibi pek çok önemli amaca hizmet etmek üzere kurulmuş enterkoneksiyon sistemleri, tıpkı enerjinin taşınmasına aracılık ettiği gibi siber saldırıların da taşınmasına aracılık edebilir. Enerji güvenliği ve sürdürülebilirliğinin sağlanmasının yanı sıra, elektrik endüstrisinin verimliliğinin artırılmasında da önemli bir rolü olan enterkoneksiyon sistemlerinin siber saldırılardan korunması da aynı önemi haizdir.

Ukrayna'ya düzenlenen bu saldırının yaşandığı tarih olan aralık 2015'ten yaklaşık 8 ay evvel Türkiye'de de, çok büyük çaplı bir elektrik kesintisi meydana gelmiştir. 31 Mart 2015 tarihinde ve saat 10.35 sularında, ülkenin büyük kısmında etkili olan elektrik kesintisi metro, tren, tramvay gibi pek çok ulaşım hattında seferlerin iptal olması ve bu esnada seyahat eden insanların mahsur kalması, Marmaray hattından ve diğer metro hatlarından insanları yer yüzüne yürüyerek çıkmalarına sebep olması, trafikte sıkışma ve sinyal sorunları nedeniyle karışıklık, pek çok fabrikada üretimin durması, işyerlerinde çalışmaların yapılamaması gibi sorunlara sebep olmuş ancak 2 saat sonunda kademeli olarak elektrik teminine başlanılmıştır. Yetkililer tarafından yapılan açıklamada siber saldırı ihtimalinin⁷⁹de üzerinde durulduğu belirtilmiştir. Kesintinin ardından ENTSO-E ve TEİAŞ işbirliği ile hazırlanan rapor sonrasında kesintinin niçin yaşandığına ilişkin daha net bir tablo ortaya konmuştur⁸⁰.

Görüleceği üzere günümüzde siber saldırılar, elektrik kesintilerin nedenleri arasında, ağırlığı önemli olan bir faktördür. Ulusal güvenliği koruyabilmek, beraberinde ulusun ihtiyaç duyduğu kaynakların da güvenliğini korumayı gerektirdiğinden bu alanda sorumluluk yalnızca hizmeti verenle sınırlı değil, aynı zamanda bu hizmetin gerektiği şekilde verilmesinde sorumluluğu olan devletlerin de politikalarına yansıtacak şekilde ses bulmalı ve buna göre düzenlemeler yapılmalıdır. Etkileri düşünüldüğünde yalnızca mum yakarak oturuyor olma romantizminden çok daha fazlası, evrensel hizmet ve kesintisiz erişim

⁷⁹ TRT Haber, "Başbakan'dan "elektrik kesintisi" açıklaması" link: <https://www.trthaber.com/haber/gundem/basbakandan-elektrik-kesintisi-aciklamasi-176150.html> (Son erişim tarihi: 22.06.2024)

⁸⁰ TEİAŞ, ENTSO-E, "Report on Blackout in Turkey on 31st March 2015", 2015.

beklentisinin kaynağı olması ve pek çok işletmenin faaliyetinin temelini teşkil eden internetin kullanılamıyor olması, artık en çok tercih edilenler arasında sayılabilecek elektrikle çalışan metro, tramvay gibi ulaşım araçlarının devreden çıkması, uzaktan çalışmanın artık sıradanlaştığı iş yerleri için şirket bağlarının kesintiye uğraması ile üretim tesisleri, fabrikaların çalışmıyor olması, lojistik faaliyetlerinin sekteye uğraması gibi pek çok tarafı etkileyen, en basit ifadeyle mağdur durumda bırakan elektriğin arzında güvenliğin sağlanmasının tartışmasız olduğu ortadır. Bu durumun, aynı zamanda ülkeye yapılacak herhangi bir saldırı için de oldukça kritik ve kilit bir faktör olduğu kötü niyetli kişilerin de ayırımında olduğu bir unsur olduğundan daima tehdit altında ve daima savunulmaya, güçlendirilmeye muhtaç durumdadır.

III. BÖLÜM

ELEKTRİK PİYASASINI ETKİLEYEN SİBER GÜVENLİK

DÜZENLEMELERİ VE STANDARTLAR

Siber güvenlik ve daha yaygın olarak bilgi güvenliği alanında yazılmış hukuki düzenlemelerden bazıları sektör ayırmadığı halde, bazıları spesifik olarak bir sektöre yönelik hazırlanmıştır. Metnin önceki kısmında siber güvenliğin çatı bir kavram olduğundan ve bilgi güvenliğinin unsurlarını da bünyesinde barındırdığı kabulüyle ilerleneceği belirtildiğinden, bundan sonra bir kavram karmaşası yaşanmaması adına bu husus yeniden belirtilerek, metnin devamında bilgi güvenliğine yönelik metinlerde siber güvenlik bakış açısıyla bir inceleme yapılacağına söylenmesinde fayda bulunmaktadır.

İlgili düzenlemelere daha yakından bakıldığında fark edilecek ilk detay, kritik altyapı olduğu kabul edilen sektörlerle yönelik düzenlemelerin diğer sektörlerle göre daha fazla ve kapsamlı olduğudur. Doğası gereği ve saldırı ihtimalinde görülecek zararın boyutları düşünüldüğünde, bu şekilde bir ayırımın yapılmasında tutarlılık bulunduğu kabul edilmelidir. Kritik altyapıların gerek etkilediği kişi sayısı gerekse de günlük hayatın olağan akışı içinde kapladığı yer ile önemi düşünüldüğünde, risk bakış açısıyla da diğer sektörlerle nazaran daha fazla korunması gerekmektedir. Bu nedenle ilgili sektörlerle yönelik daha fazla düzenleme yapılması gerekli olmuş bu gereklilik de beraberinde daha fazla sorumluluk getirmiştir. Bu hususta, Bakanlar Kurulu, Millî Savunma Bakanlığı, Sağlık Bakanlığı, İçişleri Bakanlığı, Ticaret Bakanlığı, Bankacılık Düzenleme ve Denetleme Kurumu, T.C. Merkez Bankası A.Ş. Bilgi Teknolojileri ve İletişim Kurumu, Sermaye Piyasası Kurumu, TEİAŞ, EPDK, KVKK gibi pek çok kurum ve kuruluş tarafından, yönetmelik, tebliğ ya da rehber başlığı altında siber güvenliğe yönelik sorumluluklar içeren düzenlemeler yapılmıştır. Her ne kadar çok farklı alana yönelik siber güvenliğe ilişkin düzenleme yapılmışsa da metnin amacı gereği yalnızca elektrik piyasasına etki edenlerinden bahsedilerek kalan düzenlemeler kapsam dışı bırakılmıştır.

Yalnızca elektrik piyasasına yönelik olarak hazırlanmış siber güvenlik düzenlemelerine geçilmeden evvel, daha geniş şekilde birçok farklı sektörü ve tarafı ilgilendiren genel nitelikteki hukuki düzenlemelerin gözden geçirilmesi, sektöre yönelik siber güvenlik düzenlemelerin izahından sonra da uluslararası kademedeki nelerin dikkate alınması gerektiği konusunda açıklamalardan oluşan bir sıra izlenecektir. Bu şekilde hem temel metinlerin hem de temel metinlere bağlı hazırlanmış sektöre yönelik metinlerin incelenmesi ile uluslararası boyutta sorumluluğun nasıl görüldüğünün anlaşılmasına çalışılacaktır.

3.1. ULUSAL SİBER GÜVENLİK DÜZENLEMELERİ VE İLGİLİ KURUMLAR

Türkiye’de yapılanmış ve salt siber güvenliği konu almış bir kanun hali hazırda bulunmamakla birlikte, farklı alanlarda faaliyet gösteren kurumların, bulundukları sektöre yönelik çalışmaları ve ikincil düzenlemelerinin de siber güvenliğe ilişkin yükümlülükler içerdiği görülmektedir. Baştan uca güvenli bir siber uzaya sahip olunması adına gerekli adımların başında ise kapsamlı, kapsayıcı ve etkili bir siber güvenlik mevzuatının olması, ilgili mevzuat ile belirlenen sorumluluğun herkese atfedilmesi gerektiği pek çok otorite tarafından kabul görmüş durumdadır. Amerika Birleşik Devleti başkanı olarak görev yapmış Barack Obama’nın da, 2015 yılında Siber Güvenlik ve Tüketici Koruma Zirvesi’nde söylediği gibi birbirimize hiç olmadığı kadar bağlı olduğumuz bu bilgi çağında hem fırsatları yakalamak hem de zorlukların üstesinden gelebilmek için hep birlikte çalışmanın önemi her zamankinden daha büyüktür⁸¹. Temel siber güvenlik ilkelerinden biri olarak kabul edilen, en zayıf halka kadar güçlü olduğu, teknik düzeyde biliniyor ve buna göre önlemler alınmaya çalışılıyorsa da bu bilinç ve farkındalık düzeyinin, siber uzayda bir şekilde yer alan her bir taraf için de belirli bir seviyenin üstünde olması gerekmektedir. Bilinç ve farkındalık düzeyinin artırılmasında pek çok araç kullanılabilecekse de hukukun bu hususta

⁸¹ The White House President Barack Obama, “Remarks by the President at the Cybersecurity and Consumer Protection Summit” link: <https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit>, (Son erişim tarihi: 22.06.2024)

en etkili araçlardan biri olacağı da malumdur. Bir bilgi ya da bilişim ağına sahip, aynı zamanda yerel ağlar vasıtasıyla da bir şekilde birbiriyle bağlantı halinde olan her bir kişi ya da kurum, bulunduğu siber uzayın güvenliği için hukuk vasıtasıyla sorumlu kılınmalıdır. Aksi halde oldukça güvenli ve korunaklı sistemlere de sahip olsa bu sistemlerin bağlantılı olduğu ve korumasız bir kanaldan gelecek en ufak bir müdahalenin umulmadık zararlar vermesi muhtemeldir.

Bahsedilen niteliklerde ve genel geçer, sektör bağımsız bir siber güvenlik düzenlemesi olmaması ancak bilişim sistemlerinin, hayatın ayrılmaz bir parçası olmasının getirdiği sorunlara çözüm olması açısından, pek çok farklı amaca hizmet etmek üzere kurulmuş kurum ile hazırlanmış hukuki düzenleme bu konuyu ele almak durumunda kalmıştır. Gerek ilgili mevzuatın korumaya çalıştığı hukuki değerler, gerekse de hayatın olağan akışının dijital ortamlara taşınması ve bilişim sistemlerinden bağımsız iş ve işlem yapmanın artık neredeyse mümkün olamaması, hazırlanış amaçları bambaşka olsa dahi, ilgili mevzuat hükümlerinin bir kısmının da siber güvenliğe ayrılmasına sebep olmuştur. Bu cihetle aşağıda yer alan ve amacı itibarıyla siber güvenliği konu almasa da siber güvenliğe dair yönlendirmeleri olan kurumlar ve düzenlemelerine yönelik genel bir inceleme yapılacaktır.

Bunun yanı sıra ülkeler için yeni bir savunma hattı olduğu kabul edilen siber uzayda ulusal ve uluslararası güvenliğin ne şekilde sağlanması gerektiği ve sorumluluğa ilişkin de bir inceleme yapılarak mevcut hukuki metinler uyarınca Türkiye’de siber güvenlikte görev paylaşımının ve sorumluluğun değerlendirilmesine yer verilecektir. Pek çok kurumun çalışma alanlarına siber güvenliğe ilişkin sorumluluğu da dahil etmiş olmaları, kayda değer bir gelişme olmakla beraber, uzun vadede görev ve sorumluluklara ilişkin tartışmaları ve dolayısıyla zaman zaman yetki gaspı zaman zaman da yetkilendirilmemiş alanlar nedeniyle zafiyetlerin yaşanmasına sebebiyet verilmesi muhtemeldir. Bu durumun da incelenmesi ve yapıların sorumluluklarına ilişkin değerlendirmelerle, siber güvenlik alanında yetkilerin belirlenmesine gayret edilecektir. Belirtilen kurumlar ve incelenen mevzuat dışında siber güvenliğe dokunan farklı otoriteler

yahut mevzuat hükümleri bulunduğunu kabul etmek gerekecektir. Ancak hem doğrudan ve güçlü bir etkisi olan hem de elektrik piyasasını etkilediği şüphesiz kurumların ve mevzuatın anlatımı ile sınırlı bir inceleme yapılmaya çalışılarak kapsam daraltılmıştır.

3.1.1. Ulaştırma ve Altyapı Bakanlığı⁸²

5809 sayılı Elektronik Haberleşme Kanunu, elektronik haberleşme sektörüne ilişkin etkin rekabetin tesisi, tüketicilerin korunması, elektronik haberleşme hizmetinin ülke genelinde yaygınlaştırılması gibi amaçları düzenleme ve denetleme yoluyla sağlayabilmek, bu sektörde yer alan kaynakların etkin ve verimli kullanımı ile teknolojik gelişimlerin sağlanması, yeni yatırımların artmasını tesis etmek amacıyla 2008 yılında yürürlüğü girmiştir. 5809 sayılı Kanun ile belirlenen görevlerin yerine getirilmesi noktasında ise Ulaştırma Bakanlığı görevlendirilmiştir.

5809 sayılı Kanun ile aynı zamanda Ulaştırma Bakanlığı nezdinde faaliyetlerine devam eden ve Türkiye'nin ilk sektörel düzenleyici kurumu Telekomünikasyon İletişim Başkanlığı'nın⁸³, Bilgi Teknolojileri ve İletişim Kurumu olarak yenilenmesine karar verilmiş olup Bakanlık elektronik haberleşme sektörüne ilişkin görevini BTK aracılığı ile ifa etmeyi sürdürmüştür. BTK, 2813 sayılı Bilgi Teknolojileri ve İletişim Kurumunun Kuruluşuna İlişkin Kanun ve 5809 sayılı Elektronik Haberleşme Kanunu ile sair mevzuatta verilen görevleri yerine getirmek üzere kurulan, idarî ve malî özerkliğe sahip bir kamu tüzel kişisidir.

Mevzuatta belirlenmiş ve 5809 sayılı Kanun uyarınca elektronik haberleşme alanında çalışmalarına devam eden Ulaştırma Bakanlığı'na, 2014 yılından itibaren

⁸² Bkz.28.

⁸³ 5809 sayılı Kanun ile getirilen değişikliklerin yanı sıra 671 sayılı Kanun Hükmünde Kararname ve 2813 sayılı Telsiz Kanunu'nda yapılan değişikliklerle birlikte Telekomünikasyon İletişim Başkanlığı yetki ve görevlerinin tamamı Bilgi Teknolojileri ve İletişim Kurumu'na devredilmiştir.

5809 sayılı Kanun’da yapılan deęiřiklikler ile ulusal siber gvenlięin saęlanması adına da BTK ile paylařtıęı nemli yetkiler devredilmiřtir.

Tablo 3. 1. 5809 sayılı Kanun’da Yapılan Siber Gvenlięe Ynelik Deęiřikler

Tarih ve Dayanak	Deęiřiklik
06.02.2014 tarih ve 6518 s. K. m.106 ile Ek madde 1 eklenmiřtir.	Siber Gvenlik Kurulu EK MADDE 1 (1) Siber gvenlikle ilgili olarak kamu kurum ve kuruluřları ile gerek ve tzel kiřiler tarafından alınacak nlemleri belirlemek, hazırlanan plan, program, rapor, usul, esas ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu saęlamak amacıyla; Bakanın bařkanlıęında Siber Gvenlik Kurulu kurulmuřtur. Siber Gvenlik Kurulunda yer alacak bakanlık ve kamu kurum ve kuruluřları ile yelerinin temsil dzeyi Bakanlar Kurulu tarafından belirlenir. (2) Kurulun grevleri řunlardır: a) Siber gvenlik ile ilgili politika, strateji ve eylem planlarını onaylamak ve lke apında etkin řekilde uygulanmasına ynelik gerekli kararları almak. b) Kritik altyapıların belirlenmesine iliřkin teklifleri karara baęlamak. c) Siber gvenlikle ilgili hkmlerin tamamından veya bir kısmından istisna tutulacak kurum ve kuruluřları belirlemek.

	ç) Kanunlarla verilen diğer görevleri yapmak. (3) Siber Güvenlik Kurulunun çalışma usul ve esasları Başbakanlıkça çıkartılacak yönetmelikle belirlenir.
15/08/2016 tarihinde 671 s. KhK. m.25 ile 60. Maddeye 11. Fıkra eklenmiştir.	Kurumun yetkisi ve idarî yaptırımlar MADDE 60 (11) Kurum, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin siber saldırılara karşı korunması ve bu saldırılara karşı caydırıcılık sağlamak için her türlü tedbiri alır veya aldırır.
02/07/2018 tarihinde 703 s. KhK. m.205 ile 5. Maddenin 1. Fıkrasına h bendi eklenmiştir.	Bakanlığın görev ve yetkileri MADDE 5 (h) Ulusal siber güvenliğin sağlanması amacıyla politika, strateji ve hedefleri belirlemek, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilere yönelik siber güvenliğin sağlanmasına ilişkin usul ve esasları belirlemek, eylem planlarını hazırlamak, ilgili faaliyetlerin koordinasyonunu sağlamak, kritik altyapılar ile ait oldukları kurumları ve konumları belirlemek, gerekli müdahale merkezlerini kurmak, kurdurmak ve denetlemek, her türlü siber müdahale aracının ve millî çözümlerin üretilmesi ve geliştirilmesi amacı ile çalışmalar yapmak, yaptırmak ve bunları teşvik etmek ve siber güvenlik konusunda bilinçlendirme, eğitim ve farkındalığı artırma çalışmaları yürütmek, siber güvenlik alanında faaliyet gösteren gerçek

	ve tüzel kişilerin uyması gereken usul ve esasları hazırlamak.
02/07/2018 tarihinde 703 s. KhK. m.205 ile 6. Maddenin 1. Fıkrasına v bendi eklenmiştir.	Kurumun görev ve yetkileri MADDE 6 v) Siber güvenlik ve internet alan adları konularında Cumhurbaşkanı, Bakanlık ve/veya Siber Güvenlik Kurulu tarafından verilen görevleri Telekomünikasyon İletişim Başkanlığı⁸⁴ veya diğer birimleri marifetiyle yerine getirmek.
02/07/2018 tarihinde 703 s. KhK. m.205 ile Ek Madde1'in 1. Ve 3. Fıkrası yürürlükten kaldırılmıştır.	Siber Güvenlik Kurulu EK MADDE 1 (1) ~~Siber güvenlikle ilgili olarak kamu kurum ve kuruluşları ile gerçek ve tüzel kişiler tarafından alınacak önlemleri belirlemek, hazırlanan plan, program, rapor, usul, esas ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak amacıyla; Bakanın başkanlığında Siber Güvenlik Kurulu kurulmuştur. Siber~~

⁸⁴ 671 sayılı KHK'de yer alan "(1) Telekomünikasyon İletişim Başkanlığı kapatılmıştır.

(2) Diğer mevzuatta Telekomünikasyon İletişim Başkanlığına yapılan atıflar Bilgi Teknolojileri ve İletişim Kurumuna, Telekomünikasyon İletişim Başkanına yapılan atıflar Bilgi Teknolojileri ve İletişim Kurumu Başkanına yapılmış sayılır." Şeklindeki Ek Madde 3 gereği görevli kurum BTK olarak kabul edilmektedir.

	~~Güvenlik Kurulunda yer alacak bakanlık ve kamu kurum ve kuruluşları ile üyelerinin temsil düzeyi Bakanlar Kurulu tarafından belirlenir.~~ (2) ... (3) ~~Siber Güvenlik Kurulunun çalışma usul ve esasları Başbakanlıkça çıkartılacak yönetmelikle belirlenir.~~
02/07/2018 tarihinde 703 s. KhK. m.205 ile Ek Madde 2 yürürlükte eklenmiştir.	EK MADDE 2 (1) Mevzuatta Siber Güvenlik Kuruluna yapılmış olan atıflar, Cumhurbaşkanınca belirlenen kurul veya mercie yapılmış sayılır.

5809 sayılı Kanun'unun her ne kadar Amaç başlıklı 1. Maddesinde⁸⁵ belirlenen görevi farklı ise de yapılan düzenlemeler gereği ulusal siber güvenliğe yönelik politika, strateji, hedef ve usul esasların belirlenmesi ile eylem planlarının hazırlanması, düzenlemenin yapıldığı tarih itibariyle faaliyette olan Siber Güvenlik Kurulu'nun⁸⁶ sekreteryasına yönelik görevlerin yürütülmesi, kritik

⁸⁵ 5809 sayılı Elektronik Haberleşme Kanunu madde 1: "Bu Kanunun amacı; elektronik haberleşme sektöründe düzenleme ve denetleme yoluyla etkin rekabetin tesisi, tüketici haklarının gözetilmesi, ülke genelinde hizmetlerin yaygınlaştırılması, kaynakların etkin ve verimli kullanılması, haberleşme alt yapı, şebeke ve hizmet alanında teknolojik gelişimin ve yeni yatırımların teşvik edilmesi ve bunlara ilişkin usul ve esasların belirlenmesidir."

⁸⁶ 5809 sayılı Elektronik Haberleşme Kanunu'na 06.02.2014 tarihinde getirilen Ek Madde 1 ile "Siber güvenlikle ilgili olarak kamu kurum ve kuruluşları ile gerçek ve tüzel kişiler tarafından alınacak önlemleri belirlemek, hazırlanan plan, program, rapor, usul, esas ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak amacıyla; Bakanın başkanlığında Siber Güvenlik Kurulu kurulmuştur. Siber Güvenlik Kurulunda yer alacak bakanlık ve kamu kurum ve kuruluşları ile üyelerinin temsil düzeyi Bakanlar Kurulu tarafından belirlenir." Şeklindeki hükme istinaden ve hüküm ile işaret edilen 11.06.2012 tarih 2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu kararına göre Siber Güvenlik Kurulu Ulaştırma, Denizcilik ve Haberleşme Bakanı'nın başkanlığında,

altyapıların belirlenmesi ile siber güvenliğe yönelik müdahale merkezlerinin kurulumu, siber müdahale araçlarının millileştirilmesi ile bu yöndeki çalışmaların arttırılması, halkın farkındalık ve bilinç düzeyinin geliştirilmesinin yanı sıra belirlenen bu görevlere ilişkin denetleme ve düzenleme sorumluluğu Ulaştırma Bakanlığı'na bırakılmıştır. Ayrıca 6. Madde uyarınca, siber güvenlik ve internet alan adları konularında Cumhurbaşkanı, Bakanlık ve/veya güncel mevzuat hükümleri gereği DDO tarafından verilen görevleri BTK veya diğer birimleri marifetiyle yerine getirmek şeklinde bir başka görev de Ulaştırma Bakanlığı'nın sorumluluğundadır.

5809 sayılı Kanun'un 60. Maddesinin 11. Fıkrasında yapılan değişiklik ile BTK'ya verilen bilgi ve belge isteme yetkilerin sınırlarının kişisel verilerin korunmasına ilişkin ulusal ve uluslararası düzenlemeler ile Avrupa İnsan Hakları Mahkemesi içtihatları ile belirlenmiş kriterlere aykırı şekilde genişletildiği, bu nedenle de Anayasa'nın cumhuriyetin nitelikleri, temel hak ve özgürlüklerin sınırlandırılması, özel hayatın gizliliği ile milletlerarası anlaşmalara uygunluğu düzenleyen hükümlerine aykırı olduğu belirtilerek 2017 yılında iptali istenmiştir. Anayasa Mahkemesi Genel Kurulu tarafından, yapılan iptal istemi 2017/16 esas ve 2019/64 karar sayılı dosyasında incelenmiş olup 24.07.2019 tarihinde başvuruya ilişkin karar verilmiştir⁸⁷. İlgili karara göre, Anayasa Mahkemesi tarafından, BTK'ya verilen bu yetkinin, *“siber güvenliği sağlama görevine ilişkin hükümden sonra gelen ve Kurumun “...görevi kapsamında...” ilgili yerlerden bilgi, belge, veri ve kayıtları alabilmesinin, değerlendirmesini yapabilmesinin, arşivlerden, elektronik bilgi işlem merkezlerinden ve iletişim altyapısından yararlanabilmesinin, bunlarla irtibat kurabilmesinin ve bu kapsamda diğer gerekli önlemleri alabilmesinin veya aldırabilmesinin öngörülmüş olması karşısında*

Dışişleri Bakanlığı Müsteşarı, İçişleri Bakanlığı Müsteşarı, Milli Savunma Bakanlığı Müsteşarı, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı Müsteşarı, Kamu Düzeni ve Güvenliği Müsteşarı, Milli İstihbarat Teşkilatı Müsteşarı, Genelkurmay Başkanlığı Muhabere Elektronik ve Bilgi Sistemleri Başkanı, Bilgi Teknolojileri ve İletişim Kurumu Başkanı, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu Başkanı, Mali Suçları Araştırma Kurulu Başkanı, Telekomünikasyon İletişim Başkanı ile Ulaştırma, Denizcilik ve Haberleşme Bakanınca belirlenecek bakanlık ve kamu kurumlarının üst düzey yöneticilerinden oluşacak şekilde faaliyet göstermiştir.

⁸⁷ AYM, E.2017/16, K.2019/64, 24/07/2019, § ...

Kuruma tanınan bu yetki ve imkânların Kurumun siber güvenliğin sağlanması göreviyle sınırlı olduğu anlaşılmaktadır.” Şeklinde yorumlandığı görülmektedir. Bunun yanında Anayasa Mahkemesi’nin siber güvenliğe ilişkin, siber güvenlik açıkları nedeniyle uğranılacak zararların millî güvenlik tehditlerinden, ekonomik krizlere ve önemli kişisel zararlara varana kadar birçok soruna neden olabileceği bu alana ilişkin düzenlemelerin millî güvenliğin, kamu düzeninin ve kamu güvenliğinin sağlanması için bir zorunluluk olduğu, bu durumun devlete yüklenen bir ödev olduğu da belirtilmiştir. Anayasa Mahkemesi, iptali istenen hüküm ile verilen yetkinin BTK’ya verilmiş siber güvenlik görevlerini yerine getirmek üzere ihdas edildiği, bu sebeple temel hak ve özgürlüklerin sınırlandırılmasında göz önünde bulundurulması gereken belirlilik ilkesine aykırı olmadığı, yanı sıra siber güvenliğin sağlanması için bu yetkinin ihtiyaca yönelik ve amaca ulaşmada gerekli olduğu, müdahale ile kişilerin özel hayatına getirilen sınırlamanın kamu güvenliği sağlanması amacı karşısında orantılı olduğu neticesine varılarak iptal talebinin oy çokluğu ile reddine karar verilmiştir.

Mahkemenin iptali istenen hükme ilişkin ret kararına karşı verilen 3 karşı oy bulunmaktadır. Zühtü Arslan tarafından kaleme alınan karşı oyda Anayasa’nın 20. Madde ile kişisel verilerin korunmasını isteme hakkına müdahale anlamına gelen bir müdahalenin salt kanun ile şeklen getirilmiş olmasının yeterli olamayacağı, ilgili hükmün keyfiliğe izin vermeyecek şekilde belirli, ulaşılabilir ve öngörülebilir bir düzenleme olması gerektiğinden bahsedilmiştir. Anayasa Mahkemesi tarafından yakın zamanda verilen *Fatih Saraman*, [GK], B.No: 2014/7256, 27/2/2019, § 83 sayılı kararda “*güvenlik soruşturmasına ve arşiv araştırmasına konu edilecek bilgi ve belgelerin neler olduğu, bu bilgilerin nerelerden elde edileceği ve ne suretle ve ne kadar süre ile saklanacağı, kişilerin söz konusu bilgilere itiraz etme olanağı olup olmadığı, bilgilerin bir müddet sonra silinmesinin mümkün olup olmadığı veya silinmesine dair izlenecek usulün ne olduğu, gizlilik dereceli kamu personeli ile meslek gruplarının tespiti, güvenlik soruşturmasının ve arşiv araştırmasının usul ve esasları ile bunu yapacak mercilerin kimler olduğu ile ilgili hiçbir düzenleme içermediği*”, şeklindeki

değerlendirme ile bireyleri keyfilığe karşı koruyacak hükümlere yer verilmesinin uygun görülmediği, bu anlamda “bireylerin özel hayatına saygı hakkının güvencelerini sağlayacak hükümlerden yoksun olduğu” sonucuna ulaşmıştır şeklinde hüküm kurulmuş olduğunu belirten Zühtü Arslan, belirlilik ilkesinin sağlanmasına yönelik incelemede, Anayasa Mahkemesi’nin önceki yaklaşımını da ortaya koymuştur. 5809 sayılı Kanun ile BTK’ya verilmiş 28 alt görev olduğundan bahseden karşı oyda hüküm ile BTK “tarafından istenen ve işlenen kişisel verilerin mahiyeti, bu verilerin denetimi, kişilerin durumdan haberdar edilmesi gibi hususlar yönünden de güvencelere yer verilmiş değildir” şeklindeki yorumuyla da kişisel verilerin korunması isteme hakkı için gerekli belirlilik, öngörülebilirlik koşulları ile keyfi müdahaleyi önleyecek kanuni güvencelerden yoksun bir sınırlama getirilmiş olduğu, bu nedenle de ilgili hükmün Anayasa’nın 13. ve 20. maddelerine aykırı olduğu yorumu yapmıştır.

Bir diğer karşı oyda ise Anayasa Mahkemesi’nin incelenen dava ile benzer nitelik taşıyan bir başka kararında (E.2014/149, K.2014/151, 2/10/2014) “*kişisel veri niteliğinde olan ve ciddi suçların tespiti, soruşturulması ve kovuşturulmasında kullanılmak üzere gerçek ve tüzel kişilere ilişkin trafik bilgisinin erişim veya yer sağlayıcılardan, Telekomünikasyon İletişim Başkanlığı TİB tarafından herhangi bir gerekçe veya neden göstermeksizin temin edilmesine olanak sağlayan kuralın Anayasa’nın 2., 13. ve 20. maddelerine aykırı olduğu sonucuna ulaşmıştır.*” Şeklindeki değerlendirilmesine yer verilmiş ve TİB tarafından bir çerçeve ve sınırlama getirilmeksizin dilediği şekilde ve zamanda trafik verisi temin etmesi istemini içerir, temel hak ve özgürlüklerin korunması bakımından hukuka aykırı bulunduğu belirtilmiştir. İlgili karşı oyda, insan onuruna saygı ve kişilik haklarına dayanan özel hayatın gizliliği ve bu kapsamda kişisel verilerin korunmasını isteme hakkının, hakkında yapılan müdahalenin demokratik toplum düzeninin gerekleri ile ölçülülük ilkesine de uygun olması gerektiği ifade edilmiştir. Müdahalede bulunulan hakkın, kişinin saygınlığını ve kişiliğini serbestçe geliştirmesini mümkün kılan değerlere etkisi olduğu, kişiliğin serbestçe gelişimine, kişinin kendisi ve yakınlarıyla kuracağı özerk bir yaşam alanına sahip olma şansına etkisi

olduđu, bireyin başkaları tarafından bilinmesini istemediđi hususların güvence altına alınmasını istemek hakkının göz önünde bulundurulmasının önemi vurgulanmıştır.

Belirlenen diđer yükümlölüklerin baki kalması kaydıyla, Ulaştırma Bakanlığı'na bırakılan Siber Güvenlik Kurulu sekretaryasına yönelik görevler, 02.07.2018 tarihinde 5809 sayılı Kanun'da yapılan deđişiklik ve getirilen Ek Madde 2 ile şekil deđiştirmiştir. Öncelikle Ek Madde 1'in 1. Fıkrasında Siber Güvenlik Kurulu'na atfedilen, siber güvenliğe ilişkin özel ve kamu kurum ve kuruluşlarınca alınması gereken önlemlerin, plan, program, rapor, usul, esas ve standartların belirlenerek uygulanmasına yönelik görevler kaldırılmış, yanı sıra Ek Madde 2 ile de mevzuatta Siber Güvenlik Kurulu'na yapılmış atıfların Cumhurbaşkanınca belirlenen kurul veya mercilere yapılmış sayılacağı belirlenmiştir. Yapılan bu deđişikliđin ardından 10.07.2018 tarihinde 1 sayılı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi yürürlüğe girmiş ve T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi ile bünyesinde Siber Güvenlik Dairesi Başkanlığı kurulmuştur. 1 sayılı Cumhurbaşkanlığı Kararnamesi'nin 527. Maddesinin 1. Fıkrasının d bendi ile bilgi güvenliği ve siber güvenliği arttırıcı projeler geliştirme görevi DDO'ya bırakılmış olup, görevin içeriđi de 527/B maddesinin 1. Fıkrasının ç bendinde yer alan hüküm ile netleştirilmiştir.

Ulaştırma Bakanlığı'nın, 5809 sayılı Kanun'unun 5. Maddesinin h bendinde belirlenen görevleri ile Dijital Dönüşüm Ofisi Siber Güvenlik Dairesi Başkanlığı'nın 1 sayılı 10.07.2018 tarihinde ve 30474 sayılı Resmi Gazete'de yayımlanan Cumhurbaşkanlığı Kararnamesi'nin 527/B maddesinde belirlenen görevleri karşılaştırıldığında, benzeşen görev tanımlarının da olduđu görölmektedir. Genel itibariyle Siber Güvenlik Dairesi Başkanlığı'nın siber güvenliğe ilişkin operasyonların gelişimine yönelik görevleri üstlenmiş olduđu, Ulaştırma Bakanlığı'nın ise karar verici ve yön belirleyici olduđu ilgili hükümlerden görölüyor olsa da, kritik altyapıların belirlenmesi, kamu kurumları ve kritik altyapılara yönelik siber güvenlik stratejilerin geliştirilmesi gibi konulara

ilişkin her iki kurumun ortak bir çalışma alanı olduğu görülmektedir. Aşağıda 5809 sayılı Kanun ve 1 sayılı Cumhurbaşkanlığı Kararnamesi ile her iki kuruma da verilen ve zaman zaman ortak zaman zaman tamamlayıcı olduğu görülen görevlere ilişkin bir tabloda, bu görünümün daha net bir şekilde ortaya konulmasına çalışılmıştır.

Tablo 3. 2. 5809 sayılı Kanun 5. Madde ve 1 sayılı Cumhurbaşkanlığı Kararnamesi 527/B Maddesi

5809 sayılı Kanun 5. maddesi ile Ulaştırma Bakanlığı'na verilen siber güvenliğe ilişkin görevler	1 sayılı Cumhurbaşkanlığı Kararnamesi 527/B maddesi ile CDDO Siber Güvenlik Dairesi Başkanlığı'na verilen siber güvenliğe ilişkin görevler
Ulusal siber güvenliğin sağlanması amacıyla politika, strateji ve hedefleri belirlemek, eylem planlarını hazırlamak	Siber güvenlik ile ilgili politika, strateji ve eylem planlarının ülke çapında etkin şekilde uygulanmasına yönelik gelişmeleri takip etmek
	Cumhurbaşkanınca belirlenen politikalar kapsamında kamu kurumları ve kritik altyapılara yönelik siber güvenlik stratejileri geliştirmek
Kamu kurum ve kuruluşları ile gerçek ve tüzel kişilere yönelik siber güvenliğin sağlanmasına ilişkin usul ve esasları belirlemek, eylem planlarını hazırlamak	Siber güvenlikle ilgili hükümlerin tamamından veya bir kısmından istisna tutulacak kurum ve kuruluşlar konusunda ilgili kurumlara önerilerde bulunmak

	Kamu kurumlarında ve kritik altyapı işleten kuruluşlarda bilgi güvenliği yönetim sisteminin kurulup işletilmesi, teknik standartlar ile usul ve esasların belirlenmesi, uygulamanın izlenmesi ve yönlendirilmesi konularında çalışmalar yürütmek
İlgili faaliyetlerin koordinasyonunu sağlamak	Kamu, özel sektör ve üniversiteler arasındaki iş birliğinin artırılması suretiyle ulusal siber güvenlik ekosisteminin oluşturulmasına katkı sağlamak
Kritik altyapılar ile ait oldukları kurumları ve konumları belirlemek	Kritik altyapıların belirlenmesine yönelik çalışmalar yapmak
Gerekli müdahale merkezlerini kurmak, kurdurmak ve denetlemek	Kritik teknoloji ve bilgi varlıklarını korumak amacıyla önleyici ve koruyucu faaliyetler konusunda çalışmalar yürütmek
Her türlü siber müdahale aracının ve millî çözümlerin üretilmesi ve geliştirilmesi amacı ile çalışmalar yapmak, yaptırmak ve bunları teşvik etmek	Kritik altyapılar başta olmak üzere her alanda, yerli ve milli siber güvenlik ürünlerinin geliştirilmesine ve bu çözümlerin kullanımının kamuda yaygınlaştırılmasına yönelik çalışmalar yapmak

Siber güvenlik konusunda bilinçlendirme, eğitim ve farkındalığı artırma çalışmaları yürütmek	Ulusal siber güvenlik ve bilgi güvenliğini destekleyici projeler geliştirmek
Siber güvenlik alanında faaliyet gösteren gerçek ve tüzel kişilerin uyması gereken usul ve esasları hazırlamak	Özel sektörün kapasitesinin kritik alanlara yönlendirilmesi ve mükerrer yatırımların önlenmesi için öncelikli siber güvenlik alanlarını belirlemek

Görüleceği üzere Ulaştırma Bakanlığı'nın siber güvenlik alanında düzenleyici otorite olarak faaliyet göstermesi ve yön belirlemesi, CDDO Siber Güvenlik Dairesi Başkanlığı'nın da bu hususta destekleyici, koruyucu ve yönlendirici faaliyetleriyle ülke genelinde siber güvenliğin gelişimi konusunda çalışmalar ortaya konması beklenmektedir.

5809 sayılı Kanun dışında ve ilgili Kanun'da yapılan düzenlemelerle aynı tarih olan 06.02.2014'de, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ile de siber güvenlik konulu görevler tesis edilmiştir. İdarî yapı ve görevler başlığını taşıyan 10. Maddeye eklenen 6. Fıkra⁸⁸ ile BTK, ulusal siber güvenlik faaliyetleri kapsamında, siber saldırıların tespiti ve önlenmesi konusunda, içerik, yer, erişim sağlayıcılar ve ilgili diğer kurum ve kuruluşlarla koordinasyon sağlamak, gerekli tedbirlerin aldırılması konusunda faaliyet yürütmek ve ihtiyaç duyulan çalışmaları yapmakla da yükümlü durumdadır.

⁸⁸ 5651 sayılı Kanun'da 06.02.2014 tarihinde 6581 sayılı Kanunu'nun 95. Maddesi ile İdari Yapı ve Görevler başlıklı 10. Maddenin 6. Fıkrası olarak eklenen hüküm "Kurum, ulusal siber güvenlik faaliyetleri kapsamında, siber saldırıların tespiti ve önlenmesi konusunda, içerik, yer, erişim sağlayıcılar ve ilgili diğer kurum ve kuruluşlarla koordinasyon sağlar, gerekli tedbirlerin aldırılması konusunda faaliyet yürütür ve ihtiyaç duyulan çalışmaları yapar." Şeklinde dir.

5809 sayılı Kanun’una yapılan deęişikliklerden evvel alınmış 2012/3482 Ulusal Siber Güvenlięin alıřmalarının Yürütölmesi, Yönetilmesi ve Koordinasyonuna İliřkin Karar uyarınca da hem ulusal siber güvenlięin saęlanması adına yönlendirmelerde bulunulmuş hem de Ulařtırma Bakanlığı’na siber güvenlięe iliřkin görevler verilmiştir. Bakanlar Kurulu’nun 2012/3482 sayılı kararı ile 5809 sayılı ve 5651 sayılı Kanunlara eklenen hükümlere benzer nitelikte olduęu görölen görevler ařaęıda sıralanmıştır.

- Ulusal siber güvenlięin saęlanması için politika, strateji ve eylem planlarını hazırlamak,
- Kamu kurum ve kuruluşlarına ait bilgi ve verilerin güvenlięi ile mahremiyetinin güvence altına alınmasını saęlamaya yönelik usul ve esasları hazırlamak,
- Ulusal siber güvenlięin saęlanmasında kamu kurum ve kuruluşlarında teknik alt yapının oluřturulmasını takip etmek, uygulamaların etkinlięinin doęrulanmasını ve test edilmesini saęlamak,
- Ulusal bilgi teknolojileri ve iletiřim alt yapısı ve sistemleri ile veri tabanlarının güvenlięini saęlamaya, kritik alt yapıları belirleyerek bunlara yönelik siber tehdit ve saldırı izleme, müdahale ve önleme sistemlerini oluřturmaya, ilgili merkezleri kurmaya, kurdurmaya, bu sistemlerin denetimi, iřletimi ve sürekli güçlendirilmesine yönelik alıřmaları yapmak,
- Ulusal siber güvenlięin saęlanmasında her türlü milli özömlerin ve siber saldırılara müdahale araçlarının geliřtirilmesi ve üretilmesini teřvik etmek, kullanımını saęlamak,
- Ulusal siber güvenlik aısından kritik kurum ve konumlar için gerekli ve yeterli sayıda uzman personelin temini, eęitimi ve geliřimini planlamak, koordine etmek ve yürötmek, dięer ölkeler ve uluslararası kuruluşlarla iř birlięi yapmak,

- Ulusal siber güvenlik konusunda bilinçlendirme, eğitim ve farkındalığı artırma çalışmaları yürütmek,
- Bilgi güvenliği alanında eğitim, test ve çözüm üretme alanında çalışan gerçek ve tüzel kişilere usul ve esaslarını belirleyerek güvenlik belgesi vermek.

Ulaştırma Bakanlığı'nın maddede belirtilen görevlerini, BTK ve diğer kamu kurum ve kuruluşları aracılığı ile yerine getirebileceği ve kamu düzeninin korunması açısından zorunlu hallerde, ilgili makamlar ve talepler çerçevesinde, ulusal siber güvenlikle ilgili tedbirleri alabileceği de aynı kararda düzenlenmiştir. Hali hazırda çalışmalarına son verilmiş Siber Güvenlik Kurulu'na yönelik görevlerin geçerliliğinin bulunmadığını kabul etmek gerekecekse de kalan yükümlülüklerin aksine bir karar alınmadıkça yürürlükte olduğunu kabul etmek gerekmektedir.

İzah edilen düzenlemeler uyarınca ulaştırma, denizcilik, haberleşme, uzay ve bilgi teknolojileri alanlarında; dengeli, erişilebilir, ekonomik ve güvenli hizmet anlayışıyla, toplumun yaşam kalitesinin yükseltilmesine ve ülke kalkınmasına katkı sağlamak amacıyla faaliyet gösteren Ulaştırma Bakanlığı ve bağlı kurumların siber güvenlik alanında da görevleri bulunduğu, sektöre özel düzenlemelerin yanında belirlenen bu görevlerin tüm kamu kurum ve kuruluşları ile özel ve tüzel kişileri bağlayıcı nitelikte olduğu görülmektedir.

3.1.2. Ulusal Siber Olaylara Müdahale Merkezi Ve Sektörel Olaylara Müdahale Ekibi

27.03.2013 tarihinde Bilgi Teknolojileri ve İletişim Kurumu bünyesinde kurulan Ulusal Siber Olaylara Müdahale Merkezi'nin görev ve sorumlulukları, 20/06/2013 tarih ve 28683 sayılı Resmi Gazete'de yayımlanan 2013/4890 sayılı Bakanlar Kurulu Kararı ile onaylanan "2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı" 'nın 5.3. numaralı "Ulusal Siber Olaylara Müdahale Organizasyonunun Oluşturulması" başlıklı eylem planı altında kabaca tasvir

edilmiştir. Ancak yasal zeminini, 5809 sayılı Elektronik Haberleşme Kanunu’nun 5, 60 ve Ek madde 1 maddesi ile BTK’ya verilen görev ve sorumluluklar kapsamında olduğu söylenebilir.

BTK bünyesinde yer alan USOM, Türkiye'deki siber olaylara müdahale konusunda ulusal ve uluslararası düzeyde koordinasyon sağlamaktadır. USOM, yerli ve milli tespit ve analiz sistemlerini kullanarak siber tehditleri belirler ve bu tehditlere karşı taraflara ve ülke geneline yönelik alarm, uyarı ve duyurular yapar. Bu çalışmalar, olası siber olayların etkilerini azaltmak veya ortadan kaldırmak için alınmış önleyici tedbirler kapsamında değerlendirilebilir. Bir nevi siber saldırıların alarm mekanizması görevini gören USOM bu görevinin yanı sıra, siber güvenlik olaylarına maruz kalan sistemlere yönelik koruyucu tedbirlerin alınması konusunda da faaliyetlerde bulunmaktadır. Ayrıca yapılan siber güvenlik çalışmaları esnasında konusu suç teşkil eden bulgular ile karşılaşılması halinde doğrudan idari bir yaptırım yahut siber saldırı gerçekleştirdiği tespit edilen taraflara karşı bir müdahalede bulunmuyor olsa da, USOM bu görevlerin yerine getirilmesi adına adli makamlar ve kolluk kuvvetleri ile koordinasyon içerisinde hareket etmektedir.

Sayılan görevlerin yanı sıra “Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı” kapsamında USOM’larla birlikte çalışmak için kamu kurum ve kuruluşları bünyesinde sektöre özgü ve kurumlara özgü Siber Olaylara Müdahale Ekipleri oluşturulması da öngörülmüştür. Resmi Gazete’de 11 Kasım 2013 Tarihli ve 28818 Sayılı Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ’ne göre kurumsal ve sektörel SOME’lerin kuruluşuna ilişkin düzenlemeler yapılmış olup, bu hususta ilgili kurumlar ve sorumluluklarının ortaya konmasına, görev ve çalışmalarına ilişkin usul ve esaslarını belirleyerek, hizmetlerin etkin ve verimli bir şekilde yürütülmesi sağlanmaya çalışılmıştır.

SOME Tebliğ’ine göre kurumsal SOME’lerin her bir Bakanlık bünyesinde ve tüm birimlerini kapsayacak yahut önem ve büyüklüğü gerektiriyorsa her bir

birim bazında, bunların dışında kalan kamu kurum ve kuruluşlarının da yine kendi bünyelerinde ayrıca genel bütçe kapsamındaki kamu idareleri, üniversitelerin de dahil olduğu özel bütçeli idareleri, EPDK, KVKK gibi düzenleyici ve denetleyici kurumlar ile sosyal güvenlik kurumlarının da kurumsal SOME kurabileceği düzenlenmiştir. SOME Tebliğ'inin ilgili maddesine bakıldığında da görüleceği üzere yalnızca müstakil bir bilişim sistemi ile çalışan her türlü kamu kurumunun dahil edildiği ve geniş bir kapsamı olan bir Kurumsal SOME ağının oluşmasının arzu edildiği, Kurumsal SOME'lerin yaygınlaştırılması ve özellikle devlet kurumlarının da siber güvenlik olaylarına hazırlıklı, müdahale stratejileri geliştirmiş kurumlar olarak yapılanmalarının istendiği sonucuna ulaşılabilecektir. Ancak bu hususta Tebliğ ile yapılan yalnızca bir yönlendirme olduğu ve hukuki olarak bir zorunluluk addedilmeyen bir talep olduğunu da vurgulamak gerekir. SOME Tebliğ'inin 5. Maddesinde, kurumsal SOME'lere getirilen görev ve sorumluluklar belirlenmiş olup Ulaştırma, Denizcilik ve Haberleşme Bakanlığı⁸⁹, Haberleşme Genel Müdürlüğü tarafından 2014 yılında yayımlanan Kurumsal SOME Kurulum ve Yönetim Rehberi ile de *“Kurumsal SOME'lerin kurum organizasyonu içerisindeki yerini, kapasite planlamasını, personelin niteliklerini (eğitim düzeyi ve tecrübe), alması gereken eğitimleri, bu personelin siber olay öncesi, esnası ve sonrasında yapması gereken çalışmaları, kurum içi/kurum dışı paydaşlarla iletişim esaslarını, Kurumsal SOME'lerin kurulması için gereken kuruluş süreleri ve esasları ile bu süreçte kullanılacak olan ekleri, şekilleri ve tabloları”*⁹⁰ konusunda yol gösterici olması amaçlanmıştır.

SOME Tebliğ ve Kurumsal SOME Kurulum ve Yönetim Rehberi uyarınca, Kurumsal SOME'lerin bulundukları kuruma yapılacak herhangi bir siber saldırıya karşı gerekli önlemleri alma ve müdahalede bulunabilme, kullanılan bilişim sistemlerinde teknik ve idari tedbirleri alma, çalışmalarını sektörel SOME'ler ve USOM ile koordineli şekilde gerçekleştirerek, siber olayla karşılaşıldığı anda

⁸⁹ Günümüzde Ulaştırma ve Altyapı Bakanlığı olarak faaliyet gösteren Bakanlığın ismi 2014 yılı itibarıyla Ulaştırma, Denizcilik ve Haberleşme Bakanlığı olarak anıldığından ilgili metne sadık kalınarak o dönemdeki ismi ile yer verilmiştir.

⁹⁰ Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, Haberleşme Genel Müdürlüğü, “Kurumsal SOME Kurulum ve Yönetim Rehberi”, Temmuz 2014 s: 8.

doğrudan bu kurumları haberdar etme, kurum içi farkındalığı geliştirme ve kurum personeline eğitime, siber güvenlik testleri uygulama, siber olaylara ilişkin ilgili kayıt ve raporları hazırlama, 7/24 erişilebilir olma gibi yükümlülükler yüklenmiştir. Belirlenen yükümlükler itibarıyla, bu konuda yönetim konusunda yönlendirmelerin yapıldığı, ancak doğrudan ve teknik olarak siber güvenlik alanında yapılması beklenen çalışmaların neler olabileceği konusuna ilişkin bir tavsiyede bulunulmadığı ya da beklenen önlemlerin alınmaması halinde sorumlu olup olunmayacağı konusunda bir belirlilik sağlanmadığı görülmektedir.

Kurumsal SOME'lerin yanında Sektörel SOME'lere yönelik olarak da SOME Tebliği'nde düzenlemeler yapılmıştır. Tebliğin 6. Maddesine göre Sektörel SOME'ler düzenleyici ve denetleyici kurumların bünyesinde kendi sektörlerinde faaliyet gösteren kurum, kuruluş ve işletmeleri kapsayacak şekilde ve ihtiyaç duyulması halinde, düzenleyici ve denetleyici kurumların yetki alanı dışında kalan diğer sektörlerde ilgili olduğu Bakanlık bünyesinde kurulabilmekte olup kritik sektörlerde, sektörel SOME kurulması zorunlu hale getirilmiştir. Sektörel SOME'lerin bulunduğu sektörlerdeki özel kurumlar ve diğer kuruluşların kendi bünyelerinde ayrıca kurumsal SOME'de kurabilecekleri düzenlenmiş olup, düzenleyici ve denetleyici kurumlardaki sektörel SOME'lerin koordinasyonun BTK tarafından yürütüleceği kararlaştırılmıştır. Bunun yanında kurumsal SOME'ler için olduğu gibi sektörel SOME'ler için de Ulaştırma Bakanlığı, Haberleşme Genel Müdürlüğü tarafından 2014 yılında Sektörel SOME Kurulum ve Yönetim Rehberi yayımlanmıştır. SOME Tebliği'nin 7. Maddesi ile Sektörel SOME Kurulum ve Yönetim Rehberi'ne göre sektörel SOME'lere de Kurumsal SOME'ler ile benzer şekilde, herhangi bir siber saldırıya karşı gerekli önlemleri alma ve zararların azaltılmasına yönelik faaliyetlerde bulunma konusunda USOM ile koordineli şekilde çalışma ve siber olayları bildirme, USOM tarafından iletilen alarm, uyarı ve duyuruları dikkate alarak birlikte çalıştıkları SOME'lerin gerekli tedbirleri alması konusunda yönlendirme, bilinçlendirme, bilgilendirme, eğitim faaliyetleri düzenleme, 7/24 erişilebilir olma, sektörde bulunan kritik bilgi sistemlerini belirleme, sektör içi asgari siber güvenlik kriterlerini belirleme,

sektörel siber olay müdahale prosedürü oluşturma ve tatbikatlarda test etme gibi sorumluluklar atfedilmiştir. Belirlenen yükümlükler itibariyle siber güvenlik alanında yönetim, yönlendirme ve düzenleyici görevlerin atfedildiği görülmektedir.

USOM, ulusal seviyede yapılan çalışmaların yanı sıra, sektörel ve kurumsal düzeyde siber güvenlik tehditlerinin tespiti ve ilgililerin bilgilendirilmesi için Sektörel ve Kurumsal Siber Olay Müdahale Ekipleri (SOME'ler) ile iş birliği içinde faaliyet göstermektedir. Özellikle SOME İletişim Portalı aracılığıyla, siber güvenlik çalışmalarına katılan tarafların anlık bildirimleri ve ihbarları, 7/24 çalışan ekipler tarafından alınmakta ve her türlü siber güvenlik saldırısının bildirimi ve izlenmesi sağlanarak ilgili olaylara hızla müdahalede bulunmak, kurumsal işbirliği sayesinde, siber saldırıların erken tespit edilerek zararların önlenmesine odaklanmak ve ülke genelinde gelişmiş bir siber saldırı iletişim hattının oluşturulması görevini üstlenen USOM, yaşanan siber olayları inceleyerek gerekli aksiyonların alınmasını sağlar. Kurumlar arasında yaratılan sinerji sayesinde siber saldırıların önemli zararlar verilmeden tespit edilmesine ve gerekli önlemlerin alınmasına gayret edilerek ülke çapında gelişmiş bir siber saldırı iletişim hattının kurulması görevini yürüten USOM'un olay öncesinde olduğu gibi sonrasında da inceleme ve değerlendirmeler yapılmasını sağlayarak, gerekli aksiyonların alınmasına yönelik de sorumlulukları bulunmaktadır. USOM'un tespit ettiği zararlı yazılımların analiz çalışmaları, siber güvenlik önlemlerinin şekillendirilmesine ve güvenlik açıklarının belirlenmesine yardımcı olur. Örneğin, zararlı yazılım veya internet adreslerine yönelik yapılan tespitler, erişim engellemeleri ve güvenlik açıkları üzerine yapılan çalışmalar, siber olaylardan zarar görmeden veya en az şekilde etkilenecek tüm kurum ve kuruluşların aynı düzeyde korunmasına katkı sağlar. Ayrıca iyi uygulama örnekleri, tatbikatlarda ve koordinasyon çalışmaları yapılırken, USOM uluslararası iş birliği kapsamında diğer Siber Olay Müdahale Ekipleri (Computer Emergency Response Team -CERT'ler) ile birlikte çalışır.

3.1.3. T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi

10 Temmuz 2018 tarihli, 30474 sayılı Resmî Gazete 'de yayımlanarak yürürlüğe giren, 1 Sayılı Cumhurbaşkanlığı Kararnamesi kapsamında, farklı kurumların bünyesinde devam eden dijital dönüşüm faaliyetleri ile siber güvenlik, büyük veri ve yapay zekâ ile ilgili çalışmaların tek çatı altında toplanması amacıyla T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi kurulmuştur. Dijital Dönüşüm Ofisi bünyesinde kurulan Siber Güvenlik Dairesi Başkanlığı'nda, siber güvenlik alanında ülkede yapılan çalışmaların temelini oluşturmak adına, politikalara uygun şekilde siber güvenlik stratejilerinin, bu yöndeki projelerin, bilhassa yerli ve milli siber güvenlik ürünlerinin geliştirilip yaygınlaştırılması, kamu, özel sektör ve akademi ile işbirliği içinde ulusal düzeyde bir siber güvenlik ekosisteminin oluşturulması, ülke çapında siber güvenlik önlemlerinin etkin, verimli, uyumlu bir şekilde uygulanması, mükerrer yatırımların önüne geçilmesi, kritik altyapıların belirlenmesine yönelik çalışmaların yapılması, kurumların bilgi güvenliği yönetim sistemi bağlamında siber güvenlik standartlarına uygun şekilde işletilmesi ve bu uygulamaların izlenmesi hususunda görevler yerine getirmek üzere çalışmaktadır.

6 Temmuz 2019 tarihli 30823 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren 2019/12 sayılı Bilgi ve İletişim Güvenliği Tedbirleri konulu genelge ile de siber güvenlik risklerinin azaltılıp etkisiz kılınması ve milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına yol açabilecek kritik türdeki verilerin güvenliğinin sağlanması amacıyla bir takım tedbirlerin belirlenmesinin yanında, DDO koordinasyonunda Bilgi ve İletişim Rehberi'nin hazırlanarak yayımlanacağı duyurulmuş, tüm kamu kurum ve kuruluşları ile kritik altyapı hizmeti veren işletmelerde, yeni kurulacak bilgi sistemlerinin uyumlu olması beklenen yükümlülükler belirlenmiştir. Kritik altyapı sektörlerine ilişkin Rehber'de yapılan tanım, 2020-2023 Ulusal Siber Güvenlik Stratejisine atıf yapmış olup ve burada yer alan tanımın⁹¹ da Mülga Siber Güvenlik Kurulu

⁹¹ Ulaştırma ve Altyapı Bakanlığı, "Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023", "Kritik Altyapı Sektörleri: Mülga Siber Güvenlik Kurulu'nun 20 Haziran 2013 tarihli ve 2 sayılı

kararına atıfta bulunduğu görülmektedir. İlgili atıflar uyarınca, kritik altyapılar ve dolayısıyla Bilgi ve İletişim Güvenliği Rehberi’nde yer alan yükümlülüklerden sorumlu sektörlerin “Elektronik Haberleşme”, “Enerji”, “Finans”, “Ulaştırma”, “Su Yönetimi” olduğu neticesine ulaşılmaktadır. Kritik altyapıların belirlenmesi konusunda, 5809 sayılı Kanun ile Ulaştırma Bakanlığı’na ve 1 sayılı Cumhurbaşkanlığı Kararnamesi DDO’ya görev verilmiş olduğundan kritik altyapıların neler olduğu konusunda bir uzlaşma sağlanmadığının, zira belirlenen sektörlerde onlarca alt sektör bulunduğunun göz önünde bulundurulması gerekmektedir. Bu nedenle Bilgi ve İletişim Güvenliği Rehberi’nin kimleri kapsıyor olduğu sorusuna net bir yanıt verilmesi ihtiyacının devam ettiği görülmektedir. Resmi Gazete’de yayımlanan 2019/12 sayılı genelgenin ardından ve bir yıl sonra, 20 Temmuz 2020 tarihinde Bilgi ve İletişim Güvenliği Rehberi ile ardından 10 Ekim 2020 tarihinde Bilgi ve İletişim Güvenliği Denetim Rehberi hazırlanmış ve tarafları etkilemeye başlamıştır.

Bilgi ve İletişim Güvenliği Rehberi, bilgi güvenliğine yönelik ulusal düzeyde alınması beklenen tedbirlerin yapılandırılmış hali olarak kabul edilebilecek, tüm kamu kurum ve kuruluşları ile kritik altyapı hizmeti veren işletmelerde yeni kurulacak bilgi sistemlerinin uyumlu olması beklenen yükümlülükleri belirlemiştir. Kamu kurum ve kuruluşları ile kritik altyapı hizmeti veren işletmelerden, Bilgi ve İletişim Güvenliği Denetim Rehberi’nde belirtilen süre içerisinde⁹² uyum faaliyetlerini tamamlamaları beklenmiştir.

Bu doğrultuda, T.C. Dijital Dönüşüm Ofisi Başkanlığı tarafından, ayrıca Bilgi ve İletişim Güvenliği Denetim Rehberi’nde belirlenen yükümlülüklerle uygunluğun denetim çalışmalarının yürütülmesi konusunda Bilgi ve İletişim

kararı uyarınca kritik altyapıları barındırmakta olan “Elektronik Haberleşme”, “Enerji”, “Finans”, “Ulaştırma”, “Su Yönetimi” ve “Kritik Kamu Hizmetleri” sektörleri.” S:9

⁹² Bilgi ve İletişim Güvenliği Rehberi’nde yer alan zaman planı, yayım tarihinden itibaren ilk 6 ay içerisinde Kritik Derecelendirme ve Boşluk Analizi yapılarak varlık gruplarının ve kritiklik derecelerinin belirlenmesini, mevcut durum ile birlikte boşluk analizi yapılması ile rehberle uyum için yapılması gerekenlere yönelik yol haritasının belirlenmesini öngörmüştür. Bundan sonraki süreçte 1, 2 ve 3 olarak belirlenen kritiklik derecelerine uygun seviyelerde yer alan tedbirlerin uygulanmasını beklemiş ve her halükârda bu çalışmanın 24 ay içerisinde tamamlanması konusunda kamu kurumları ile kritik altyapıları yönlendirmiştir.

Güvenliği Denetim Rehberi'nin takip edilmesi beklenmektedir. Yalnızca siber güvenlik önlemlerinin temin edilmesinin değil, aynı zamanda kontrol edilmesi ile varsa risklere karşı önlem alınması sürecinin bir parçası olarak kabul edilen denetimlerin, yılda en az bir kez gerçekleştirilmesi beklenmekte olup, bu hususta çalışacak kurumların da belirli standartları karşılaması gerekmektedir. Bilgi ve İletişim Güvenliği Denetim Rehberi, kurum ve kuruluşlara bilgi ve iletişim güvenliği uyum faaliyetlerinin denetiminde; denetimin planlanması, denetim prosedürlerinin uygulanması ve denetim sonuçlarının raporlanması konusunda izlenmesi gereken metodolojiye yer vermektedir.

Bilgi ve İletişim Güvenliği Denetim Rehberi kapsamındaki tüm kurum ve kuruluşların, denetim faaliyetlerini öncelikli olarak iç denetim birimlerinde görev alan ve bilgi teknolojileri alanında denetim yapmak üzere görevlendirilen iç denetçiler tarafından gerçekleştirilmesi esas alınmıştır. İç denetim birimlerinin bulunmadığı ya da iç denetim birimi olmasına rağmen, denetimi yürütecek yeterlik ve yetkinlikte denetçiye sahip olunmadığı hallerde denetim faaliyetlerinin bağımsız bir şekilde yürütülmesini sağlamak üzere, kurum içi diğer personel ya da diğer kamu kurum ve kuruluşlarından görevlendirilecek personel ile denetim faaliyetlerinin gerçekleştirilmesi gerekmektedir. Kurum ve kuruluşlar, iç kaynaklar ile denetim çalışmalarını gerçekleştiremediği durumda, denetimi hizmet alımı yolu ile gerçekleştirebilme imkanına sahiptir.

Denetim hizmeti alınacak firmaların ve personelinin sahip olması gereken kriterler ile bunların eğitim ve belgelendirme hususlarını içeren “Bilgi ve İletişim Güvenliği Rehberi Uyum Denetimi Hizmeti Sağlayan Personel ve Firma Belgelendirme Programı” T.C. Dijital Dönüşüm Ofisi Başkanlığı koordinasyonunda TSE ve TÜBİTAK BİLGEM iş birliği ile hayata geçirilmiştir.

Cumhurbaşkanlığı tarafından yayımlanan, 2019/12 sayılı Bilgi ve İletişim Güvenliği Tedbirleri'nde de belirtildiği üzere dijitalleşme beraberinde ciddi güvenlik risklerini getirmekte, bu risklerin zaman zaman milli güvenliği tehdit edecek boyutlara ulaşabileceği kabul edilmektedir. Gerek işlenen verilerin,

gerekse de kullanılan sistemlerin güvenliğini sağlanması bilinen savunma yöntemleri ve alanlarının yanında siber uzaya kaydığına, bu alanlarda da yerli teknolojiler ile ürünlerin kullanılması ulusal güvenlik politikalarının temelini teşkil eden kurallardan biri haline gelmiştir. Haberleşmede de gizliliğin sağlanması adına güvenlik önlemlerinin alınmasının teşvik edilmesi, siber tehdit bildirimlerinin en hızlı şekilde gerçekleştirilerek gerekli önlemlerin alınması, endüstriyel kontrol sistemlerinin kapalı şekilde kullanımı, internet erişiminde güvenlik zafiyeti oluşmasına imkân tanımayacak önlemlerin alınması yönünde yönlendirmeler yapan 2019/12 sayılı Genelge ile de siber güvenliğin ulusal düzeyde bir savunma anlayışının parçası olduğu görülmektedir.

3.1.4. Bilgi ve İletişim Güvenliği ve Denetim Rehberi

Ulusal Siber Güvenlik Stratejileri sayesinde siber güvenliğin, kamu güvenliğinin bir parçası olduğu kabul edilmiş ve deniz, hava, kara güvenliğinden sonra siber uzayda da güvenliğin sağlanması adına önemli adımlar atılmıştır. Bu alanda belirlenen yükümlülükler, Bilgi ve İletişim Güvenliği Rehberi sayesinde daha yapısal ve kapsayıcı bir şekil almış durumdadır. Temelde 12 hedefin⁹³ çevresine inşa edilmiş Bilgi ve İletişim Güvenliği Rehberinin, Ulusal Siber Güvenlik Stratejileri ile de paralel amaçlar izlediği görülmektedir. Ulusal siber güvenlik anlayışı bakımından pek çok otorite nezdinde kabul görmüş ve önem arz eden amaçlardan biri, yerli ve milli teknolojilerin geliştirilmesi ve desteklenmesidir. Siber güvenliğin bir kamu güvenliği meselesi haline gelmiş olması ile de bağlantılı şekilde, bu alanda yapılacak yatırımların iç kaynaklar aracılığı ile geliştirilmesi, bir bakıma dışa bağımlılığın azaltılması, savunulabilirlik açısından önemli ve bir yönüyle de siyasi bir kabul olarak da görülebilir. Bu minvalde belirlenen amaçlar ve alınması beklenen güvenlik tedbirleri de yerli ve milli teknolojinin gelişmesine hizmet gayesi gütmektedir.

⁹³ Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, “Bilgi ve İletişim Güvenliği Rehberi”, Temmuz 2020, s.11.

Milli kaynakların kullanılmasının yanında, Bilgi ve İletişim Güvenliği Rehberi, güvenlik açısından pratikte karşılık bularak etkili olması ve bu etkinliğinin korunabilmesi için ürün ve teknolojilerden bağımsız, uygulayıcısı olan tüm kurum ve kuruluşların yapısına uyumlu ve uygulanabilir, ihtiyaçlar ve değişen şartlara göre devamlılığı sağlayabilen, mevzuata, ulusal ve uluslararası standartlara uyumlu olma gibi amaçları içeren bir yaklaşım ile hazırlanmıştır.

Bilgi ve İletişim Güvenliği Rehberi, alınması gereken önlemlerin en başına kurum içinde yer alan varlık gruplarının belirlenmesini koymuştur. Bir organizasyonun faaliyetlerini sürdürebilmesi için sahip olduğu ve korunması gereken bilgiler, sistemler, cihazlar, fiziksel ya da dijital ortamlar, nesneler, kaynaklar ve süreçlerin tamamı olarak kabul edilebilecek varlık gruplarının belirlenmesi, korunması gereken varlıkların neler olduğunun ortaya konabilmesi adına en temel adım olarak kabul edilmektedir. Varlık gruplarının tespitinden sonra alınması gereken güvenlik önlemlerinin kritiklik derecesinin belirlenmesi adına bir anketle başlayan ve anketin neticesine göre 3 seviyede kritiklik derecesi belirleyen ilgili Rehberin, güvenlik tedbirlerine ilişkin yatırımın risk açısından önem arz eden alanlara ayrılmasına ve kaynakların etkin kullanımına önem verdiği görülmektedir. Rehberde kritiklik derecesinin belirlenmesinde, işlenen veri ile ilgili unsurlar ve etki alanının göz önünde bulundurulması gerekmektedir. İşlenen veri ile ilgili boyutlar arasında, bilginin gizliliği, bütünlüğü ve erişilebilirliği yer almaktadır. Bilginin yetkisiz kişilerin erişimine karşı korunması, bilginin tam ve doğru olma durumunun korunması ve bilginin ihtiyaç duyulduğu anda yetkili kişilerce ulaşılabilir ve kullanılabilir durumda olması boyuta ilişkin özelliklerdir. Etki alanı ise, varlık grubuna bağımlı olan diğer varlıklar, bilgi güvenliği ihlali meydana geldiğinde etkilenebilecek kişi sayısı, kurumsal sonuçlar, varlık grubunun hizmet verdiği sektöre etkisi ve toplumsal sonuçlar bulunmaktadır. Bu unsurların değerlendirilmesi, varlık gruplarının kritiklik derecesinin belirlenmesinde önemli bir rol oynar ve organizasyonun bilgi güvenliği stratejilerinin etkin bir şekilde planlanmasına yardımcı olur. Bunun yanı sıra izlenebilir, modüler, ulusal ve uluslararası mevzuat ya da standartlar ile de

uyumlu şekilde geliştirilen tedbirlerin devamlılığının sağlanması da odaklanılan diğer önemli amaçlar arasında yer almaktadır. Mevcut durumda alınan güvenlik önlemlerinin analizi ile güvenlik önlemi alınmayan durumlara ilişkin boşluk analizlerinin ardından, gerekli önlemlerin nasıl uygulamaya geçirileceği, önlemlerin alınması ile kontrolü ve gerekmesi halinde önlemlere ilişkin güncellemelerin yapılması Bilgi ve İletişim Güvenliği Rehberi kapsamındaki kurumlardan beklenenler arasındadır.

Bilgi ve İletişim Güvenliği Rehberi, varlık grubuna yönelik sınıflandırmaya da uygun şekilde, aşağıda verilen 6 ana başlık altında alınması beklenen tedbirlerin nelere yönelik ve ne şekilde olduğunu belirlemiştir.

Tablo 3. 3. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Bilgi ve İletişim Güvenliği Rehberi Varlık Gruplarına Yönelik Güvenlik Tedbirleri ⁹⁴

Ağ ve Sistem Güvenliği
Uygulama ve Veri Güvenliği
Taşınabilir Cihaz ve Ortam Güvenliği
Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği
Personel Güvenliği
Fiziksel Mekanların Güvenliği

Varlık grubunun yanı sıra, ayrı bir başlık olarak uygulama ve teknoloji alanlarına yönelik güvenlik tedbirlerine de yer verilmiştir.

⁹⁴ Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, Bilgi ve İletişim Güvenliği Rehberi, Temmuz 2020, s.35-46

Tablo 3. 4. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Bilgi ve İletişim Güvenliği Rehberi Uygulama ve Teknoloji Alanlarına Yönelik Güvenlik Tedbirleri⁹⁵

Kişisel Verilerin Güvenliği
Anlık Mesajlaşma Güvenliği
Bulut Bilişim Güvenliği
Kripto Uygulamaların Güvenliği
Kritik Altyapıların Güvenliği
Yeni Gelişmeler ve Tedarik

Kritik altyapıların da ayrı bir bölüm olarak yer aldığı bu başlığın altında, enerji ve elektronik haberleşme dışındaki kritik altyapılara ilişkin doğrudan bir yönlendirme yapılmamış olması da ayrıca incelemeyi gerektirmektedir. Zarar görmesi halinde karşılamak etkilere bakılarak riski seviyesinin yüksek olduğu görülen ve dolayısıyla ayrıca güvenlik tedbirleri belirlenen kritik altyapılara yönelik, ENISA tarafından da benzer bir yaklaşım belirlenmiş olup, kritik altyapıların siber uzayda korunması, tüm siber uzayın korunmasına ilişkin basamaklardan biri olarak kabul edilmiştir⁹⁶. Bu bakış açısıyla kritik altyapılar için yeterli korumanın sağlanamıyor olması siber uzayda yeterli koruma olmadığı anlamına gelmektedir.

⁹⁵ age. S. 14-185.

⁹⁶ ENISA, “ENISA overview of cybersecurity and related terminology”, Temmuz 2017, s.4.

Enerji sektöründe oldukça yaygın şekilde kullanılan endüstriyel kontrol sistemlerinin⁹⁷ güvenliğine yönelik olarak da ilave tedbirlerin getirilmesi gerek kullanım alanı ve önemi gerekse de kendine has özellikleri itibariyle oldukça değerli bir detaydır. Rehber’de yer alan enerji sektörü özelinde belirlenmiş güvenlik tedbirleri aşağıda sıralanmıştır.

- Cihaz konfigürasyonları
- Ağ erişim kontrolü
- Ağ segmentasyonu
- Kimlik doğrulama
- Erişim yönetimi
- Fiziksel erişim güvenliği
- Sistem sürekliliğinin sağlanması
- Veri manipülasyonunun engellenmesi
- Kullanıcı erişim yönetimi
- SSL/TLS korumalı iletişim
- GPS iletişim ve senkronizasyonunun güvenliği
- Ekipman güvenliğinin sağlanması

⁹⁷ Endüstriyel kontrol sistemleri (Industrial Control Systems), endüstriyel işletmelerde üretim süreçlerini kontrol etmek ve otomatize etmek için kullanılan bir tür bilgisayar sistemidir. Bu sistemler, genellikle elektrik, su, gaz, petrol ve kimyasal işlemleri gibi endüstriyel tesislerde kullanılır. Endüstriyel kontrol sistemleri, çeşitli bileşenlerden oluşur ve genellikle bir kontrol merkezi veya kontrol odası aracılığıyla yönetilir. EKS’lerin temel bileşenleri arasında sensörler, kontrol cihazları, veri toplama ve analiz ekipmanları, iletişim ağları ve kullanıcı arayüzleri bulunur. Bu sistemler, üretim süreçlerinin verimliliğini artırmak, maliyetleri düşürmek, kaliteyi iyileştirmek ve güvenliğini sağlamak için kullanılır.

- Tehdit istihbaratı yönetimi
- Otoritelerle iletişim
- Veri iletimi⁹⁸

Belirlenen tüm önlemlerin yanında, yalnızca enerji sektöründe faaliyet gösteren taraflara yönelik farklı önlemlerin belirlenmiş olması ilgili sektörün siber güvenlik bakış açısındaki önemini de ortaya koymaktadır. Herhangi bir üretim tesisi yahut işletmeden farklı olarak tüm toplumu ilgilendiren ve pek çok sürecin de işlerliğine kaynaklık eden enerji sektörünün sahip olduğu sistemlerin güvenliği de etki alanı ile doğru orantılı şekilde daha fazla detay içermektedir.

Bilgi ve İletişim Güvenliği Rehberi ile belirlenmiş tüm yükümlülüklerin tam ve doğru bir şekilde uygulanıp uygulanmadığının kontrolü adına da denetimlerin yapılması beklenmektedir. Değişen teknolojilere uygun şekilde güvenlik önlemlerinin de güncellenmesi, sızma testlerinin yapılması ve eklenmiş yeni sistemlere de uygun güvenlik tedbirlerinin entegre edilmiş olması, kesintisiz bir güvenlik sağlamak adına gerekli adımlardan yalnızca bir kaçıdır. Bu nedenle hazırlanan Bilgi ve İletişim Güvenliği Denetim Rehberinin amacı ise Bilgi ve İletişim Güvenliği Rehberi kapsamında yer alan kurumların bu çalışmalarını yerine getirip getirmediğinin kontrolüne yöneliktir. Siber güvenlik yönetimi kapsamında belirlenen adımlardan olan kontrol etme ve önlem alma sürecinin bir parçası olan denetimin, yılda en az bir kez gerçekleştirilmesi, kurumlar tarafından gerekli planlamaların yapılması ve işletilmesi, denetim çalışmalarının Bilgi ve İletişim Güvenliği Denetim Rehberinde belirlenmiş metodolojide, denetimi yürütecek ekibin ise alanında yetkin ve belirlenen koşulları taşıyor olması, denetim çalışmalarının verimliliği adına ortaya konan beklentilerdir. Denetimin bağımsız bir şekilde planlanması, yürütülmesi ve raporlanması konularında kurumlara ve denetçilere yol göstermek amacıyla hazırlanan Bilgi ve İletişim Güvenliği Denetim Rehberi, özünde siber güvenlik önlemlerinin olması gerektiği

⁹⁸ age. S. 179-180.

şekilde sağlanıp sağlanmadığının tespitine ilişkin usul ve esasları içermektedir. Ayrıca ilgili tarafların denetimlerinin tamamlamalarının ardından, çıktılarının Dijital Dönüşüm Ofisi'ne iletilmesi de beklenmektedir. Bu raporlardan elde edilen çıktılarına göre DDO'nun gözetim faaliyetlerine devam edeceği belirtilmekle birlikte, bulguların önem derecesine göre nasıl bir yol izlenmesi gerektiğine ya da denetim yaptırılmaması, ilgili tedbirlerin yerine getirilmemiş olması halinde kurumlara ne gibi yaptırımların uygulanacağı ya da uygulanıp uygulanmayacağına yönelik net bir çerçeve çizilmemiştir⁹⁹. Her ne kadar Bilgi ve İletişim Güvenliği Denetim Rehberi'nde DDO'un denetim sonuçları üzerinden ilgili mevzuat çerçevesinde gözetim faaliyetlerini yürüteceği belirtilmişse de bir yaptırımdan bahsedilmiyor olduğu da görülmektedir.

3.1.5. Kişisel Verilerin Korunması Kanunu ve İkincil Düzenlemeleri

7 Nisan 2016 tarihinde kabul edilen 6698 sayılı Kişisel Verilerin Korunması Kanunu, amacı itibarıyla gerçek kişilere ait olup, onların kimliğini belli ya belirlenebilir kılacak kişisel verilerin işlenmesi esnasında başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektedir. Bu bağlamda kişisel veri¹⁰⁰ ve işlenmesine¹⁰¹ yönelik esasların yanında kişisel verilerin korunmasına ilişkin olarak da veri sorumluları¹⁰² ile veri işleyenlere¹⁰³

⁹⁹ Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, “Bilgi ve İletişim Güvenliği Denetim Rehberi”, Ekim 2021, s.35.

¹⁰⁰ 6698 sayılı Kanun uyarınca kişisel veri “ Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,” ifade etmektedir.

¹⁰¹ 6698 sayılı Kanun uyarınca kişisel verilerin işlenmesi “Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi,” ifade etmektedir.

¹⁰² 6698 sayılı Kişisel Verilerin Korunması Kanunu 3. Madde, 1. Fıkra, 1 bendinde “Veri sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi,” şeklinde tanımlanmaktadır.

¹⁰³ 6698 sayılı Kişisel Verilerin Korunması Kanunu 3. Madde, 1. Fıkra, 2 bendinde “Veri işleyen: Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi,” şeklinde tanımlanmaktadır.

yükümlülükler atfetmiş durumdadır. 6698 sayılı Kanun, verilerin işlenmesine yönelik düzenlenmelerle birlikte, özel nitelikli verileri¹⁰⁴ de belirleyerek bunların işlenmesine yönelik ayrıca yeterli önlemlerin alınması gerektiğini belirtilmiş ve buna ilişkin olarak 2018 yılında 2018/10 sayılı Kurul kararı yayımlamıştır¹⁰⁵. Bu kapsamda Kurul'un almış aldığı kararların bir kısmı eğitim verilmesi, gizlilik sözleşmesi imzalanması, fiziksel ortamların güvenliğinin sağlanması, yetki kontrollerinin periyodik olarak yapılması gibi idari unsurlara ilişkinken, bir kısmı da doğrudan siber güvenlik adına alınan siber savunma yöntemlerine ilişkindir. Örneğin 2018/10 sayılı Kurul kararında,

- Verilerin kriptografik yöntemler kullanılarak muhafaza edilmesi,
- Kriptografik anahtarların güvenli ve farklı ortamlarda tutulması,
- Verilerin üzerinde gerçekleştirilen işlemlere ilişkin log kayıtlarının alınması,
- Verilerin bulunduğu ortamlara ait güvenlik güncellemelerinin takip edilmesi, güvenlik testlerinin düzenli yapılması/yaptırılması, sonuçlarının kayıt altına alınması,
- Verilere bir yazılım aracılığı ile erişiliyorsa bu yazılıma ait kullanıcı yetkilendirmelerinin yapılması, bu yazılımların güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,
- Verilere erişim için gerekli yetkilendirmelerin yapılması,
- Verilere erişim için çift faktörlü kimlik doğrulamanın kullanılması,

¹⁰⁴ 6698 sayılı Kişisel Verilerin Korunması Kanunu 6. Madde, 1. Fıkra, uyarınca “Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir.”

¹⁰⁵ Kişisel Verileri Koruma Kurulu, "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" ile ilgili Kişisel Verileri Koruma Kurulunun 31/01/2018 Tarihli ve 2018/10 Sayılı Kararı link: <https://www.kvkk.gov.tr/Icerik/4110/2018-10>, (Son erişim tarihi: 22.06.2024)

- Verilerin bulunduğu ortama ilişkin fiziksel güvenlik önlemlerinin alınması,
- Verilerin aktarımında şifreli kurumsal e-posta hesaplarının yahut KEP hesaplarının kullanılarak aktarılması,
- Verilerin taşındığı araçların kriptografik yöntemlerle şifrelenmesi ve kriptografik anahtarın farklı ortamda tutulması,
- VPN kurularak veya sFTP yöntemiyle veri aktarımının gerçekleştirilmesi gerekliliklerinden bahsedilmiştir.

Kişisel Verileri Koruma Kurumu ayrıca genetik verilerin işlenmesine¹⁰⁶ ve biyometrik verilerin¹⁰⁷ işlenmesine yönelik rehberler ile de ilgili verilerin işlenmesi esnasında uyulması beklenen güvenlik önlemlerini izah etmiştir. Yalnızca özel nitelikli verilerin değil, her türlü kişisel verinin korunması ve güvenliğine ilişkin, Kişisel Verileri Koruma Kurumu tarafından hazırlanmış pek çok rehber ve yardımcı doküman bulunmaktadır¹⁰⁸. Yayımlanan bu rehberlerin içinde yer alan teknik tedbirler ve veri güvenliğine ilişkin yönlendirmeler özü itibarıyla siber güvenlik tedbirlere karşılık gelmektedir. İlgili yayınların, veri güvenliğine ilişkin yükümlülükler bağlamında yönlendirici ve teknik içerikler de olduğu, iyi uygulama örneklerinin yayımlanmasına katkı sağladığı görülmektedir. Bunun yanında hazırlanan tebliğ, yönetmelik ve ilke kararların da

¹⁰⁶ Kişisel Verileri Koruma Kurulu, “Genetik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber”, link: <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/703442e0-690c-4618-91c3-83e7583170ca.pdf> (Son erişim tarihi: 22.06.2024)

¹⁰⁷ Kişisel Verileri Koruma Kurulu, “Biyometrik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber”, link: <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/bd06f5f4-e8cc-487e-abe1-d32dc18e2d7e.pdf> (Son erişim tarihi: 22.06.2024)

¹⁰⁸ Kişisel Verileri Koruma Kurulu, “Kişisel Veri Güvenliği Rehberi”, link: <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7512d0d4-f345-41cb-bc5b-8d5cf125e3a1.pdf> (Son erişim tarihi: 22.06.2024), “Mobil Uygulamalarda Mahremiyetin Korunmasına Yönelik Tavsiyeler”, link: <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/8ba209bb-fa93-4479-84f0-dd55aac97a0f.pdf>, (Son erişim tarihi: 22.06.2024) “Seçim Faaliyetlerinde Kişisel Verilerin Korunması Rehberi”, link: <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/a4622d77-624b-4105-8064-14933319abc1.pdf>, (Son erişim tarihi: 22.06.2024)

6698 sayılı Kanunun, Kurulun görev ve yetkileri başlıklı 22. Maddesinin 1. Fıkrasının f bendine yer alan “veri güvenliğine ilişkin yükümlülükleri belirlemek amacıyla düzenleyici işlem yapmak” şeklindeki sorumluluğuna ilişkin olduğunu kabul etmek de yanlış olmayacaktır¹⁰⁹. Zira Kurul yapacağı bir inceleme neticesinde KVKK’nin 12. Maddesine¹¹⁰ yer alan ve veri güvenliğine ilişkin yükümlülükler başlığını taşıyan ilgili hükme göre veri sorumluları ve veri işleyenleri, kişisel veriler ile sınırlı olmak üzere

- Hukuka aykırı işlemenin önlenmesi,

- Hukuka aykırı olarak erişilmesinin önlenmesi,

- Muhafazasının sağlanması amacıyla uygun güvenlik düzeyinin temin edilmesi için belirlenen her türlü teknik ve idari tedbirlerin almasını zorunlu tutmuştur. Bunun yanı sıra belirlenen yükümlülüklerin ve dolayısıyla veri güvenliğine ilişkin tedbirlerin yerine getirildiğinin teyidi amacıyla ilgililere denetim yapma yükümlülüğü de getirilmiştir. Veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemiş olması halinde bahsi geçen kanunun 18. Maddesinin birinci fıkrasının be bendi¹¹¹ gereği Kurul’un idari para cezası

¹⁰⁹ Samet Saygı, “6698 Sayılı Kanun’un Sistematiğinde Yargısal Başvuru Yolları”, Cilt:2, Sayı:2, 2020, 30-61, s.56-57.

¹¹⁰ 6698 sayılı Kişisel Verilerin Korunması Kanunu, Veri güvenliğine ilişkin yükümlülükler *MADDE 12- (1) Veri sorumlusu;*

a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,

b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,

c) Kişisel verilerin muhafazasını sağlamak,

amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır. (2) Veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, birinci fıkrada belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur. (3) Veri sorumlusu, kendi kurum veya kuruluşunda, bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır. (4) Veri sorumluları ile veri işleyen kişiler, öğrendikleri kişisel verileri bu Kanun hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamazlar. Bu yükümlülük görevden ayrılmalardan sonra da devam eder. (5) İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.

¹¹¹ 6698 sayılı Kişisel Verilerin Korunması Kanunu 18. Madde, 1. Fıkra, b bendi (1) *Bu Kanunun;*

a) 10 uncu maddesinde öngörülen aydınlatma yükümlülüğünü yerine getirmeyenler hakkında 5.000 Türk lirasından 100.000 Türk lirasına kadar,

uygulama hakkı haizdir. Dolayısıyla hukuk düzeni içinde bağlayıcılığı konusunda tartışma yaşanması ihtimali bulunuyor olsa da KVKK yayınlarının, kişisel verilerin korunmasına ilişkin olarak siber güvenlik alanında alınması gereken önlemlere yönelik yayınlarının dikkate alınması gerekmektedir.

6698 sayılı Kanun ile getirilen yükümlülüklerin yalnızca kişisel verilerin işlenmesine yönelik olduğu, veri sorumlularının, veri güvenliğini sağlayamaması halinde ödemekle yükümlü oldukları idari para cezası dışında ilgili kanunda verilerinin güvenliği zarar gören kişilere yönelik bir düzenleme bulunmadığını ya da kişisel veri kabul edilmeyen verilere ilişkin de yükümlülük getirmediği görülmektedir. Farklı kanunlar uyarınca hak iddiasında bulunmak mümkünse de mevzuatın amaç maddesiyle de bağlantılı şekilde özel hayatın gizliliği başta olmak üzere temel hak ve özgürlüklerin korunması ve verilerin işlenmesine yönelik gerçek ve tüzel kişilere getirilmiş yükümlülükleri belirleme ihtiyacına binaen düzenlenmiş olduğu görülmektedir. Bunun yanı sıra ilgili kişinin, veri sorumlusuna karşı, verilerinin işlenmesi nedeniyle hak talebinde bulunabileceği 6698 sayılı Kanun'un 11. Ve 14. Maddelerinde sayılmıştır. 11. Maddenin g fıkrası bu hakkın veri sorumlusuna bir ilgili kişi başvurusu olarak iletilebileceğini, 14. Maddesi ile genel hükümler uyarınca tazminat hakkının saklı olduğunu düzenlemektedir. Sorumluluk kısmında konunun detayları ve işlevselliği de ayrıca incelenecektir.

3.1.6. Sermaye Piyasası Kanunu Ve İkincil Düzenlemeleri

6362 sayılı Sermaye Piyasası Kanunu, amacı itibarıyla sermaye piyasası için güvenilir, şeffaf, etkin, istikrarlı, adil ve rekabetçi bir ortamda işleyişin ve gelişmenin sağlanması, yatırımcıların hak ve menfaatlerinin korunması için gerekli işleyiş ve kontrol kurallarını belirlemek amacıyla 30.12.2012 tarihinde Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. Bu kapsam doğrultusunda, sermaye piyasası araçları, bu araçların ihracı, ihraççılar, halka arz edenler,

b) 12 nci maddesinde öngörülen veri güvenliğine ilişkin yükümlülükleri yerine getirmeyenler hakkında 15.000 Türk lirasından 1.000.000 Türk lirasına kadar,

sermaye piyasası faaliyetleri, sermaye piyasası kurumları, borsalar ile sermaye piyasası araçlarının işlem gördüğü diğer teşkilatlanmış piyasalar, piyasa işleticileri, Türkiye Sermaye Piyasaları Birliği, Türkiye Değerleme Uzmanları Birliği, merkezî takas kuruluşları, merkezî saklama kuruluşları, Merkezî Kayıt Kuruluşu ve Sermaye Piyasası Kurulu'nun 6362 sayılı Kanun hükümlerine tabi olacağı belirlenmiştir.

Günümüz koşulları itibarıyla iş ve işlemlerin bilgi sistemleri üzerinden yürütülmesinin zaruriyeti gereği, sermaye piyasacılarının hukuka uygun ve güvenilir şekilde faaliyet gösterdiğine ilişkin itimadın sağlanması gerekmektedir. Sermaye Piyasası Kanunu'nunda yer alan 128. Maddesinin birinci fıkrasının h bendi¹¹² uyarınca oluşturulmuş Bilgi Sistemleri Yönetimi Tebliği, bu güven ortamının yaratılabilmesi adına, sermaye piyasası kurumları, halka açık şirketler, borsalar, öz düzenleyici kuruluşlar ile Tebliğin kapsamında giren tarafların bilgi sistemlerinde bulunması gereken siber güvenlik yükümlülüklerini de içermektedir.

BSYT'in, kapsamı 2. Madde de belirtilen taraflar ile sınırlı olacak şekilde, sermaye piyasasının işletimi ve yönetiminin adil bir şekilde yürütülebilmesi, iş sürekliliğinin sağlanması ile güvenli kalabilmesi adına gerekli yükümlülükleri belirlemek adına yayımlanmıştır. BSYT, temel siber güvenlik ilkelerine uygun şekilde ve risk temelli bir yaklaşım ile,

- Varlıkların tespiti ile önem derecesine göre sınırlanması,
- Ağ güvenliğinin sağlanması,

¹¹² 6362 sayılı Sermaye Piyasası Kanunu, Kurulun görev, yetki ve sorumlulukları
MADDE 128 – (1) Kurulun görev ve yetkileri şunlardır:

...

h) Sermaye piyasası kurumlarının, halka açık şirketlerin, borsaların ve öz düzenleyici kuruluşların bilgi sistemlerinin işletimine ve bu Kanun çerçevesindeki denetimine ilişkin usul ve esasları belirlemek

...

- Kimlik doğrulama süreçlerini uygun şekilde planlanması,
- Yapılan işlemlerin kayıtlarının tutulması,
- Gerekli kontrollerin belirlenen periyotlarda yapılması,
- Sızma testlerinin yapılması ve yapılırken dikkate alınması gereken usul ve esaslar,
- Bilgi güvenliği ihlallerinin tespiti ile kayıtların, çözümlerin belirlenmesi, personellerin bilgilendirilmesi, kök sebeplerin tespiti ile düzeltici aksiyonların alınması ile kritik ihlallerin yönetime bildirilmesi,

• Bilgi güvenliği ihlallerine ilişkin bildirimde bulunmak isteyen müşterilere gerekli imkanların sağlanması gibi yükümlülükler belirlemektedir. Bilgi Sistemleri Bağımsız Denetim Tebliği, BSYT’de belirlenen yükümlülüklerin kontrol ve denetimine ilişkin usul ve esaslara yönelik olup, ilgili denetimin halka açık şirketlerin bağımsız denetimine ilişkin yükümlülükleriyle koordineli şekilde yürütmesini amaç edinmektedir. Siber güvenliğe ilişkin önlemlerin alınmasını şart koşuyor olsa da BSYT ve dayanağı olan Sermaye Piyasası Kanunu’nun koruduğu değerler, yatırımcıların güvenli bir şekilde yatırım yapabilmesi, sermayenin adil ve rekabetçi bir şekilde piyasada değer kazanması ile izlenir, şeffaf bir yatırım ortamının oluşturulmasından ibaret olduğundan, özü itibarıyla siber güvenliğin bu anlamda bir amaç değil araç olduğunu kabul etmek gerekir. Halka açık şirketlerin, BSYT’de belirlenen yükümlülükleri yerine getirilmemiş olduğunun, Bilgi Sistemleri Bağımsız Denetim Tebliği hükümleri uyarınca tespiti halinde yerine getirilmemiş yahut eksik yerine getirilmiş yükümlülükleri nedeniyle idari yaptırımlara tabi kalması ihtimali bulunmaktadır.

3.1.7. Türk Ceza Kanunu

İdare hukukunun konusuna giren düzenlemelerin yanında ceza hukuku bağlamında da bilişim sistemlerinde işlenen ve siber güvenliği tehdit edecek nitelikteki fiillere ilişkin düzenlemeler mevcuttur. Dünya üzerinde yaygın

kullanımı siber suçlar olan ilgili suçların, ülkemiz mevzuatında ismi bilişim suçları olarak geçmektedir. Amacı itibariyle kişilerin hak ve özgürlüklerine zarar verilmesinin yanında kamu düzeni ve güvenliğinin ihlal edilmesi amacına aykırı eylemlerin cezalandırılması olan ve ceza yargılamasının konusuna girenlerle sınırlı olan Türk Ceza Kanunu hükümlerinde düzenlenen bilişim alanındaki suçlar,

1. Bilişim sistemine girme¹¹³,
2. Sistemi engelleme, bozma, verileri yok etme veya değiştirme¹¹⁴
3. Banka veya kredi kartlarının kötüye kullanılması¹¹⁵

¹¹³ 5237 sayılı Türk Ceza Kanunu, Bilişim sistemine girme Madde 243- (1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıla kadar hapis veya adli para cezası verilir.

(2) Yukarıdaki fıkra tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir.

(3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur.

(4) Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleyen kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır.

¹¹⁴ 5237 sayılı Türk Ceza Kanunu, Sistemi engelleme, bozma, verileri yok etme veya değiştirme Madde 244- (1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(2) Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.

(3) Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır.

(4) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezasına hükmolunur.

¹¹⁵ 5237 sayılı Türk Ceza Kanunu, Banka veya kredi kartlarının kötüye kullanılması Madde 245 (1) Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır.

(2) Başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üreten, satan, devreden, satın alan veya kabul eden kişi üç yıldan yedi yıla kadar hapis ve onbin güne kadar adli para cezası ile cezalandırılır.

(3) Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, dört yıldan sekiz yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır.

(4) Birinci fıkra yer alan suçun;

4. Yasak cihaz veya programlar¹¹⁶ başlıklarını taşıyan 4 suçla sınırlı olup, işleyen tüzel kişilere yönelik olarak da güvenlik tedbirlerinin hükmolunmasına imkan tanımaktadır.

Belirtilen suçların eylemi kabul edilecekler hususlar,

- Bilişim sistemine/parçasına hukuka aykırı şekilde girilmesi,
- Bilişim sistemine/parçasında hukuka aykırı bulunulması,
- Tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi,
- Bilişim sistemi/parçasının içerdiği verilerin sisteme girilmesi yüzünden yok edilmesi,
- Bilişim sistemi/parçasının içerdiği verilerin sisteme girilerek değiştirilmesi,
- Bilişim sistemi içinde gerçekleşen veri nakillerinin sisteme gerilmeksizin izlenmesi,
- Bilişim sistemi arasında gerçekleşen veri nakillerinin sisteme gerilmeksizin izlenmesi,

a) Haklarında ayrılık kararı verilmemiş eşlerden birinin,

b) Üstsoy veya altsoyunun veya bu derecede kayın hısımlarından birinin veya evlat edinen veya evlâtlığın,

c) Aynı konutta beraber yaşayan kardeşlerden birinin,

zararına olarak işlenmesi hâlinde, ilgili akraba hakkında cezaya hükmolunmaz.

(5) Birinci fıkra kapsamına giren fiillerle ilgili olarak bu Kanunun malvarlığına karşı suçlara ilişkin etkin pişmanlık hükümleri uygulanır.

¹¹⁶ 5237 sayılı Türk Ceza Kanunu, Yasak cihaz veya programlar Madde 245/A (1) Bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun; münhasıran bu Bölümde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için yapılması veya oluşturulması durumunda, bunları imal eden, ithal eden, sevk eden, nakleden, depolayan, kabul eden, satan, satışa arz eden, satın alan, başkalarına veren veya bulunduran kişi, bir yıldan üç yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır.

- Bilişim sisteminin işleyişinin engellenmesi,
- Bilişim sisteminin işleyişinin bozulması,
- Bilişim sistemindeki verilerin bozulması,
- Bilişim sistemindeki verilerin yok edilmesi,
- Bilişim sistemindeki verilerin değiştirilmesi,
- Bilişim sistemindeki verilerin erişilemez kılması,
- Bilişim sistemine veri yerleştirilmesi,
- Bilişim sisteminde var olan verilerin başka yere gönderilmesi,
- Bilişim sistemindeki yapılan eylemler neticesinde eylemi gerçekleştiren yahut başkası yararına haksız bir çıkarın elde edilmesi,
- Bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun; bilişim suçlarının işlenmesi yahut bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için yapılması veya oluşturulması,
 - Üretilmesi,
 - Temin edilmesi,
 - Sevk edilmesi,
 - Nakledilmesi,
 - Depolanması,
 - Kabul edilmesi,
 - Satılması,

- Satışa aracılık edilmesi,
- Satın alınması
- Başkalarına verilmesi
- Yalnızca bulundurulması

şeklinde sıralanabilir.

Sayılanların dışında, banka veya kredi kartlarının kötüye kullanılmasına ilişkin eylemler de suç olarak kabul edilmiştir. Görünüşü itibariyle banka ve kredi kartlarının ele geçirilmesi yahut elde bulundurulmasının bilişim suçları ile bağlantılı olmadığı düşünülecekse de banka sistemlerine yetkisiz giriş sağlanması, bu sistemlerin yetkisiz şekilde kullanımı, yarar sağlanması ya da sisteme yetkisiz şekilde giriş imkanı sağlayabilecek nitelikte banka yahut kredi kartı oluşturuluyor olması gibi eylemlerin, bilişim sistemlerine yetkisiz erişim ve sistemde yetkisiz mühadele unsurlarını barındırdığı görülecektir. Suçun işlenmesi, banka veya kredi kartının ele geçirilmesi veya kullanılması gibi eylemlerin, genellikle elektronik yöntemlerle gerçekleştirilmesi, kart bilgilerinin çalınması, kopyalanması veya sahtecilik amacıyla kullanılması gibi eylemler esnasında bilişim sistemlerinin kullanılması yahut bilişim sistemlerinin güvenlik açıklarının sömürülmesini gerektirmektedir. Ayrıca banka veya kredi kartı bilgilerinin ele geçirilmesi veya sahtecilik amacıyla kullanılması, kişisel ve finansal bilgilerin izinsiz olarak ele geçirilmesi anlamına da geldiğinden aynı zamanda veri ihlalini de bünyesinde barındırmaktadır. Kartlı ödeme sistemlerinin arkasında ve fiziki dünyada bıraktıkları etkinin yanı sıra, büyük bir sanal ortam ayağının ve dijital bankacılık hizmetlerinin de bulunması ve elde edilen kart bilgilerinin bu alanda da kullanımına imkan veren bilgiler içerdiği de unutulmamalıdır¹¹⁷.

¹¹⁷ Enes Bakkaloğlu, “Gerçek Banka veya Kredi Kartlarının Kötüye Kullanılması (TCK. 245/1)” Oniki Levha Yayıncılık, 1. Baskı, Mart 2022, s.32.

5237 sayılı Kanunu'nun onuncu bölümünde ve Bilişim Suçları başlığı altında yer alan suçların yanı sıra, ilgili Kanun'da farklı kısımlarda düzenlenmiş ancak bilişim sistemlerinin hukuka aykırı şekilde kullanımıyla gerçekleştirilen farklı suçların da bulunduğunu vurgulamak gerekir¹¹⁸. Özellikle özel hayata ve hayatın gizli alanına karşı suçlardan bazılarının, siber saldırı niteliğinde kabul edilecek eylemlere karşılık geldiği, örneğin kişiler arasındaki haberleşmenin gizliliğinin ihlalinin, siber uzayda yer alan e-posta, sosyal medya uygulamalarında yer alan mesajlaşma özelliğine yetkisiz şekilde erişilmesi ya da benzer şekilde telefon üzerinden ancak internet aracılığı ile kullanılan haberleşme araçları ile gerçekleştirilen haberleşmenin, yetkisiz şekilde erişimi ile gizliliğinin ihlal edilmesi de siber saldırı yöntemlerinden birinin kullanımı ile gerçekleştirilebilecek nitelikte suçlardır.

Belirtilen suçlar hakkında farklı görüşler bulunuyor olsa da,

- TCK m. 243'te düzenlenen suç ile bilişim sistemlerinin güvenliği hukuki değerinin korunması amaçlandı¹¹⁹,
- TCK m. 244 ile mülkiyet ve fikri mülkiyetin korunmasının yanında bilişim sistemlerinin bütünlüğü ile güvenliğinin korunması amaçlarının öne çıktığı¹²⁰,
- TCK m.245 ile mal varlığının korunmasına yönelik unsurların da mevzu bahis edilebileceği ancak bilişim alanında güvenliğin sağlanmasıyla,

¹¹⁸ 5237 sayılı Kanun'da yer alan Kişisel verilerin kaydedilmesi, (Madde 135), Verileri hukuka aykırı olarak verme veya ele geçirme, (Madde 136), Verileri yok etmeme (Madde 138), Haberleşmenin gizliliğinin ihlali suçu (Madde 132), Hakaret (Madde 125), Haberleşmenin engellenmesi suçu (Madde 124), Bilişim sisteminin kullanılması yoluyla işlenen hırsızlık suçu (Madde 142/2-e), Bilişim sisteminin kullanılması yoluyla işlenen dolandırıcılık suçu (Madde 158/1-f) bilişim sistemleri vasıtasıyla işlenebilen ve bu yönüyle de siber saldırı kabul edilebilecek nitelikteki diğer suçlardır.

¹¹⁹ Büşra Özçelik, “Bilişim Sistemine Girme Suçu” Oniki Levha Yayıncılık, 1. Baskı, Şubat 2021, s.50.

¹²⁰ Mehmet Can Karagöz, “Bilişim Sistemleri Teorisine Giriş İle Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu” Oniki Levha Yayıncılık, 1. Baskı, Ekim 2020, s.154-155.

ekonomik sistemler üzerinden bireylerin maddi korunmalarının yer aldığı karma nitelikte bir korumanın gerçekleştirilmesinin amaçlandığı ve

- TCK m.245/A aracılığıyla karma nitelikte ancak bilişim sistemlerine güvenin devamlılığının sağlanması amacını¹²¹ taşıdığına ilişkin görüşler bulunmaktadır.

Bununla birlikte ilgili suçlara ilişkin herkesin fail sıfatını taşıyabileceği görülmektedir. Ancak ceza sorumluluğun şahsiliği sebebiyle tüzel kişilerin bu kapsamın dışında tutulması gerekecektir. Mağdur sıfatına ilişkin olarak gerçek kişilerin mağdur olacağından şüphe yok ise de tüzel kişilerin bilişim sistemlerinin maliki olması halinde suçtan zarar gören olarak kabul edilebileceği görüşü de mevcuttur¹²². Herhalde sisteme ilişkin eylemlerin, sistemin maliki tüzel kişiye zarar vermediği durumlarda bu sıfatın kazanılmasına imkan bulunmamaktadır¹²³. Tüm bunların yanında, suça konu eylemlerin doğrudan yöneltildiği kişi olmasalar dahi, suça konu sistemde verileri bulunan 3. Kişilerin de mağdur olarak kabul edilebileceği durumlar söz konusu olabilmektedir¹²⁴. Bilişim suçları ve ceza hukuku muhakemesini gerektiren eylemler özelinde yapılacak incelemenin somut olayın özellikleri uyarınca farklı yorumlar doğmasına imkan vermesi mümkündür.

3.1.8. Afet ve Acil Durum Yönetimi Başkanlığı

2009 yılında yayımlanan 5902 sayılı, Afet ve Acil Durum Yönetimi Başkanlığı ile İlgili Bazı Düzenlemeler Hakkında Kanun ile Başbakanlık’a bağlı şekilde çalışmak üzere kurulan Afet ve Acil Durum Yönetimi Başkanlığı daha evvel farklı kurumlara bağlı olarak faaliyet gösteren Sivil Savunma Genel Müdürlüğü, Afet İşleri Genel Müdürlüğü, Türkiye Acil Durum Yönetimi Genel Müdürlüğü görevlerinin tek bir çatı altında toplanması amacına hizmet etmek

¹²¹ Yasin Yanar, “Ceza Hukuku Ve Bilişim Hukuku Bağlamında Tek Md. 245/A Yasak Cihaz Veya Programlar Suçu” (Yüksek Lisans Tezi) İstanbul Bilgi Üniversitesi, 2019, s.

¹²² Özçelik, 2021, s.51, Karagöz, 2020, s.161.

¹²³ Karagöz, 2020, s.161.

¹²⁴ Özçelik, 2021, s.51, Karagöz, 2020, s.161.

üzere kurulmuştur. 15 Temmuz 2018 tarihinde yayınlanan 4 Nolu Cumhurbaşkanlığı Kararnamesi ile Afet ve Acil Durum Yönetimi Başkanlığı, İçişleri Bakanlığına bağlanmıştır. Afet ve Acil İşler Durum Yönetimi Başkanlığı 4 Nolu Cumhurbaşkanlığı Kararnamesi uyarınca¹²⁵ afet ve acil durumlar ile sivil savunmaya ilişkin hizmetlerin gerçekleştirilmesi, meydana gelmeden evvel ilgili olaylara ilişkin hazırlıklar yapılarak riskin azaltılması ile olay sırasında gerekli müdahalelerin planlanması, gerekmesi halinde yurt içinde ve dışında insani yardım operasyonlarının düzenlenmesi konusunda görevlendirilmiştir. Belirtilen afet ve insani yardımların kapsamına teknolojik afetlerin de dahil edilmiş olması¹²⁶ AFAD'ın siber saldırılara yönelik de belirli görevler üstelenmesini gerekli kılmıştır.

Teknoloji kaynaklı afet, AFAD bünyesinde yayımlanan Afet Yönetimi Terimleri Sözlüğü'ne göre *“İnsan faaliyetleri ya da doğa kaynaklı afetlerin tetiklemesi sonucunda oluşan endüstriyel, maden, nükleer ve ulaşım kazaları, kritik yapılara yönelik tehditler, siber tehlikeler, büyük yangınlar, terörizm (kimyasal, biyolojik, radyolojik, nükleer tehditler) ile çevresel tehlikeler gibi can kaybına, hastalıklara, sosyal, ekonomik ve çevresel bozulmalara neden olan afet ya da acil durum.”* olarak kabul edilmekte olup, aynı sözlüğe göre siber tehlike *“Bilgisayar ağlarını kullanan erişim ve iletişim sistemlerinin, kötü amaçlı*

¹²⁵ Bakanlıklara Bağlı, İlgili, İlişkili Kurum ve Kuruluşlar ile Diğer Kurum ve Kuruluşların Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi'nin İkinci Bölüm Afet ve Acil Durum Yönetimi Başkanlığı kısmında, Amaç ve Kapsam başlıklı 30. Maddesi ile *“(1) Bu Bölümün amacı, afet ve acil durumlar ile sivil savunmaya ilişkin hizmetleri yürütmek üzere İçişleri Bakanlığına bağlı Afet ve Acil Durum Yönetimi Başkanlığının kurulması, teşkilatı ile görev ve yetkilerini düzenlemektir. (2) Bu Bölüm; afet ve acil durumlar ile sivil savunmaya ilişkin hizmetlerin ülke düzeyinde etkin bir şekilde gerçekleştirilmesi için gerekli önlemlerin alınması ve olayların meydana gelmesinden önce hazırlık ve risk azaltma, olay sırasında yapılacak müdahale ve olay sonrasında gerçekleştirilecek iyileştirme çalışmalarını yürüten kurum ve kuruluşlar arasında koordinasyonun sağlanması, yurt içinde ve yurt dışında insani yardım operasyonlarının yapılması ve koordine edilmesi ile bu konularda politika önerilerinin geliştirilmesi ve uygulanması hususlarını kapsar.”* Şeklinde düzenlenmiştir.

¹²⁶ Bakanlıklara Bağlı, İlgili, İlişkili Kurum ve Kuruluşlar ile Diğer Kurum ve Kuruluşların Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi, 31. Madde 1. Fıkra 9) bendi *“İnsani yardım: Doğal afetler, teknolojik afetler, savaş ve toplumsal çatışmalar neticesinde can güvenliği, açlık, susuzluk, kıtlık, geçici barınma, salgın hastalık ve benzeri nedenlerle ihtiyaç sahibi olan yerler için uluslararası toplumun istikrarında önemli bir unsur olması nedeniyle siyasi, ekonomik ve askeri amaçlardan bağımsız yapılacak yardımları,”*

kişilerin (hacker) sanal ortamdaki saldırısı nedeniyle çökmesi veya devre dışı kalmasına sebep olan tehdit.”¹²⁷ olarak tanımlanmıştır.

Bu görevlendirme ve tanımlama gereği AFAD’ın herhangi bir sanal ortam saldırısı nedeniyle -ki bunun siber uzayda gerçekleşen bir siber saldırı olabileceğini düşünmek mümkün görünmektedir- yaşanacak afetlere ilişkin ve ayrıca kritik altyapılara yönelik tehditlere karşı üstlendiği rollerin bulunduğu görülmektedir. Bu hususta, AFAD bünyesinde görev yapan Teknolojik Afetler Risk Azaltma Çalışma Grup Başkanlığı kurulmuştur. Teknolojik Afetler Risk Azaltma Çalışma Grup Başkanlığı’nın çalışmaları arasında,

- Ulusal Teknolojik Afetler Stratejik Planının hazırlanması,
- Ulusal Kritik Altyapı, Varlık ve Tesisleri Belirleme, Risk Değerlendirme ve Önceliklendirme Projesi,
- Ulusal Teknolojik Afetler Stratejik Yol Haritası Belgelerinin Hazırlanması Projesi,
- Teknolojik Afetlere Yönelik Tehlike ve Risk Haritalarının Hazırlanması İçin Yöntem Geliştirilmesi ve Pilot Bölge Uygulaması Projesi, gibi projelerin yer aldığı bilinmektedir.

Teknolojik Afetler Risk Azaltma Çalışma Grup Başkanlığı bünyesinde devam eden çalışmaların, diğer kamu kurum ve kuruluşları ile işbirliği ve koordinasyon içerisinde, gerekmesi halinde uygulayıcı, yerel, merkezi kurum ve kuruluşlar, üniversiteler ve STK’lar ile işbirlikleri yapılarak devam etmekte, bu kapsamda AR-GE çalışma ve projeleri takip edilip desteklenmektedir.

Sayılan çalışmaların yanı sıra, AFAD tarafından yayımlanmış 2014-2023 Teknolojik Afetler Yol Haritası Belgesi ile 2014-2023 Kritik Altyapıların

¹²⁷ Afet ve Acil Durum Yönetimi Başkanlığı, “Açıklamalı Afet Yönetimi Terimleri Sözlüğü” link : <https://www.afad.gov.tr/aciklamali-afet-yonetimi-terimleri-sozlugu>, (Son erişim tarihi : 22.06.2024)

Korunması Yol Haritası Belgesi’de elektrik sektörüne yönelik bir teknolojik afete ilişkin gereksinimler ve eylemler detaylı şekilde incelenmiştir.

2014-2023 Teknolojik Afetler Yol Haritası Belgesi’nde, mevcut durumun analizi ile başlangıç yapılmış, AB Politikası da göz önünde bulundurularak, teknolojik afetlere yönelik bir metodoloji belirlenmiş ve ardından konuya ilişkin gereksinimler ile eylemlerin tespiti yapılmıştır. Türkiye’nin AB üyeliğine adaylık sürecinin olumlu şekilde sonuçlanabilmesinin temel koşullarından biri kabul edilen ve Uyumlaştırma Süreci’nin de bir parçası kabul edilen mevzuat uyumlaştırılması, mevzuatın uygulanmasına yönelik organların tesisi ile yaptırımların düzenlenmesi konularını da içeriyor olduğundan hazırlanan çalışma bu süreç için oldukça değerli bir katkıdır. Uyumlaştırma Süreci kapsamında yapılması gereken çalışmaların, sivil savunma başlığına da sirayet etmesi gerektiğinden ve AFAD’ın da sivil savunma yapılanmasında önemli bir rolü olduğu göz önünde bulundurulduğunda ilgili belgenin hazırlanmasının önemli motivasyonlarından birinin de AB üyeliği süreci olduğu kabul edilebilir¹²⁸. 2014-2023 Teknolojik Afetler Yol Haritası belgesi hazırlanırken ;

- Avrupa Komisyon'un 2006/12/12 sayılı "Kritik Altyapıların Korunmasına Yönelik Avrupa Programı Hakkında" Tebliği,

- "Avrupa Kritik Altyapılarının Tanımlanması ve Belirlenmesi ile Bunların Korunmasının İyileştirilmesi İhtiyacının Değerlendirilmesine İlişkin" 8 Aralık 2008 tarihli ve 2008/114/EC sayılı Avrupa Konseyi Direktifi,

- 12 Şubat 2007 tarih ve 2007/124/EC sayılı Avrupa Konsey Kararı uyarınca "2007-2013 dönemi için, Güvenlik ve Özgürlüklerin Korunması Genel Programının bir parçası olarak, 'Terörizm ve Güvenlikle ilgili diğer risklerin Önlenmesi, Hazırlıklılık ve Sonuç Yönetimi' Özel Programının oluşturulması"belgesi,

¹²⁸ Afet ve Acil Durum Yönetim Başkanlığı, “2014-2023 Teknolojik Afetler Yol Haritası Belgesi”, 2014, syf: 14.

- Kritik Altyapı Uyarı Bilgi Ağı (CIWIN) hakkında 27 Ekim 2008 tarihli Konsey Kararı Teklifi'nin final versiyonu gibi pek çok önemli kaynağın incelendiği belirtilmiştir¹²⁹. Teknolojik Afetler Yol Haritası Belgesi kapsamında, kritik altyapıların korunmasına yönelik pek çok gereksinim ve eylem planı bulunmakla beraber temel gereksinimler aşağıdaki şekilde belirlenmiştir.

- Yetkili (sorumlu) otoritelerin belirlenmesi,
- Yetkili koordinasyon otoritesinin belirlenmesi, iş bölümü bazında kritik altyapı sektörleri (KAS) belirlemekte kullanılacak kıstasların tespit edilmesi,
- Avrupa Birliği Direktifinin uyumlaştırılması ile ilgili taslak yönetmelik hazırlanması ve kapsam, büyüklük ve zaman etkisi faktörlerinin göz önünde bulundurularak kritik altyapılarının belirlenmesi ve koruyucu tedbirlerin artırılması
- Kritik altyapıların etkin korunması, ulusal seviyede veya AB seviyesinde bütün ilgili paydaşlar arasında iletişim, koordinasyon ve işbirliği,
- KAS'lerle ilgili işletmeci güvenlik planı yapılması,
- Güvenlik İrtibat Görevlisi atamak,
- Eğitim programı oluşturulması ve uygulanması,
- Ulusal düzeydeki kritik altyapıların korunması amacı ile Kritik Altyapı Koruma Planı hazırlanması,
- En iyi uygulamaların ve anlık tehdit ve alarmların güvenli bir şekilde paylaşımı yoluyla uygun koruma tedbirlerinin geliştirilmesini teşvik

¹²⁹ Afet ve Acil Durum Yönetim Başkanlığı, 2014, s.21.

edebilecek AB Kritik Altyapı Uyarı Bilgi Ağı (KAUBA) çalışmalarına entegrasyon,

- Raporlama.

Belirtilen gereksinimlerden de görüleceği üzere, kritik altyapıların etkin bir şekilde korunabilmesinde öncelikle kritik altyapıların belirlenmesinde kullanılacak kıstaslar ve devamında kritik altyapıların belirlenmesi, güçlü bir iletişim ve koordinasyon zincirinin oluşturulması, bu iletişimin faydasını ortaya koyabilmek adına farkındalığın arttırılması gibi hususların öne çıktığı görülmektedir.

2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi, kritik altyapı¹³⁰ olarak kabul edilen yapılara yönelik afetin neden olduğu zararların en aza indirgenmesi, teknolojik afetlerin de bu kapsamda değerlendirilmesi ve incelenmesi, yetkili kurum ve kuruluşlar arasında işbirliği kurularak ve AB mevzuatına uyumlu şekilde, insanların, çevrenin ve mal varlığının daha iyi korunmasının sağlanması, kritik altyapılara yönelik risk yönetimi ve zarar azaltma planlarının devreye alınması, uluslararası ilişkileri etkileyecek kritik altyapıların belirlenmesi ve korunması ile Kritik Altyapılar Uyarı Bilgi Ağı'na yönelik verilerin hazırlanması amaçlarına hizmet etmek üzere hazırlanmıştır¹³¹. AB mevzuatının da detaylı şekilde incelendiği ve Türkiye'deki mevcut durumunun analizinin yapıldığı ilgili belgede öne çıkan ve atılması beklenen adımlar sıralanmıştır. Teknolojik Afetler Yol Haritası Belgesi kapsamında belirlenen ve yukarıda sayılan gereksimlerin birebir aynısını içeren Kritik Altyapıların Korunması Yol Haritası Belgesi gereksinimleri, kritik altyapılar açısından gerekli korumanın en önemli ayağının teknolojik afetler bağlamında olduğunu düşündürmükte ve bu kapsamda en fazla önlemin ve çalışmanın yapılmasının da bu alana aktarılması gerekliliğini ortaya koymaktadır. AFAD tarafından

¹³⁰ Afet ve Acil Durum Yönetim Başkanlığı, “2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi”, 2014, s. 4.

¹³¹ Afet ve Acil Durum Yönetim Başkanlığı, 2014, syf: 20-23.

hazırlanmış ilgili belgeler, her ne kadar siber saldırılardan korunmanın yahut uğranılması halinde ortaya çıkacak zararların en aza indirilmesinin, bir afet bakış açısıyla ne şekilde gerçekleşmesi gerektiğini belirleyen metinler olsa da, ortak bir gereksinim olan kritik altyapıların belirlenmesinden bahsetmesi, iletişim ve koordinasyonun siber saldırılara ilişkin savunmada önemi ve teknoloji afet seviyesine dönüşebilecek olması nedeniyle kritik altyapıların bu bağlamda korunmasına verilen önem ile AB mevzuatının aynı konudaki çalışmaları neticesinde gelmiş oldukları seviyenin görülmesi bakımından kayda değer ve kıymetli çalışmalardır.

3.1.9. Milli İstihbarat Teşkilatı

Milli İstihbarat Teşkilatı, 1984 yılından bugüne yürürlükte olan 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu kapsamında görevine devam eden ve mevzuatta yapılan güncelleme¹³² ile Cumhurbaşkanı'na bağlı olarak, devlet politikalarının yapılması ile milli güvenliğe ilişkin önlem ve faaliyetlerin planlanması, amacıyla ihtiyaç duyulan bilgi ve belgeleri toplayarak değerlendirmek üzere istihbari faaliyetleri göstermekte olan bir kurum olarak varlığını sürdürmektedir¹³³. 2937 sayılı Kanun'nun 4. Maddesinde, görevler başlığı altında sayılan sorumlulukları haiz Milli İstihbarat Teşkilatı'nın görevleri özetle, Türkiye Cumhuriyeti'nin güvenliğine yönelik ülke içinden ya da dışından, mevcut ya da muhtemel faaliyetler hakkında milli güvenlik istihbaratı sağlamak ve ilgili organlara ulaştırmak, milli güvenlik siyaseti ile ilgili planları yürüterek, Genelkurmay Başkanı, Milli Güvenlik Kurulu Genel Sekreteri ve ilgili bakanların istihbarat ihtiyaçlarına yanıt vermek, Milli Güvenlik Kurulu tarafından

¹³² 694 Olağanüstü Hal Kapsamında Bazı Düzenlemeler Yapılması Hakkında Kanun Hükmünde Kararname, madde 60 "1/11/1983 tarihli ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanununun 3 üncü maddesinin birinci fıkrasında yer alan "Başbakana" ibaresi "Cumhurbaşkanına" şeklinde değiştirilmiş ve aynı maddenin dördüncü fıkrasında yer alan "merkez ve taşra" ibaresi yürürlükten kaldırılmıştır."

¹³³ Milli İstihbarat Teşkilatı, İstihbarat Sözlüğü, İstihbarat : Politika yapımcıların ve ilgili devlet kuruluşlarının milli güvenlik ve menfaatlara ilişkin konularda doğru kararları verebilmek için ihtiyaç duydukları, rakip vetya düşman tarafından korunan haber, bilgi ve tecrübeleri esas alan, bunların gizli toplama, işleme analiz ve değerlendirme işleminden geçirilmesiyle üretilen, ilgili olduğu konuda karar vericiler için yeni bir anlayış geliştiren nihai ürün ve bu ürünü ortaya çıkaran faaliyet.

verilen görevleri yerine getirmek ve ülkemizden dışarıya yapılan istihbarat faaliyetlerini önlemek, dış güvenlik, terörle mücadele ve milli güvenliğe ilişkin Cumhurbaşkanınca verilen görevleri yerine getirmek şeklindedir. Belirtilen görevlerin özetle milli güvenliğin sağlanması odağında toplandığı görülmekle birlikte, bu faaliyetlerin çağımızın yeni savunma alanı olarak kabul edilen siber uzaya yönelik konuları da kapsamına dahil etmesi bir zorunluluk halini almış ve dolayısıyla 2937 sayılı Kanun'nun 4. Maddesi'ne bu ihtiyaca hizmet edecek şekilde 2014 yılında, 6532 Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanununda Değişiklik Yapılmasına Dair Kanun'nun 1. Maddesi ile “i) *Dış istihbarat, millî savunma, terörle mücadele ve uluslararası suçlar ile siber güvenlik konularında her türlü teknik istihbarat ve insan istihbaratı usul, araç ve sistemlerini kullanmak suretiyle bilgi, belge, haber ve veri toplamak, kaydetmek, analiz etmek ve üretilen istihbaratı gerekli kuruluşlara ulaştırmak.*” Şeklindeki i bendi eklenmiştir. Eklenen bent ile Milli İstihbarat Teşkilatına, siber güvenliğe yönelik olarak da teknik istihbarat ve insan istihbaratına ilişkin usul, araç ve sistemleri kullanarak bilgi, belge, haber ve veri toplamak, kaydetmek, analiz etmek ve üretilen istihbaratı ilgili kuruluşlara ulaştırma görevini getirilmiştir. Ayrıca, yine 6532 sayılı Kanun ile 2937 sayılı Kanun'nun yetkiler başlıklı 6. Maddesinin g bendi olarak, Milli İstihbarat Teşkilatı'nın telekomünikasyon kanallarından geçen dış istihbarat, millî savunma, terörizm ve uluslararası suçlar ile siber güvenlikle ilgili verileri toplayabilmesine ilişkin de yetki tanımlanmıştır.

3.1.10. TÜBİTAK

Türkiye Bilimsel ve Teknolojik Araştırma Kurumu, 1963 yılından beri ve hali hazırda Sanayi ve Teknoloji Bakanlığı'nın¹³⁴ ilgili kuruluşu olarak akademik ve endüstriyel alanda araştırma, geliştirme çalışmaları düzenlemek, ülke çapında bilim ve teknoloji politikalarını belirlemek ve bu konuda toplum farkındalığını arttırabilmek adına gerekli faaliyetlerine devam etmektedir. 1999 yılı itibariyle,

¹³⁴ Kalkınma Bakanlığı'nın, Kalkınma Ajansları adı altında faaliyet gösteren biriminin Sanayi ve Teknoloji Bakanlığı'na bağlanması ve diğer birimlerinin ilgili kurum ve kuruluşların bünyesinde faaliyetlerine devam edecek şekilde yetki devirlerinin yapılması ile birlikte 2018 yılında kapatılmıştır.

TÜBİTAK, Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM) bünyesinde Siber Güvenlik Enstitüsü'nün kurulumuyla bu faaliyetlerinin arasına siber güvenliği de dahil etmiştir. Genelkurmay Başkanlığı ile yürütülen ortak çalışmaların yanında, yurt dışında siber güvenlik çalışma gruplarına, eğitim ve tatbikatlara da katılım gösteren TÜBİTAK, Siber Güvenlik Enstitüsü aracılığı ile ulusal siber güvenlik tatbikatları da düzenlemekte, ulusal siber güvenliğin geliştirilmesi adına, sanal siber güvenlik laboratuvarının kurulması, siber güvenlik yazılımlarının geliştirilmesi, kalite ve konfigürasyon alanında geliştirmeler yapılması, siber güvenliğe yönelik sistem testleri, stratejiler ve ürünlerin geliştirilmesi gibi pek çok operasyonel faaliyete imza atmaktadır. NATO'nun Siber Savunma Mükemmeliyet Merkezi'nin daimî temsilciliğinin yan sıra, yine siber güvenlik alanında gelişim ve iyileştirme amacına hizmet etmek üzere, NATO bünyesinde faaliyetlerinde devam eden, Kötü Amaçlı Yazılım Bilgi Paylaşım Platformu, Ortak Kriter Yeteneği Ekibi ve Takımı çalışma grubu ile Siber Savunma için Modelleme ve Simülasyon Desteği çalışmalarına katılım sağlayan TÜBİTAK, siber güvenliğe ilişkin araştırma ve geliştirme faaliyetlerinin uluslararası düzeyde Türkiye temsilcisi konumundadır.

TÜBİTAK Siber Güvenlik Enstitüsü, ayrıca Enerji Kritik Altyapılarına Yönelik Siber Güvenlik Yeteneklerinin Geliştirilmesi Projesi kapsamında, Enerji Kritik Altyapıları Siber Atak Platformunun kurulması çalışmalarını gerçekleştirmiş, Kritik Altyapılar Sektörel Risk Analizi Metodolojisinin hazırlanmasında rol oynamış, Ulusal Bilgi Sistemleri Güvenlik Programı kapsamında ülkemizin siber güvenliğinin sağlanması için TÜBİTAK BİLGEM bünyesinde Türkiye Bilgisayar Olaylarına Müdahale Ekibi (TR-BOME) kurulmasını sağlamıştır.

Türk Standartları Enstitüsü ve TÜBİTAK – BİLGEM arasında imzalanan bir iş birliği protokolü ile akıllı cihazların siber güvenlik, test, denetim ve sertifikasyon faaliyetlerinin de iki kurumun ortak çalışmasıyla gerçekleştirilmektedir. Protokol ile internete bağlı cihazların ve endüstriyel sistemlerin, uluslararası alanda geçerli sertifikasyonu yerli üretiminin sağlanması

ve dünya genelinde belirlenen standartlara uygun hale gelmesi amacına hizmet eden iş birliğinin analiz ve test çalışmalarının TÜBİTAK BİLGEM tarafından yapılması belgelendirme sürecinin ise TSE tarafından yürütülmesi kararlaştırılmıştır¹³⁵. Bunun yanında, Dijital Dönüşüm Ofisi tarafından yayımlanan ve detaylarına metnin öncesinde değinilmiş olan Bilgi ve İletişim Güvenliği Rehberine uygun şekilde, uyum denetimi hizmeti sağlayacak personel ve firmaların belgelendirme programı da protokol ile düzenlenmiş ve TÜBİTAK ilgili programda TSE ile birlikte rol almıştır¹³⁶.

TÜBİTAK tarafından, siber güvenlik alanında gerçekleştirilen faaliyetler, ülke çapında teknolojik ürünlerin güvenli şekilde kullanımı ile gelişimine katkı sağlayama amacıyla, ürün geliştirme, laboratuvar çalışmaları, ulusal ve uluslararası siber güvenlik tatbikatları, siber güvenlik profesyonelleri yetiştirme, siber güvenlik sertifika süreçlerine dahil olma, farklı düzeyde kişilere siber güvenlik eğitimleri verme gibi operasyonel hususlar ile NATO'nun da dahil olduğu uluslararası siber güvenliğe yönelik faaliyetlerinde ülkemizi de temsil etmek olduğu söylenebilir. Yanı sıra pek çok kurumda, siber güvenliğe ilişkin yapılanmaların, sistemlerin yahut önem arz eden projelerin hayata geçirilmesinde de TÜBİTAK ve ilgili ekiplerin büyük katkısı vardır. Belirlenen amaç ve görevler uyarınca siber güvenlik alanında TÜBİTAK'ın teknik süreçlerin gelişimine katkı sağladığı, siber güvenliğe yönelik ürün ve laboratuvarları ile kurumlara destek olduğu ancak düzenleyici standartlara ilişkin yaptığı iş birlikleri ile verilen destek dışında denetleyici bir kurum olmadığını belirtmek gerekir.

¹³⁵ TÜBİTAK, “Endüstride Önemli İmza”, link: <https://tubitak.gov.tr/tr/haber/endustride-onemli-imza>, (Son erişim tarihi: 22.06.2024)

¹³⁶ Türk Standartları Enstitüsü, “Bilgi ve İletişim Güvenliği Rehberi Denetim Hizmeti Veren Firma Belgelendirilmesi”, link : <https://www.tse.org.tr/bilisim-belgelendirme-hizmetleri/>, (Son erişim tarihi : 22.06.2024)

3.2. ULUSLARARASI SİBER GÜVENLİK STANDART VE DÜZENLEMELERİ İLE AB DÜZENLEMLERİ

3.2.1. ISO/IEC 27001:2022 – ISO/IEC 27001:2022

Kurum ve kuruluşların çalışmaları için gerekli olan bilgi ve barındıkları sistemlerin, bu çalışmalara dahil olan insanların, süreçlerin, kural, politika ve prosedürlerin devamlı olarak iyileştirilmesine odaklanan ISO/IEC 27001:2022 yalnızca teknik sistem kontrollerini değil, bu kontrollerin nasıl gerçekleştirileceğine ilişkin planlamaların yapılması ile uygulanmasına, gerekmesi halinde kontrol edilerek gerekli önlemlerin alınmasına dair bir çerçeve çizmektedir¹³⁷. Tam adı "ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements standardı" olan bilgi güvenliği yönetim gerekliliklerini içeren standart, 25 Ekim 2022 tarihinde güncellenerek yayımlanmıştır. Türk Standartları Enstitüsü tarafından ise "TS ISO/IEC 27001: 2022 Bilgi Güvenliği, Siber Güvenlik Ve Gizlilik Koruması- Bilgi Güvenliği Yönetim Sistemleri- Gereksinimler" olarak Aralık 2022 tarihinde Türkiye için güncel versiyonu yayınlanmıştır. Yaygın kullanılan ismi ile ISO 27001, yapısal bir bilgi güvenliği yaklaşımı belirlenmesine yardımcı, uluslararası bir standart olup, akredite belgelendirme kuruluşları tarafından kontrol ve denetimleri sağlanarak, talep eden kurum ve kuruluşlar için bazı şirketlerin çalışmaları için yasal bir yükümlülük olsa da genel itibarıyla gönüllü olunması halinde temin edilebilmektedir. ISO 27001 sertifikasına sahip olabilmesi için kurum veya kuruluşların, bilişim sistemlerinin doğrudan kendisi ile kullanıcılarına bağlı süreçlerinin her daim güvenli bir şekilde çalışabilmesi adına tüm yapısını dahil edilerek baştan uca standardın gereksinimlerini yerine getirmeleri ve bilgi sistemlerinde yaşanacak bir aksama nedeniyle faaliyetlerine ara vermeksizin

¹³⁷ Yılmaz, H. (2016). TS ISO/IEC 27001 Bilgi Güvenliği Yönetimi Standardı Kapsamında Bilgi Güvenliği Yönetim Sisteminin Kurulması Ve Bilgi Güvenliği Risk Analizi. Denetim(15), 45-59., Syf :41

çalışabilmelerini sağlayacak iş sürekliliği planlarını hazırlayarak, kapsamlı ve etkin bir bilgi güvenliği yönetim sistemi (BGYS) kurmaları gerekmektedir¹³⁸.

ISO/IEC 27001 standardının tarihi, bilgi güvenliğinin bir yönetim sistemi içerisinde yürütülmesine yönelik atılan ilk adımları içerir. ISO 27001'in temelini oluşturan British Standard 7799, İngiliz Standartlar Enstitüsü (British Standards Institute) tarafından yayımlanan bir bilgi güvenliği standardı olarak planlanmış ve organizasyonlara bilgi varlıklarını yönetme ile koruma konusunda rehberlik etmeyi amaçlamıştır. Sonrasında BS 7799-1 ve BS 7799-2 olmak üzere ikiye ayrılan standart, 2 numaralı parçasıyla, organizasyonların bilgi güvenliği yönetim sistemlerini kurmaları, kurumsal bir bilgi güvenliği anlayışının oluşturulabilmesi için temel gereksinimleri belirlerken, 1 numaralı parçasıyla bir kuruluşun baştan uca bilgi güvenliği yönetim sistemide bulunması gereken teknik kontrollerin neler olduğunu belirlemiştir. Günümüzdeki karşılıkları BS7799-2 için ISO 27001, BS-7799-1 için ise ISO 27002 olarak düşünülebilir. ISO 27002 bir organizasyonda bulunması gereken temel bilgi güvenliği kontrollerinin neler olması gerektiğini içermektedir. ISO 27001 ise bilgi güvenliği sisteminin nasıl inşa edilmesi gerektiğini değerlendirirken alınması gereken bilgi güvenliği önlemlerine ilişkin olarak EK – A metni ile ISO 27002 kontrollerini işaret eder.

Her ne kadar İngiltere menşeli bir kuruluş tarafından hazırlanarak yayımlansa ve uygulanmasına başlanılsa da, getirdiği yaklaşım ve organizasyonlara, bilgi güvenliği yönetim sistemlerinin kurulması, uygulanması, denetlenmesi ve iyileştirilmesi yoluyla sağladığı değer sebebiyle gelişim gösteren ve yayılan BS 7799'dan temelini alan ISO (Uluslararası Standartlar Örgütü) , bu metni uluslararası bir standarda dönüştürme sürecini başlatmış ve neticesinde Uluslararası Elektroteknik Komisyonu ile birlikte (International Electrotechnical Commission-IEC) hazırlanan ISO/IEC 17799 standardı ortaya çıkmıştır. 2005 yılında yapılan güncellemeler ile de ismi ISO/IEC 27001 olarak değiştirilmiştir. Gelişen teknoloji ve bilgi güvenliği yönetimi anlayışının da değişmesiyle birlikte

¹³⁸ Age s.51.

2005 yılında yenilenen standart, sonrasında 2013 yılında önceki versiyonuna ve nihayetinde 2022 yılında ise günümüzdeki versiyonuna dönüşmüştür. Önceki versiyonlarının güncellenmiş hali olarak hazırlanan 2022 versiyonunda, bilgi güvenliği yönetiminin sürekli iyileştirme ve risk yönetimi konularını da içerir şekilde dizayn edilmesi vurgulanmış olup, organizasyonların hızla değişen tehditlere ve teknolojik gelişmelere nasıl uyum sağlayabileceğini de ele alınmıştır. ISO/IEC 27001:2022 bilgi güvenliği yönetim sistemleri için dünya çapında kabul gören bir standart olarak kullanılmakta olup, kurum ve kuruluşların hem saygınlığı hem de güvenilirliğini simgeleyen bir gösterge olarak kabul edilmektedir.

ISO 27001'in bilgi yönetimi sistemlerinde odaklandığı konular ve standarta sahip olabilmek için yapılması gerekenler aşağıdaki gibidir;

1. Risk Yönetimi: ISO 27001, organizasyonların bilgi güvenliği risklerini belirlemelerini, değerlendirmelerini ve yönetmelerini gerektirir. Bu gereklilik, potansiyel tehditlere karşı savunma mekanizmalarının kurulmasını da içerir.
2. Politika ve Süreçler: Standart, organizasyonların bir bilgi güvenliği politikası oluşturmalarını ve bu politikayı uygulamak için süreçler geliştirmelerini bekler.
3. İzleme ve Denetleme: ISO 27001, organizasyonların bilgi güvenliği süreçlerini sürekli izlemelerini ve düzenli denetimler yapmalarını gerektirir.
4. Sürekli İyileştirme: Standart, organizasyonların bilgi güvenliği yönetim sistemlerini sürekli olarak gözden geçirmelerini ve iyileştirmeler yapmalarını öngörür.
5. Taahhüt ve Katılım: ISO 27001, organizasyon liderliğinin ve çalışanların bilgi güvenliği konusundaki taahhüt ve katılımını vurgular.

Belirlenen kořullara uygun bir bilgi ynetimi sistemi geliřtirdiđini gsterebilen kuruluřlar, ISO 27001 sertifikasyonu ile organizasyonlarının mřterilerine, ortaklarına ve paydařlarına karřı gvenilir bir bilgi gvenliđi ynetim sistemine sahip olduklarını gsterebilmektedir. Bu durum ile aslında byk bir ođunluđu dijitalleřen hizmetlerin gvenli yrtlmesi adına gsterilen abayı ortaya koymaktadır. Ynetim anlayıřının uygulanır, srekli gncel, yeniliki ve zmsenmiř olması da kurumun gvenliđi aısından ayrıca nemli faktrlerdir. Genel itibariyle ISO 27001 sertifikası temin etmek, kurum ve kuruluřlar iin bir tercih olsa da elektrik piyasası aısından durum aynı deđildir. Almanya’da enerji piyasası aısından getirilen zorunluluk gibi Trkiye’de de Elektrik Piyasası Lisans Ynetmeliđi hkmleri uyarınca,

- retim lisansı sahipleri (retim lisansı sahibinin hak ve ykmllkleri bařlıklı 30. Madde, 2. Fıkra, f bendi)
- İletim lisansı sahibi - TEİAř iřaret edilmektedir (İletim lisansı sahibinin hak ve ykmllkleri bařlıklı 31. Madde, 2. Fıkra, p bendi)
- Piyasa iřletim lisansı sahibi - EPİAř iřaret edilmektedir (Piyasa iřletim lisansı sahibinin hak ve ykmllkleri bařlıklı 32. Madde, 3. Fıkra, ğ bendi)
- Dađıtım lisansı sahipleri (Dađıtım lisansı sahibinin hak ve ykmllkleri bařlıklı 33. Madde, 2. Fıkra, y bendi)
- Tedarik lisansı sahipleri (Tedarik lisansı sahibinin hak ve ykmllkleri bařlıklı 34. Madde, 4. Fıkra, ğ bendi)

Hem ISO 27001 geređi olarak, hem de ilgili standartın iřaret ettiđi ve bir parası olan ISO 27002 sertifikasının gereklerini de yerine getirmekle ykml tutulmuřlardır. Bu ortak ISO standardı dıřında retim, iletim, dađıtım lisansı sahipleri iin ISO/IEC TR 27019 standardı ve tedarik lisansı sahipleri iin ise TS EN ISO 9001 ve TS ISO 10002 standartlarının sađlanması gerektiđi ilgili

hükümlerle belirlenmiştir. Bu yükümlülüğün yerine getirilmesi, sahip olunan lisansın devamlılığı açısından bir koşul olarak kabul edilmiş olup Elektrik Piyasası Lisans Yönetmeliği'nin 27. maddesi uyarınca belirtilen standartlara ilişkin yükümlülüklerin yerine getirilmemiş ve dolayısıyla sertifikaların kaybedilmiş olması halinde, Elektrik Piyasası Kanunu'nun 16. Maddesi ile belirlenen yaptırımların uygulanması ihtimali gündeme gelmektedir.

Enerji sektöründe ISO 27001 standardının bir yasal zorunluluk olması yalnızca Türkiye'ye özgü bir durum da değildir. Almanya'da enerji sektörü için ilgili standartın zorunlu tutulmasının yanında, Birleşik Krallık'ta da enerji sektörüne ilişkin regülasyonlarda ilgili standartların sağlanması gönüllülük esasına bağlı olmak kaydıyla yer almaktadır¹³⁹.

2022 tarihinde yapılan güncelleme sebebiyle, ISO 27001 denetimi yapabilmesi için 1 Kasım 2023 tarihine kadar belgelendirme kuruluşlarının akreditasyonlarını tamamlamaları gerekmektedir. Uluslararası Akreditasyon Forumu tarafından, yeni versiyon için geçiş şartları açıklanmış olup, TS ISO/IEC 27001:2022 Bilgi Güvenliği, Siber Güvenlik Ve Gizlilik Koruması- Bilgi Güvenliği Yönetim Sistemleri- Gereksinimler standardına uygunluk talep eden kuruluşlarının ilk belge başvurularını ve/veya yeniden belgelendirme tetkiklerini 31 Ekim 2023 tarihinden itibaren (standardın yayınlanmasından itibaren belirlenen kademelere uygun olarak toplam 36 ay içerisinde) 31 Ekim 2025 tarihine kadar geçişlerin tamamlanmasının gerektiği belirtilmiştir¹⁴⁰. ISO 27001 standardı, bir organizasyonun bilgi varlıklarını nasıl koruması gerektiğini belirleyen, uygulama ve bu uygulamaları sürdürme süreçlerini tanımlayan bir çerçeve sunuyor olduğundan, güncel gelişmelere uygun şekilde revize edilen versiyonda belirlenen kontrollerin bulunuyor olduğunu, kısaca yeni versiyona da

¹³⁹ Dea Saka Kurnia Putra, Saffana Tistiyani, Septia Ulfa Sunaringtyas, "The Use of ISO/IEC 27001 Family of Standards in Regulatory Requirements in Some Countries" Konferans yayını: 2021 2nd International Conference on ICT for Rural Development, Aralık 2021, s: 2.

¹⁴⁰ Uluslararası Akreditasyon Forumu, "ISO/IEC 27001:2022'ye Geçiş Şartları", 2022, syf:7

uyumlu olunduğunun gösterilmesi kurum ve kuruluşların güvenilirliğinin devamı adına önem arz etmektedir. Bilgi ve İletişim Güvenliği Rehberi’de, ISO 27001 standardı ile diğer uluslararası standartlar ile uyumluğunun mukayesesine yönelik olarak Uluslararası Standartlar Ve Yayınları Kılavuzları Eşleştirme Tablosu yayımlanarak pek çok kontrol adımında referans olarak göstermiş durumdadır.

Bu standartın yanında elektrik piyasasının da içinde kabul edileceği enerji altyapıları için hazırlanmış ve enerji altyapılarının süreçlerine özgülenmiş bulunan 27000 ailesinden bir başka standart olan ISO/IEC 27019 Enerji Altyapıları Bilgi Güvenliği Standardı da, bahsi geçen yönetmelik hükmü gereği elektrik piyasası lisans sahipleri için önem arz etmektedir. İlgili standarta ilişkin detaylara doğrudan bu piyasayı etkileyen düzenlemeler başlığında daha detaylı şekilde yer verilecektir.

3.2.2. Tallinn El Kitabı (Tallinn Manual)

Tallinn Manual, NATO Müşterek Siber Savunma Mükemmelliyet Merkezi (Cooperative Cyber Defence Centre of Excellence) öncülüğünde, bağımsız siber güvenlik uzmanları, ordu mensupları, hukukçular, ekonomistler ve pek çok yetkinlikten insanın katkılarıyla hazırlanan, siber savaş hukuku konusunda referans olarak kullanılan bir belgedir. NATO CCD COE, Estonya'nın başkenti Tallin'de faaliyet gösteren bir merkez olarak, siber savunma konusundaki iş birliği ve eğitim faaliyetlerini gerçekleştirmekte olup, merkez olarak Tallin'i seçerek bu kenti siber saldırı tarihçesi açısından bir nevi anıtlıştırmıştır. 2007 yılında Estonya'nın başkenti Tallin'de yaşanan ve 27 Nisan'dan 18 Mayıs'a kadar devam eden siber saldırılar ile ülkenin resmi web siteleri, medya kuruluşları, bankalar ve pek çok kurum işlevsiz hale gelmiştir. Estonya'nın Sovyetler Birliği'nden bağımsızlığını kazandığı 1991 yılına ait Sovyet askeri mezarlığında bulunan ve "Bronze Soldier" olarak bilinen bir anıtı taşıma kararı sonrasında çıkan anlaşmazlıkların neticesi başlayan ve arkasında Rusya'nın olduğu düşünülen saldırıların nasıl yapıldığına dair detayları Rus dilinde pek çok dokümanın

yayımlanması ¹⁴¹da bu ihtimali kuvvetlendirmiş ancak saldırının, doğrudan devlet destekli olup olmadığı konusunda kesin bir ispat sağlanamamıştır.

Kötü tecrübelerle sebep olan bu olay, uluslararası camianın da dikkatini çekmiş ve siber saldırıların etkileri ile siber güvenliğin önemi konusundaki tartışmaları tetiklemiştir. Estonya'daki siber saldırılar, devletler arası ilişkilerde siber boyutta yaşanan gerilimleri ve uluslararası normlar konusundaki eksiklikleri de ortaya çıkarmıştır. Bu tür siber saldırıların, genellikle geniş kapsamlı etkilere sahip olabildiği ve toplumun farklı kesimlerinde zararlara neden olabileceği, siber güvenlik önlemlerinin ve hükümetlerin siber tehditlere karşı hazırlıklarının ne kadar önemli olduğu vurgusu neticesinde, NATO bünyesinde kurulan CCD COE ile siber iş birliği, güçlendirme çalışmaları, bilgi paylaşımları, destek mekanizmaları gibi oluşumların önü açılmıştır.

Tallinn Manual, siber savaş hukuku bağlamında, siber saldırıların hukuki boyutuna odaklanarak, uluslararası hukukun, siber uzaydaki uygulanabilirliğini ve yorumlanabilirliğini ele almaktadır. Özellikle siber savaşın tanımı ile siber silahların kullanımı, misilleme ve savunma, uluslararası hukuk kuralları ve hukuki sorumluluk bu kapsamda odaklanılan konulara karşılık gelmektedir. Tallinn Manual, bu konuları tartışarak siber saldırılara karşı nasıl bir hukuki çerçeve oluşturulabileceğine dair NATO üyesi ülkelere rehberlik sağlamayı amaçlar. İlk metni 2003 yılında yayımlandıktan sonra 2017 yılında Tallinn Manual 2.0 ismiyle ikinci ve güncellenmiş metin yayınlanmıştır. Yapılan resmi açıklamaya göre 2021 yılında 3.0 için, 5 yıl sürmesi planlanan güncelleme çalışması da başlamıştır.

Tallinn Manual ile alakalı, ülkelerin silahlı çatışma yahut saldırı olarak kabul edilemeyecek tehditler altında yahut silahlı çatışma devam ederken yaşadıkları siber saldırılara ilişkin bir kaynak olarak kullanılmasına yönelik

¹⁴¹ Rain Ottis, “Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective”, NATO Müşterek Siber Savunma Mükemmeliyet Merkezi (CCDCOE) Talin, Estonya, Ocak 2008, s.2-3.

eleştiriler de mevcuttur¹⁴². Herhangi bir bağlayıcılığı olmadığı halde ve sınırlı kabul edilebilecek savaş halinin, siber uzaydaki yansımalarına ilişkin görüşlerin bulunduğu metnin, çeşitli siber terimlerin, siber suç ya da saldırı tanımlarının referansı olarak kullanılmasının, metnin amacı dışında olduğunu belirten eleştiriler sınırlı bir kullanım alanı olduğunu da vurgulamaktadır. Uluslararası hukuk ve devlet politikaları bakımından bir değeri olduğu muhakkak kabul edilecek bu metnin, özel hukuk kişileri nezdinde ve savaş ortamı dışında rehber olarak kabul edilmesi tartışmaya açıktır.

3.2.3. Avrupa Konseyi Siber Suç Sözleşmesi (Sanal Ortamda İşlenen Suçlar Sözleşmesi)

1 Temmuz 2004 tarihinde imzaya açılan ve Avrupa Konseyi tarafından hazırlanmış, orijinal ismiyle “Convention on Cybercrime”, siber suçlara ilişkin düzenlenmiş ilk uluslararası metin olma özelliğini göstermektedir. Avrupa Birliği üyesi ülkeler ile imzacısı olacak ülkeler arasında siber suçlara yönelik, uluslararası iş birliği ve adli yardımlaşma sağlanabilmesi, ortak bir ceza politikasının belirlenmesi ve siber suçlarla etkili bir şekilde mücadele edilebilmesi amaçlarına hizmet etmek üzere hazırlanan sözleşme, internet ve diğer bilgisayar ağları üzerinden işlenen suçlara yönelik olarak da özellikle telif hakkı ihlalleri, dolandırıcılık, çocuk pornografisi ve ağ güvenliği ihlalleri ile ilgili suçların tespiti konusunda, delil temin edebilmek için bilgisayar ağlarının aranması ve dinlemesine dair yetki ve usulü de içermektedir. Sanal Ortamda İşlenen Suçlar Sözleşmesi, Budapeşte Sözleşmesi gibi farklı isimlerle de anılan ve Türkiye’de daha yaygın kullanılan ismiyle Avrupa Konseyi Siber Suç Sözleşmesi, Türkiye tarafından da bazı çekince ve beyanlarla kabul edilmiş olup, 1 Ocak 2015 tarihinden itibaren yürürlüktedir ¹⁴³ . Sözleşmeye öncelikle 2003 yılında

¹⁴² Michael J. Adams, “A Warning About Tallinn 2.0 ... Whatever It Says”, The Lawfare Institute, 4 Ocak 2017, link: <https://www.lawfaremedia.org/article/warning-about-tallinn-20-%E2%80%A6-whatever-it-says>, (Son erişim tarihi: 22.06.2024)

¹⁴³ Sanal Ortamda İşlenen Suçlar Sözleşmesi’nin, 28988 sayılı ve 2 Mayıs 2014 tarihli Resmi Gazete’de yayımlanan 6533 sayılı Kanun ile çekinceler ve beyanlarla onaylanması uygun bulunmuş olup, 29083 sayı ve 9 Ağustos 2014 tarihli Resmi Gazete’de yayımlanan 2014/6656 sayılı Bakanlar Kurulu kararında çekince beyanlarla onaylandığı ilan edilmiştir.

“Bilgisayar sistemleri aracılığıyla işlenen ırkçı ve yabancı düşmanı nitelikteki eylemlerin suç sayılmasına ilişkin Siber Suçlar Sözleşmesine Ek Protokol” yapılmış ve 1 Mart 2006’dan itibaren yürürlüğe gireceği kararlaştırılmış¹⁴⁴, sonrasında da 2022 yılında yeni bir ek protokol düzenlemiştir. 12 Mayıs 2022 tarihinde imzaya açılan ikinci protokol *“Gelişmiş işbirliği ve elektronik delillerin ifşasına ilişkin Siber Suçlar Sözleşmesi İkinci Ek Protokolü”* olarak anılmaktadır¹⁴⁵.

Gelişen teknoloji ve bilişim altyapısına sahip araçların çeşitliliği neticesinde, daha önce Avrupa Konseyi Siber Suç Sözleşmesi’nde yer verilmiş olan bilgisayar verisi ve bilgisayar sistemi tanımları gibi tanımlar ile sistemlere düzenlenen saldırılara ilişkin yaklaşımın da gözden geçirilmesi gerekmiştir. Kimlik hırsızlığı, oltalama, hizmet engelleme saldırıları, kritik bilgi altyapısı saldırıları ve yeni kötü amaçlı yazılım türleri¹⁴⁶ gibi çeşitli siber suç alanlarında sözleşmenin tarafları arasında ortak bir anlayış sağlamak belirlenmesi adına 2019 yılında bir rehber yayınlamıştır¹⁴⁷. Bunun yanında 2016 yılında ABD seçimlerinde yaşanan dijital manipülasyonun yarattığı etkinin önemine binaen, ilgili metinde elektronik seçimlere müdahale konusunda ayrıca değerlendirmelerde bulunmuştur¹⁴⁸. Bilgisayarların erişilebilirliği ve dolayısıyla kullanımı sınırlıyken, günümüzde pek çok insanın sahip olduğu akıllı telefonlar ile de bilgisayarlar aracılığıyla yapılması mümkün işlemlerin yapılabilir olması, siber suçların bu gelişimle paralel olarak çok farklı aracı hedef alıp yöntemlerini değiştirmesi bu güncellenmenin yapılmasını zorunlu kılan bir başka neden olarak gösterilebilir.

¹⁴⁴ Bkz. AB Konseyi, “Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189)”, 28 Ocak 2003.

¹⁴⁵ Bkz. AB Konseyi, “Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224)”, 12 Mayıs 2022.

¹⁴⁶ AB Konseyi, Siber Suçlar Sözleşmesi Komitesi, “T-Cy Guidance Notes” Strazburg, Fransa, 8 Temmuz 2019, s.4-24.

¹⁴⁷ age. S.2.

¹⁴⁸ age. S.36.

Avrupa Konseyi Siber Suç Sözleşmesi'nin, siber suçların tüm dünyada önlenmesi, suç tanımlarının yeknesaklaştırılması, yaptırımlar ve yargılamaya yönelik yol gösterici niteliğinin yanında, 3. Kısımda düzenlenen uluslararası işbirliğine ilişkin yükümlülüklerin oldukça önem arz ettiği söylenebilir. Teknolojik gelişme hızıyla beraber gelişim gösteren siber suç tanımlarına yönelik ve uygun şablonların hazırlanmasında yaşanan zorluk, ilgili suçların yeni olması sebebiyle tahlilinde farkındalık ve bilgi eksikliği, suç tanımlarına ilişkin ülkeden ülkeye tanımların farklılık göstermesi, sınırötesi ve mekan bağımsız şekilde işlenebilen suçların işlenmesindeki kolaylık ile tespitinde yaşanan zorluklar bu nitelikte bir uluslararası işbirliği ile yardımlaşmayı gerekli kılmıştır¹⁴⁹. Bu yolda BM, OECD, G-8 organizasyonları tarafından siber suçlara ilişkin atılan adımların, metin ile somutlaşmış hali kabul edilebilecek ilgili sözleşme, bu kapsamda yapılacak farklı anlaşmaların yahut ulusal mevzuatın da önünü açmakta olup¹⁵⁰ ayrıca etkin, pratik ve siber suçların doğasına uygun yöntemleri de adli yardımlaşma kurallarına dahil etmektedir.

Avrupa Konseyi açıklaması uyarınca, hukuki bir metin olmaktan daha fazlasına hizmet etmesi beklentisi taşıyan sözleşmenin, bir rehber, kontrol listesi ve hatta model kanun olarak kullanılabileceği belirtilmektedir.¹⁵¹ Avrupa Konseyi Siber Suç Sözleşmesi, siber suç tanımı yapmış olmasa da bilgisayar verisi, bilgisayar sistemi, hizmet sağlayıcı ve trafik verisi gibi genel tanımlar yaparak metnin özüne ve uluslararası düzeyde siber saldırıların kabulü ile yönetimine ilişkin önemli bir çerçeve belirlemiştir. Ulusal düzeyde alınması gereken tedbirler bakımından, hangi eylemlerin suç olarak düzenlenmesi gerektiği, yaptırımları, yargılanmasına ilişkin usul kuralları, suçun tespitine ilişkin delillerin tespiti, yargılamanın yapılacağı yerin yetkisine ilişkin düzenlemelerin yanında,

¹⁴⁹ Murat Önok, “Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede uluslararası İşbirliği”, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, Prof. Dr. Nur Centel'e Armağan, Cilt: 19 Sayı: 2, 1229 - 1270, 01 Aralık 2013, s.1232-1236.

¹⁵⁰ Age. S.1249.

¹⁵¹ Council of Europe, The Budapest Convention on Cybercrime: benefits and impact in practice, Strazburg, 2020, syf:44.

uluslararası iş birliği bakımından önemli ilkelerin belirlendiği ilgili Sözleşme, siber suçlara ilişkin suçluların iadesi, karşılıklı yardımlaşma ilkeleri, 7/24 iletişim hattı gibi gerçek hayatta uygulamaya ilişkin usulleri de belirlemiş durumdadır.

İlgili sözleşme sayesinde, belirli çekinceler ve beyanları bulunuyor olsa dahi Türkiye ile imzacı ülkeler arasında adli bir işbirliği bulunduğu ve gerekmesi halinde, yalnızca bilgisayar sistemleri aracılığıyla işlenen suçlar yönünden değil elektronik bir delili içeren herhangi bir suç tipine ilişkin olarak delil toplanması, suçluların iadesi yahut bir diğer devlet tarafından haberdar olunmayan ve suç unsuru içeren konulara yönelik bilgilendirmelerde bulunulması mümkün görünmektedir. Bu kapsamda gelecek taleplere yanıt vermiyor olmak, sözleşme hükümleri uyarınca bir yaptırımı gerekli kılmıyorsa da çift taraflı bilgi akışı ve işbirliğine imkan sağlayan hükümler gereği işlevselliğini kaybetmeyeceği ve siber suçlara ilişkin gerçek ve tüzel kişilerin mahiyetinde bulunması muhtemel delillerin toplanması, sistemlere erişilmesi, kaydedilmiş verilerinin iletiminin sağlanması gibi ulusal olarak önemi haiz desteklerin devamlılığının sağlanacağı öngörülmektedir.

3.2.4. AB Siber Güvenlik Düzenlemeleri

Siber güvenliğin tüm dünyada olduğu gibi AB için de önemi, siber tehditlerin, uluslararası bir tahribat yöntemi olarak kullanılmaya başlanması ve bunlardan korunulması için koordineli, topyekün bir çaba gerektirdiğinin farkına varılmasıyla artmıştır. AB, siber güvenlik konusunda Komisyon raporları, Konsey direktifleri ve çeşitli inisiyatiflerin aracılığı ile yürütülen çalışmalar ve bilhassa kritik altyapıların korunması, kişisel verilerin korunması, siber güvenlik stratejisi, ağ ve bilgi güvenliği regülasyonları ile sağlam temeller inşa etmiş siber güvenliğe yönelik pek çok düzenlemeye imza atmış ve nihayetinde de, 2019 yılında çıkardığı Siber Güvenlik Yasası'yla kapsayıcı ve etkin bir çerçeve çizmiştir¹⁵². Bu

¹⁵² Oğuz, 2021 s. 40.

yasanının oluşturulmasından evvel de AB siber güvenliğe yönelik pek çok düzenlemeye imza atmıştır.

Siber güvenlik alanında yapılandırılmış bir iş birliği ve politika geliştirilmesi gerektiği, bunun yanında uluslararası düzeyde de iş birliği aracılığı ile etkin bir koruma sağlanacağına kabulü ve gerekli yatırımların yapılması adına öncelikle, 1992 yılında Bilgi Sistemlerinin Güvenliği Kararı yayımlanmıştır¹⁵³. Siber güvenliğe ilişkin komite kurulmasından, yapılacak çalışmalar için öngörülen bütçeden ve konuya ilişkin bir eylem planının hazırlanması gerekliliğinden bahsedilen karar ile siber güvenliğe yönelik çalışmaların ilk adımları atılmıştır. Kararın ardından, AB Komisyonu tarafından 2000 yılında yayımlanan Bilgi Altyapılarının Güvenliğinin Artırılması ve Bilgisayarla İlgili Suçlarla Mücadele Tebliği ile de daha güvenli bir bilgi toplumu yaratmak için bilgi altyapılarının güvenliğini artırma ve bilgisayar vasıtasıyla işlenen suçlarla mücadele etme ihtiyacı, fikri mülkiyetin ve kişisel verilerin korunması, elektronik ortamın teşvik edilmesi, elektronik imzaların kullanımıyla işlem güvenliğinin sağlanması ve çocukların internet ortamında istismarı da ele alınmıştır. Ulusal ve uluslararası düzeyde bildirimlerin artırılması, etkili yaptırımlar, bilgisayar suçları konusunda uzmanlaşmış polis birimleri, kolluk kuvvetleri için teknik eğitim ve bilgisayarla ilgili suçlarla mücadelede karşılıklı anlayış ile işbirliğini geliştirmek üzere bir AB Forumu kurulması önerilmiştir¹⁵⁴. Bir sonraki yıl 2001’de ise, bu önerinin hayata geçirilmesi adına atılan bir diğer adım olarak Avrupa Konseyi Siber Suç Sözleşmesi’nin kabul edilmesi gösterilebilir. Bu sözleşme, ulusal yasaları uyumlu hale getirmeyi ve siber suçlarla mücadelede uluslararası iş birliğini güçlendirmeyi amaçlamıştır. Yalnızca AB üyesi ülkelerin değil diğer devletlerin de imzacısı olduğu sözleşmenin, siber suçların uluslararası düzeyde etkin bir iş birliği içinde çözümü konusunda önemli bir kaynak olduğu

¹⁵³ AB Konseyi, 92/242/EEC Sayılı Karar, in the field of security of information systems”, Mart 1992.

¹⁵⁴ Bkz. AB Komisyonu, 2000/890 Sayılı Rapor, “Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime”, Ocak 2001, s.2-3.

söylenir. 3.1.3 sayılı başlıkta Türkiye'nin de imzacısı olduğu sözleşmeye ilişkin detaylı açıklamaya yer verilmiştir.

Siber suçlar konusunda çalışmalar devam ederken, 1995 yılında kişisel verilerin işlenmesine ilişkin bireylerin korunması ve verilerin serbet dolaşımı adına hazırlanmış olan 95/46/EC sayılı Direktif ile de kişisel verilerin işlenmesi ve korunmasına, dolayısıyla da kişisel veriler açısından siber güvenliğe temas eden önemli bir düzenleme yapılmıştır. AB pazarının gelişimin önünün açılmaya çalışıldığı ancak bu cihetle kişisel verilerin güvenliğinin de önemini vurgulayan ilgili direktif ile veri işlemeye yönelik ilkelerin yanı sıra teknik ve idari seviyede korunmasına yönelik önlemlerin alınması gerekliliği ortaya konmuştur.

Devam eden süreçte AB adına, AB Forumu, Ortak Araştırmalar Merkezi (Joint Research Center) gibi farklı kurum çatıları altında devam eden siber güvenliğe ilişkin çalışmaların yeknesaklaştırılması ve bu konuda uzmanlığın geliştirilmesi amacıyla 2004/460/EC sayılı Tüzük ile Avrupa Birliği Siber Güvenlik Ajansı (European Union Agency for Cybersecurity) kısa adıyla "ENISA" kurulmuştur¹⁵⁵. 2004/460/EC sayılı Tüzüğün 3. Maddesi ENISA'ya,

- Ağ ve bilgi güvenliğinde mevcut ve ortaya çıkabilecek riskleri analiz etmek ve bu hususta üye devletler ile AB Komisyonu'nu bilgilendirmek,
- Avrupa Parlamentosu, Avrupa Komisyonu ve diğer Avrupa Birliği kurumları ve ulusal kurumlara ağ ve bilgi güvenliği konularında tavsiye ve yardım sağlamak,
- Özel sektörde yer alan, üniversiteler ve ilgili diğer sektörler ile ağ ve bilgi güvenliği alanındaki farklı aktörler arasında işbirliğinin geliştirilmesi,
- Ağ ve bilgi güvenliği sorunlarının önlenmesi,

¹⁵⁵ AB Konseyi ve Parlamentosu, 460/2004 Sayılı Tüzük, "establishing the European Network and Information Security Agency", Mart 2004, madde 1.

- Ağ ve bilgi güvenliği sorunlarına müdahale edilmesi için ortak metodolojilerin geliştirilmesi,
- Donanım ve yazılımların güvenlik sorunlarına yönelik AB ülkeleri ve AB Komisyonu ile işbirliğinin kolaylaştırılması,
- Ağ ve bilgi güvenliğine yönelik ürün ve hizmetlere ilişkin standartların geliştirilmesi,
- Belirtilen hususlarda farkındalığın artırılması,
- Kamu ve özel sektör kuruluşları bünyesinde risk değerlendirme faaliyetlerinin, birlikte çalışabilir risk yönetimi çözümlerinin ve önleme yönetimi çözümlerine ilişkin çalışmaların geliştirilmesi,
- Üçüncü ülkeler ve uluslararası kuruluşlarla işbirliği yapılması ve koruma önlemlerine ilişkin küresel bir yaklaşımın teşvik edilmesi gibi görevler verilmiştir.

ENISA'ya ayrıca AB Komisyonu'na siber güvenlik konusunda danışmanlık yapılması ile belirtilen görevlere yönelik tavsiyelerde bulunulması imkanı da sağlanmıştır. Verilen bu görevler ile AB içerisinde yüksek ve etkili bir ağ ve bilgi güvenliği seviyesi sağlanması, vatandaşların, tüketicilerin, işletmeler ile kamu sektörü kuruluşlarının yararına bir siber güvenlik kültürü geliştirilmesi amaçlanmıştır. İlk etapta 14 Mart 2004 tarihinden itibaren 5 yıl süreyle görev yapacağı belirlenen ENISA'nın görev süresi, etki ve önemi itibarıyla devamlı uzatılmıştır. ENISA'nın kuruluşuna kaynaklık eden 2004/460/EC sayılı Regülasyon ise 2013 tarihinde güncellenmiştir¹⁵⁶. 2013/526/EC sayılı Regülasyon ile ENISA'nın görev ve sorumlulukları yeniden belirlenmiş ve kurum içi yapısına

¹⁵⁶ Bkz. AB Konseyi ve Parlamentosu, 526/2013 Sayılı Tüzük, “concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004”, Mayıs 2013.

ilişkin ayrıntılı düzenlemelere yer verilmiş olup, görev süresi 19 Haziran 2013'te itibaren 7 yıl olarak güncellenmiştir.

Siber güvenliğe ilişkin kurum altyapısının güçlendirilmesi adına devam eden çalışmaların yanında AB, 2013 yılında siber savunmaya yönelik bütünleşik bir yaklaşımın temelini atan, kendi siber güvenlik stratejisini de geliştirmiştir. 2013 yılının şubat ayında AB Komisyonu tarafından için Siber Güvenlik Stratejisi: Açık, Güvenilir ve Güvenli Siber Alan (Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace") ismiyle siber güvenlik alanındaki ilk strateji belgesi yayımlanmıştır. AB Siber Güvenlik Stratejisi'nin siber çevikliğin sağlanması başlıklı 2.1 bölümünde, siber güvenlik için etkili adımlar atılmış olmasına rağmen özel sektör ve bilhassa kritik altyapıların katılımının geliştirilmesi, aksi halde siber güvenlik olaylarını önlemek, tespit etmek ve ele almak için kamu ve özel kapasitelerini, kaynaklarını ve süreçlerini geliştirmek adına yeterli çabayı göstermezse kamu ve özel sektörün savunmasız kalacağı vurgulanmıştır. AB'nin siber güvenliğine ilişkin genel performansını artırabilmek adına, ulusal düzeyde Ağ ve Bilgi Güvenliği (NIS) için ortak asgari gerekliliklerin oluşturulması, siber güvenlik olaylarına ilişkin önleme, tespit, azaltma ve müdahale mekanizmalarının koordinasyonu ve tüm bunlara özel sektörün katılımının de geliştirilmesi gerektiği belirtilmiştir¹⁵⁷. AB Siber Güvenlik Stratejisi'nde ayrıca AB genelinde ortak ve yüksek bir Ağ ve Bilgi Güvenliği (NIS) seviyesi yakalanabilmesi adına bir mevzuat düzenlenmesinin gerekliliğinden de bahsedilmektedir. Özellikle,

- Ulusal düzeyde ağ ve bilgi sistemleri için ortak asgari gerekliliklerin belirlenmesi,
- Üye Devletlerin ağ ve bilgi güvenliğine yönelik ulusal yetkili makamları belirlenmesi,

¹⁵⁷ AB Komisyonu, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace" 2013/1, 2013, s.5-7.

- Üye Devletlerin ulusal bir ağ ve bilgi güvenliği stratejisi hazırlanması ve ulusal düzeyde bir işbirliği planının kabul edilmesi,
- Ulusal ağ ve bilgi güvenliği yetkili makamları arasında bilgi paylaşımını ve karşılıklı yardımı mümkün kılan koordineli önleme, tespit, hafifletme ve müdahale mekanizmalarının kurulması,
- Ulusal ağ ve bilgi güvenliği yetkili makamları arasında, özellikle sınır ötesi boyutu olan siber olaylara müdahale etmek üzere tasarlanmış AB geneli için bir işbirliği planı oluşturulması,
- Siber güvenlik açısından önem arz eden özel sektör kuruluşlarının hazırlığı ve katılımının geliştirilmesi,
- Özel sektör kuruluşlarının teknik düzeyde kendi siber dayanıklılık kapasitelerini geliştirmesinin önünün açılması ve iyi uygulama örneklerinin sektörler arasında paylaşmanın desteklenmesi konularını içeren ve AB üye ülkeleri arasında minimum güvenlik seviyesinin sağlanmasının gerekliliği AB Siber Güvenlik Stratejisinin öne çıkan başlıklarını oluşturmaktadır.

AB Siber Güvenlik Stratejisi'nde yer alan bu beklentileri karşılamak üzere, AB Konseyi tarafından 2016 yılının Temmuz ayında, 2016/1148 sayılı "Ağ ve Bilgi Sistemlerinin Güvenliği Hakkında Direktif (concerning measures for a high common level of security of network and information systems across the Union) kısa adıyla NIS Direktifi yayınlanmıştır. NIS Direktifi, AB üye devletleri arasında ağ ve bilgi güvenliğini, özel sektör kuruluşlarına da belirli sorumluluklar yükleyerek AB Siber Güvenlik Stratejisinde yer alan şekilde yüksek ve bir ortak seviyede buluşmasını amaçlamaktadır. Bu direktif, temel hizmet operatörleri ve dijital hizmet sağlayıcıları için güvenlik ve bildirim yükümlülüklerini belirlemiş olup, AB üye devletleri arasında siber güvenlik olaylarına ilişkin işbirliği ve bilgi paylaşımını teşvik etmektedir. 2016/1148 sayılı Direktifin, stratejik işbirliği ve bilgi alış veriş, farkındalığın artırılması, tatbikatlar düzenlenmesi, iyi uygulama örneklerinin paylaşılması gibi görevlerin yerine getirmesi adına İş Birliği

Grubunun¹⁵⁸ kurulması, üye ülkelerin belirlenen sektörlere ilişkin CSIRT'leri (Bilgisayar Güvenliği Olay Müdahale Ekibi) oluşturularak birliktelik içinde çalışması¹⁵⁹ ve bu amaçla ENISA'nın koordinasyonunu yürüteceği bir ağ kurulması ile çalışmalarının İş Birliği Grubu ile paylaşılması yönündeki hükümleri¹⁶⁰ de paylaşım, işbirliği ve ortak iradeye verilen önemi göstermektedir.

NIS Direktifi, yükümlülük bağlamında tarafları ikiye ayırarak temel hizmet operatörlerinin yanı sıra dijital servis sağlayıcılara da belirli sorumluluklar yüklemiştir¹⁶¹. Temel hizmet operatörü olarak tanımlanmış bu kuruluşlar, NIS Direktifi'nin ekinde alt sektörlere ayrılarak sayılmıştır. NIS Direktifi'nin 4 ve 5. Maddeleri uyarınca bir kuruluşun faaliyetlerinin;

- Kritik bir toplumsal hizmet ya da ekonomik faaliyete karşılık geliyor olması,
- Söz konusu hizmetin sağlanmasının ağ ve bilgi sistemlerine bağlı olarak olması,
- Söz konusu hizmetin sağlanamıyor olması halinde toplumda önemli bir etki ve aksamanın olması halinde, ilgili kuruluşun temel hizmet operatörü olarak kabul edileceği belirtilmiştir.

Temel hizmet operatörü olarak tanımlanmış bu kuruluşlar NIS Direktifi'nin ekinde alt sektörlere ayrılarak sayılmıştır. Buna göre enerji sektöründe elektrik, petrol ve gaz temel hizmet operatörleri olarak kabul görmüş ve elektrik sektörünün alt sektörleri olarak Avrupa Parlamentosu ve Konsey'in 2009/72/EC sayılı Direktifindeki tanımlanmalarına göre 'tedarik' işlevini yerine getiren kuruluşlar, dağıtım sistemi operatörleri ve iletim sistemi operatörleri temel hizmet

¹⁵⁸ AB Komisyonu, 1 Şubat 2017 tarih ve 2017/179 sayılı karar ile "NIS Cooperation Group" kurulmuştur.

¹⁵⁹ AB Konseyi, 2016/1148 Sayılı Direktif, "concerning measures for a high common level of security of network and information systems across the Union", Temmuz 2016, , m.9, s.19.

¹⁶⁰ age. M.10,S.19-20.

¹⁶¹ Age. Gerekçe 7, s.2.

operatörü olarak kabul edilmiştir. Ancak üye ülkelerin bu listede olmayan sektör ya da alt sektör gruplarını da temel hizmet operatörleri kategorisine ekleme imkan ve ihtimali bulunmaktadır¹⁶². Enerji sektörünün de dahil edildiği ve ayrıca önem atfedildiği temel hizmet operatörlerine yönelik yükümlülükler NIS Direktifi'nin 14. Maddesinde yer verilmiştir. İlgili görevler;

- Faaliyetlerinde kullandıkları ağ ve bilgi sistemlerinin güvenliğine yönelik riskleri yönetmek için uygun ve orantılı teknik ve organizasyonel önlemlerin alınması,
- Temel hizmetlerin sağlanması için kullanılan ağ ve bilgi sistemlerinin güvenliğini etkileyen olayların önlenmesi ve etkisinin en aza indirilmesi için, bu hizmetlerin sürekliliğini sağlamak amacıyla uygun önlemlerin alınması,
- Sundukları temel hizmetlerin sürekliliği üzerinde önemli bir etkisi olan olayları gecikmeksizin yetkili makama veya Bilgisayar Güvenliği Olay Müdahale Ekibine (CSIRT) bildirilmesi ve bildirimin yetkili makamın veya CSIRT'in olayın sınır ötesi etkilerini belirlemesini sağlayacak bilgileri içermesi,
- Bir olayın etkisinin önem derecesini belirlemek için etkilenen kullanıcı sayısı, olayın süresi ve etkilenen alana ilişkin coğrafi yayılım gibi parametrelerin dikkate alınması,
- Olayın Üye Devletlerdeki temel hizmetlerin devamlılığı üzerinde önemli bir etkisi olması halinde, etkilenen diğer Üye Devletlerin bilgilendirilmesi,
- Olay bildiriminin takibine ilişkin ilgili bilgilerin sağlanmasında yetkili makam veya CSIRT ile işbirliği yapılması,

¹⁶² Age. Gerekçe 19, 5. Madde 1. Fıkra s.2,14.

- Devam eden bir olayı önlemek veya bu olayla başa çıkmak için kamu farkındalığının gerekli olduğu münferit olaylar hakkında kamuoyunu bilgilendirmeden önce yetkili makam veya CSIRT ile istişarede bulunulması,
- Bir olayın etkisinin önem derecesini belirlemeye yönelik parametreler de dahil olmak üzere, olayların hangi durumlarda bildirilmesi gerektiğine ilişkin kılavuz ilkelerin geliştirilmesi ve kabul edilmesi, şeklinde sıralanmıştır.

Görüleceği üzere bu yükümlülükler, temel hizmetlerin güvenliğini ve sürekliliğini sağlamak ile temel hizmet operatörleriyle yetkili makamlar veya CSIRT'ler arasında işbirliği ve bilgi paylaşımını arttırmayı hedef almaktadır.

NIS Direktifi ilgili sektörlerde yaşanacak siber tehditlerin yarattığı özel zorlukların da giderilmesi amacıyla, AB içinde siber güvenliği güçlendirmek ve enerji, ulaşım, bankacılık, sağlık hizmetleri ve dijital altyapı gibi sektörlerdeki siber tehditlere karşı direnci artırmak amacıyla farklı yükümlülükler de getirmiştir. NIS Direktifi ile ağ ve bilgi sistemlerinin tüm AB genelinde yüksek bir koruma seviyesinde bulunabilmesi için bir çerçeve oluşturulması, üye devletlerin ulusal siber güvenlik stratejileri ve olay müdahale mekanizmaları benimsemesi gerekliliği bunlardan bir kaçıdır. İlgili Direktif ile ENISA'ya da siber güvenlik seviyesini geliştirilmesi aşamasında önemli roller verilmiştir. ENISA'dan genel ve yüksek bir siber güvenlik seviyesi sağlanması adına tavsiyelerde bulunması, iyi uygulamaların değişimini kolaylaştırması ve yaygınlaştırması, ulusal stratejilerin değerlendirilmesine yardımcı olup, kılavuzlar geliştirmesi, ilgili kurumlarla işbirliği yapması ve bu amaçla uluslararası ağlara katılmanın yanı sıra, ulusal CSIRT'lerin ve kurulacak ağ için sekretarya görevini üstlenerek geliştirilmesine yardımcı olmaya ilişkin sorumluluk alması beklenmektedir. ENISA, ayrıca ağ ve bilgi sistemi güvenliği için standartların ve spesifikasyonların gelişimi ile kullanımını teşvik etmek konusunda da görevli konumundadır. Ancak 2016 yılında getirilen bu yükümlülükler 2019 yılında

yürürlüğe giren Siber Güvenlik Yasası¹⁶³ ile yeniden düzenlemiş ve genişletilmiştir. Özellikle ENISA ile alakalı sorumluluk alanını genişleten ve netleştiren Siber Güvenlik Yasası ile 2013/526/EC sayılı regülasyon yürürlükten kaldırılmışsa da 2016/1148/EC sayılı NIS Direktifi yürürlükte kalmaya devam etmektedir.

Siber Güvenlik Yasası, IoT cihazlarının gelişimi ile bu alandaki yetersiz güvenlik uygulamalarından, Türkiye’de hazırlanmış siber güvenlik stratejilerine benzer şekilde ürünlerin millileştirilmesi anlamına gelebilecek AB dışından gelen ürünlere olan bağımlılığın azaltılması gerektiğinden bahsedilmiştir. Avrupa Veri Koruma Tüzüğü’nde (GDPR) vurgulandığı ve yer verildiği şekilde “varsayılan güvenlik” anlayışının geliştirilmesi vurgulanmış ve bilgi ve iletişim teknolojilerine ilişkin süreç ve ürünlerin bu yaklaşımla hazırlanması gerektiğinden bahsetmiştir.

Tüketici güvenin tesisi amacıyla, ortak bir güvenlik sertifikasyon çalışmasının başlatılması gerektiği de belirtilerek, Siber Güvenlik Yasası’nın 51. Maddesinde tanımlanan güvenlik hedeflerine uygun şekilde bu yöndeki planların geliştirileceği anlaşılmaktadır. Bu amaçla 1992 yılından itibaren sağlanmaya çalışılan standartizasyon çalışmalarına yönelik somut adımlardan biri kabul edilebilecek Siber Güvenlik Yasası ile bu konuda alınacak aksiyonların şeklini de çizmiştir. Standardizasyona yönelik çalışmalar için Madde 8’de görevli kuruluşun ENISA olduğu ve standartizasyon için kurulması planlanan Avrupa Siber Güvenlik Sertifikasyon Grubunun koordinasyonunu sağlayacağı, sekreteryaya görevlerini yerine getireceği, kılavuzluk edeceği ve standartlara ilişkin teknik şartname konusunda teklifte bulunacağı gibi görevler tesis edilmiştir. Avrupa Siber Güvenlik Sertifikasyon Grubu kurulması, ürün, hizmet veya süreçlerin değerlendirilmesi ile siber güvenlik sertifikasyon programının düzenlenmesi

¹⁶³ AB Parlamentosu ve AB Konseyi 2019/881 sayılı Regülasyon “on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)”

hedefi doğrultusunda çalışmalar devam etmektedir. Standardizasyona yönelik ENISA tarafından atılması beklenen adımlar;

- Siber güvenlik standartları ve en iyi uygulamalar hakkında bilgi toplamak ve analiz etmek.,
- Siber güvenlik standartlarına ilişkin bilgi ve bilgileri yaymak.,
- Standartlaştırılmış kriterleri ve gereklilikleri içeren Avrupa siber güvenlik sertifikasyon programlarının geliştirilmesi ve uygulanması,
- Bu sertifikasyon programlarının benimsenmesini ve gözden geçirilmesini sağlamak için ilgili paydaşlarla işbirliği yapmak şeklinde sıralanmıştır.

Üye Devletlerin ayrıca kendi ulusal siber güvenlik sertifikasyon programlarını oluşturmalarının da önü açılmış olup aynı zamanda bu hususta bir yeknesaklığın sağlanması gerektiği de belirtilmiştir. Siber Güvenlik Yasası'nın farklı hükümleriyle ENISA'ya sertifikasyon sürecinin koordinasyonu, tatbikat düzenlenmesi, siber güvenliğe ilişkin farkındalık ve eğitimlerin yapılması, yaşanan siber olaylara ilişkin ardıl denetimler yapılması, uluslararası kuruluşlarla işbirliği hususlarına ilişkin pek çok görev de tesis edilmiştir.

AB'nin siber güvenlik anlayışının yansıması ve gelişimin parçası olarak yayımladığı Siber Dayanaklılık Yasası tasarısı ve etki analizi ile de siber güvenlik hukukunun geliştirilmesi ve güncellenmesine devam edilmektedir. AB'de başlı başına siber güvenlik alanına yönelik hukuki düzenlemelerin yapılması ise bu alanda gelişimin sağlanması adına örnek alınması gereken tablo ortaya koymaktadır.

3.3. ELEKTRİK PİYASASINA ÖZGÜ SİBER GÜVENLİK DÜZENLEMELERİ

3.3.1. Enerji Sektöründe Siber Güvenlik Yetkinlik Modeli Yönetmeliği

6 Haziran 2023 tarihinde yayımlanan güncel ve Enerji Sektöründe Siber Güvenlik Yetkinlik Modeli Yönetmeliği (bundan sonra Siber Güvenlik Yetkinlik Modeli olarak anılacaktır), 2017’de yayımlanmış Enerji Sektöründe Kullanılan Endüstriyel Kontrol Sistemlerinde Bilişim Güvenliği Yönetmeliği isimli ilk versiyonunu mülga hale getirmiştir. Siber Güvenlik Yetkinlik Modeli, enerji piyasasında kullanılan endüstriyel kontrol sistemlerinin güvenliğine ilişkin alınması beklenen önlemlere belirlilik kazandırılması adına önemli bir çerçeve oluşturulmuştur. Yeni yönetmeliğin özellikle Enerji Sektöründe Kullanılan Endüstriyel Kontrol Sistemlerinde Bilişim Güvenliği Yönetmeliği ile yalnızca endüstriyel kontrol sistemlerinin güvenliği ile sınırlı bir düzenleme getirilmiş olması bakımından yetkinliği ve yeterliliği konusunda endişeleri bertaraf ettiği düşünülebilir. Bir işletmenin endüstriyel kontrol sistemlerine bağlı olarak çalışmalar gerçekleştiriyor olması, yalnızca bu alanda gerekli güvenlik önlemlerinin alınmasıyla risk faktörünün bertaraf edildiği anlamına gelmeyeceğinden, bunun dışında ya da buna bağlı sistemlerin güvenliği açısından da gerekli önlemlerin alınması gerekmesi de ilgili yönetmeliğin yürürlükten kaldırılarak Siber Güvenlik Yetkinlik Modeli’nin yürürlüğe girmesine sebep olarak kabul edilebilir görünmektedir.

Güncel versiyonu ile mülga yönetmelik karşılaştırılması yapıldığında öne çıkan hususlardan biri endüstriyel kontrol sistemleri¹⁶⁴ ve kritik enerji

¹⁶⁴ Mülga Enerji Sektöründe Kullanılan Endüstriyel Kontrol Sistemlerinde Bilişim Güvenliği Yönetmeliği, Madde 4’e göre endüstriyel kontrol sistemleri “Enerjinin üretilmesi, enerji sağlayan ham petrol, taş kömürü ve benzeri hammaddelerin işlenip tüketime hazır hale getirilmesi, enerjinin iletim veya dağıtım katmanları aracılığı ile aktarılması gibi süreçlerin bir veya birden fazla merkezden izlenmesini, bazen de yönetilmesini sağlayan, kendisi ve/veya bileşenleri bilinen işletim sistemleri üzerinde koştan ya da bilinen zaafiyetleri bulunan özel işletim sistemine sahip yönetim ve kontrol sistemlerini (Veri Tabanlı Kontrol ve Gözetleme Sistemi “SCADA”, Dağıtılmış Kontrol Sistemi “DKS”, Gelişmiş Süreç Kontrol Sistemi “APC”, Programlanabilir Mantık Kontrolcüsü “PLC”, Uzak Terminal Ünitesi (RTU) vb.)” şeklinde tanımlanmıştır.

altyapıları ¹⁶⁵ tanımlarına ilişkindir. Bir mevzuat ile tanımlanmamış olması nedeniyle enerji piyasası bakış açısıyla bu iki tanımın karşılık geldiği anlamlar oldukça önemlidir. Tanımın başlığı itibariyle kritik altyapıları değil kritik enerji altyapılarını belirlemeye yönelik olduğunu belirtmek gerekir. Mülga yönetmelikte 6. Madde ile yükümlü kuruluşların kimler olduğu sayılmış olup, kapsam başlıklı 2. Madde ile de bu altyapıların kritik enerji altyapısı olarak kabul edildiği yorumu yapılabilmektedir. Zira mülga yönetmeliğin, kapsam başlıklı 2. Maddesinde “Enerji Piyasası Düzenleme Kurumu tarafından kritik altyapı olarak belirlenen yükümlü kuruluşların EKS’lerinde kullanılan bilişim sistemlerinin güvenliği ve güvenilirliğinin sağlanması” amacıyla ilgili Yönetmelik’in düzenlendiği belirtilmiştir. Ancak Siber Güvenlik Yetkinlik Modeli’nde, Yönetmelik kapsamındaki kuruluşların kritik altyapı olarak kabul edildiğine ilişkin bir hüküm bulunmamakta olup, yükümlü kuruluşları düzenleyen 2. maddesinin 28 Ocak 2024 tarihinde değişen hali ile,

- Elektrik iletim lisansı sahibi,
- Elektrik dağıtım lisansı sahibi,
- Kurulu gücü 100 MWe ve üzeri lisansa sahip her bir elektrik üretim tesisi sahibi, (kabulü yapılmış)
- Boru hattı ile iletim yapan doğal gaz iletim lisansı sahibi,
- Sevkiyat kontrol merkezi kurmakla yükümlü doğal gaz dağıtım lisansı sahibi,
- Doğal gaz depolama lisansı sahibi (LNG, yer altı depolama),

¹⁶⁵ Mülga Enerji Sektöründe Kullanılan Endüstriyel Kontrol Sistemlerinde Bilişim Güvenliği Yönetmeliği, Madde 4’e göre kritik enerji altyapısı, “İşlevlerini kısmen veya tamamen, yerine getiremediğinde, toplumsal düzenin sürdürülebilirliğinin ve/veya kamu hizmetlerinin sunumunun olumsuz etkileneceği enerji ağı, varlığı, sistemi ve yapıları bütünü” olarak tanımlanmıştır.

- Ham petrol iletim lisansı sahibi,
- Rafinerici lisansı sahibi,
- Black-Start¹⁶⁶ özelliğine sahip olup ulusal şebekeye katkı verebilecek olan elektrik üretim tesisi sahibi (kabulü yapılmış)
- TEİAŞ SCADA/EMS ile seri tabanlı iletişim yöntemlerini kullanmadan haberleşmekte olan elektrik üretim tesisi sahibi (kabulü yapılmış)
- OSB dağıtım lisansı sahipleri ile OSB üretim lisansı sahipleri dışındaki tüzel kişiler şeklindedir. Belirtilen bu kurumlar, Siber Güvenlik Yetkinlik Modeli kapsamında olup gerekli yükümlülükleri yerine getirmek dışında bir tanım altında toplanmamıştır.

Her ne kadar Siber Güvenlik Yetkinlik Modeli'nde kritik altyapıyı işaret eden bir hüküm bulunmasa da, kapsam dahilindeki kuruluşların enerji piyasası içinde önemli ve hassas olarak kabul edilmiş ve buna bağlı olarak belirli yükümlülükler altında bırakılmış olduğu, her halükarda siber güvenlik bağlamında önlem alması gerekli görülen kuruluşlar olduğu yorumu, mülga yönetmelikte yer alan kritik enerji altyapısına ilişkin hüküm de göz önünde bulundurulduğunda uygun görünmektedir. Bunun yanında güncel yönetmelikte, kritik enerji altyapılarına yönelik bir tanım yapılmaktan kaçınılmış olunmasının bir kanun hükmü ile açıkça ortaya konmamış, yalnızca sektör bazlı şekilde belirlenmiş kritik altyapılara karşılık gelen şirketlerin kimler olduğunun belirlenmesinde daha kapsayıcı bir bakış açısının gerekli olabileceği endişesi ile vazgeçildiği düşünülebilir. Ancak siber güvenlik konusunda olgunluğun artırılması adına Siber Güvenlik Yetkinlik Modeli'nde değişiklik yapılmak üzere 2023 aralıkta kamuoyuna açılmış taslak metin ile birlikte yayımlanan gerekçede diğer lisans sahipleri için teknik kontrol madde setlerinin çalışmasına devam

¹⁶⁶ Enerji Sektöründe Siber Güvenlik Yetkinlik Modeli Yönetmeliği, Tanımlar başlıklı 4. Maddesi gereği Black-Start “Bir elektrik santralının veya bir elektrik şebekesinin bir bölümünün, tamamen veya kısmen kapandığında, harici elektrik güç iletim şebekesinin desteği olmadan yeniden başlatılmasını,” ifade etmektedir.

edildiği, güncel durumda dikkate alınan sektör dinamiklerinin elektrik üretim ve rafinericisi lisans sahibi kuruluşlar için de teknik kontrol madde setlerinin yayımlanmasının öncelikli olduğu belirtilmiş olup¹⁶⁷ taslak metin ile ilk adımlar atılmıştır. Bu durum da kritik altyapı tanımı yapılsın yapılmasın önem arz ettiği düşünülen sektörlere yönelik siber güvenlik alanında çalışmaların yapılacağını ortaya koymuştur.

Siber Güvenlik Yetkinlik Modeli'nin ilişkili düzenlemeler başlıklı 5. maddesi ile Bilgi ve İletişim Güvenliği Rehberi, Enerji Sektöründe Kullanılan Endüstriyel Kontrol Sistemleri İçin Güvenlik Analiz ve Test Usul ve Esasları, TS ISO/IEC 27001 ile TS ISO/IEC 27019'da yer alan esasların da kaynak olarak kabul edildiği ve bunlarla çalışmıyacak şekilde hazırlanmış bir düzenleme olduğu anlaşılmaktadır. Mülga yönetmelikten farklı olarak, bir siber güvenlik modeli geliştirilmesi aşamasında, dahil edilmesi gereken tedarikçi yönetimi, akıllı cihaz yönetimi, insan kaynakları gibi pek alan ve bu alanlardaki kontroller de oldukça detaylı bir şekilde sayılmış durumdadır. Yetkinlik modelinin içermesi beklenen başlıklar ve içerikler aşağıdaki tabloda yer almaktadır. Belirlenen bu başlıklara ilişkin sağlanması beklenen kontrol maddeleri ise Siber Güvenlik Yetkinlik Modeli eki olarak yayımlanmış durumdadır.

Tablo 3. 5. Enerji Sektöründe Siber Güvenlik Yetkinlik Modeli Yönetmeliği Kapsamında Belirlenen Yetkinlik Modeli Kontrol Başlıkları ile Tanımları

Yetkinlik Modeli Kontrol Başlıkları	Yetkinlik Modeli Kontrol Başlığı Tanımı
Endüstriyel ağ güvenliği	Endüstriyel altyapılar için yerel ağ güvenliği, geniş alan ağ güvenliği, iletişim güvenliği, protokol güvenliği, kablosuz ağ

¹⁶⁷ EPDK, “Enerji Sektöründe Siber Güvenlik Yetkinlik Modeli Yönetmeliğinde Değişiklik Yapılmasına Dair Yönetmelik Taslağı Gerekçesi”, 2023.

	güvenliği, entegrasyon güvenliği kontrollerini içerir.
Endüstriyel istemci ve sunucu güvenliği	Endüstriyel altyapıda yer alan tüm istemci ve sunuculara ilişkin mantıksal ve fiziksel güvenlik kontrollerini içerir.
Endüstriyel tehdit ve zafiyet yönetimi	Endüstriyel altyapılarda uygulanan tehdit ve zafiyet yönetimi kontrollerini içerir.
Endüstriyel siber güvenlik risk yönetimi	Endüstriyel altyapının dinamiklerine uygun endüstriyel siber güvenlik risk yönetimi kontrollerini içerir.
Endüstriyel varlık, değişim ve konfigürasyon yönetimi	Endüstriyel altyapılarda bulunan varlıkların yönetimi, bileşenlerin değişim ve konfigürasyon yönetimi kontrollerini içerir.
Endüstriyel kimlik ve erişim yönetimi	Endüstriyel altyapıda bulunan bileşenler için kimlik ve erişim yönetimi kontrollerini içerir.
Endüstriyel olay yönetimi ve süreklilik	Endüstriyel siber güvenlik olay yönetimi, süreklilik, yedekleme ve yedeklilik kontrollerini içerir.

Akıllı cihaz güvenliği	Sayaç ve nesnelerin interneti teknolojisinin kullanıldığı endüstriyel altyapılar için güvenlik kontrollerini içerir.
Endüstriyel operasyon güvenliği	Endüstriyel operasyon güvenliğine yönelik kontrolleri içerir.
İnsan kaynakları güvenliği	Kritik enerji altyapılarında çalışan tüm personel için istihdam öncesi, sırası ve sonrasında uygulanması gereken kontrolleri içerir.
Fiziksel güvenlik	Endüstriyel altyapıların sektörlerine uygun, dağıtık veya tekil yapıdaki fiziksel ortamların güvenlik kontrollerini içerir.
Tedarikçi yönetimi	Endüstriyel altyapılar için teknoloji, insan ve altyapı tedarikçilerine ilişkin siber güvenlik kontrollerini içerir.
PLC güvenliği	PLC güvenliğine ilişkin güvenlik kontrollerini içerir.

Belirlenen başlıkların her biri için ayrı ayrı kontrol adımları belirleyen Siber Güvenlik Yetkinlik Modeli, hali hazırda uygulandığı ya da kolayca uygulanabileceği değerlendirilen kontroller için 1. Seviye, sistemlerde veya süreçlerde değişiklik yapılmasını gerektiren yükümlülükler ve kontroller için 2.

Seviye, yeni bir proje ya da uzun soluklu deęişim gerektiren yükümlölükler için de 3. Seviye olmak üzere toplam 3 seviyede yetkinlik belirleyerek, güvenlik sağlanması açısından önem derecesine uygun şekilde efor harcanabilmesine adına oldukça pratik bir yaklaşım geliştirmiş durumdadır.

28 Ocak 2024 tarihinde yapılan deęişiklik sonrasında, Siber Güvenlik Yetkinlik Modeli'nin Uygulama başlıklı 9. Maddenin 1. Fıkrası uyarınca, kritiklik derecelerinin ve dolayısıyla asgari seviyelerin EPDK tarafından belirleneceęi düzenlenmiştir. EPDK'nın resmi sayfasında yapılan açıklamaya ve EPDK tarafından belirlenen parametrelere göre ilgili şirketler kritiklik dereceleri sınıflandırılmış ve listesi güvenlik gerekçesi ile halka açık olarak yayımlanmayacağı, ancak kritiklik derecesi ve sağlanması beklenen asgari güvenlik seviyesinin, yükümlü kuruluşun yalnızca kendisi ile paylaşılacağı belirtilmiştir¹⁶⁸. Ayrıca ilgililere ilişkin yetkinlik süreç uyum takvimleri ile siber güvenlik yetkinlik modeline ilişkin referans topolojiler de yayımlanmıştır¹⁶⁹. Bu seviyelerin yanı sıra Siber Güvenlik Yetkinlik Modeli ile kritiklik dereceleri de A sınıfı, B Sınıfı ve C Sınıfı olarak belirlenmiştir. 3. Seviyede kontrolleri alması beklenen kuruluşlar A sınıfı 2. Seviyede kontrolleri alması beklenenler B sınıfı 1. Seviye kontrolleri alması beklenen kuruluşların C sınıfı olarak kabul edilmiştir.

Tablo 3. 6. Siber Güvenlik Yetkinlik Modeli Uyarınca Sektörel Kritiklik Dereceleri

Sektör	Asgari Seviye	Kritiklik Derecesi
Elektrik Dağıtım	Seviye 2	Yükümlü kuruluşa özel

¹⁶⁸ EPDK, “Enerji Sektöründe Siber Güvenlik Yetkinlik Modeli Yönetmelięi Sıkça Sorulan Sorular” link: <https://www.epdk.gov.tr/Detay/Icerik/3-33073/enerji-sektorunde-siber-guvenlik-yetkinlik-modeli->, (Son erişim tarihi: 22.06.2024)

¹⁶⁹ EPDK, “Sektörel Bilgi Güvenlięi Listesi” link: <https://www.epdk.gov.tr/Detay/Icerik/3-0-57/sektorel-bilgi-guvenligi>, (Son erişim tarihi: 20.04.2024)

Doğal Gaz Dağıtım	Seviye 1	Yükümlü kuruluş özel
Elektrik Üretim	Seviye 1	Yükümlü kuruluş özel
Rafineri	Seviye 3	Yükümlü kuruluş özel

1. Seviye giriş seviyesi kontrolleri açısından Siber Güvenlik Olgunluk Modeli kapsamındaki bir kuruluşun analiz ve ilk geliştirme seviyesi olduğu düşünülebilir. 2. Seviye kontrollerin ise siber güvenlik seviyesinin ilerletildiği gelişim aşaması olarak kabul edilmesi mümkündür. 3. Seviye kontrolleri ise kuruluşun Siber Güvenlik Olgunluk Modeli ile hedeflenen aşamaya gelmesini sağlayacak kademe olarak değerlendirilmesi anlamına gelebilecektir. Her halükarda ilgili seviyeler için belirlenen ve Siber Güvenlik Olgunluk Modeli ekinde gösterilen kontrollerin, hedef olarak ve alt sektörlere göre farklılık gösterir şekilde gösterilmiş sürede tamamlanması beklenmektedir. Belirlenen 3. Seviyenin yanında ek kontrollerin de her daim uygulamaya geçirilebilmesinin önünde Siber Güvenlik Olgunluk Modeli gereği bir engel bulunmamakla birlikte, uygulanmasının zorunlu olmadığı belirtilmiştir. Sistem ve teknolojilerin hızlı değişimi de göz önünde bulundurularak, EPDK tarafından güncellemelerin yapılacağı ve güncellemeler neticesinde değişen kontrol maddeleri ile bu maddelere ilişkin yetkinlik seviyelerinin de değişebileceği belirtilmiş olduğundan, enerji piyasası ve dolayısıyla elektrik piyasası adına siber güvenlik alanında sürekli bir iyileştirme ve gelişimin amaçlandığı anlaşılmaktadır. Her ne kadar Siber Güvenlik Yetkinlik Modeli içinde elektrik piyasası içinde elektrik dağıtım kuruluşlarının asgari olarak 2. Seviyede belirlenen yükümlülükleri yerine getireceği ve elektrik üretim kuruluşlarının ise 3. Seviyede belirlenen yükümlülükleri yerine getireceği Sektörel Kritiklik Derecesi Belirleme başlıklı 8. Maddede belirtilmişse de, metnin öncesinde bahsedilen 9. Madde gereği EPDK

tarafından ilgili kuruluş özelinde bir değerlendirme yapılarak farklı bir kritiklik derecesi belirlenmesi veyahut bir dağıtım ya da üretim sektörü kuruluşundan asgari seviyenin dışında farklı bir seviyede belirlenmiş yükümlülükleri yerine getirmesinin beklenebileceği de *"Kritiklik derecesi ise Kurumca çeşitli parametreler kullanılarak belirlenmekte olup belirlenen kritiklik derecelerine göre uygulanan asgari kontrol maddelerine yeni kontroller eklenebilir."* Şeklindeki 8. Maddenin 2. Fıkrasının son cümlesinden anlaşılmaktadır.

Mülga yönetmelik ile kuruluşların öncelikle EKS olarak kabul edilecek varlıkları tanıma ve tanımlama yükümlülüğü verilmiş, ardından bu varlıkların risk yönetiminin gerçekleştirilmesine yönelik temel kuralları belirleyerek bunun yanından talep olunabilecek hususların Kurul tarafından belirlenmesi ve EKS'lere yönelik risklerin tespitinden sonra hangilerinin azaltılacağına yönelik kararın kuruluşlara bırakılmış olması, güvenliğe ilişkin yükümlülüklerin sahiplenilmesine ilişkin muğlaklık ve güvenlik seviyesinde asimetrinin oluşması gibi problemleri akıllara getirmektedir. Yeni Siber Güvenlik Yetkinlik Modeli ile düzenlenen seviye ve kritiklik derecesi kavramları sayesinde bu belirsizlik de ortadan kaldırılmış durumdadır. Yanı sıra, belirlenen güvenlik önlemlerine yönelik denetim yükümlülüğü güncel versiyonda da yerini şekil değiştirerek korumuştur. Siber Güvenlik Yetkinlik Modeli'nde yer alan yükümlülüklerle ilişkin EPDK tarafından yapılacak güncelleme periyodunun ve kuruluşlara bildirilen kritiklik derecelerine ilişkin değerlendirmenin 3 yıl olduğu da düzenlenmiştir¹⁷⁰.

Siber Güvenlik Yetkinlik Modeli ile belirlenen yükümlülüklerin denetimi için öncelikle kritiklik derecesi belirlenerek kendisine tebliğ edilen kuruluşun, 3 ay içinde kendi kaynakları ile öz denetim/fark analizi yapması, sonrasında ise koşulları belirlenmiş bağımsız firmalar aracılığı ile sektörel denetim

¹⁷⁰ Enerji Sektöründe Siber Güvenlik Yetkinlik Modeli Yönetmeliği, Yetkinlik Seviyeleri, Madde 7 fıkra 3 "Üç yıllık periyotlarda, Kurum tarafından yapılacak güncellemeler ile kontrol maddeleri ve kontrol maddeleri için tespit edilen yetkinlik seviyeleri değiştirilebilir." Sektörel Kritiklik Derecesi Belirleme, Madde 8 fıkra 3 "Sektörlerin kritiklik derecelendirmesinde kullanılan parametreler, Kurum tarafından üç yıllık periyotlarda güncellenebilir, bu periyotların sonunda yapılan değerlendirmelerde yükümlü kuruluşların kritiklik dereceleri değişebilir."

gerçekleştirilmesi, hem kuruluşların hem de denetim firmalarının ise EPDK tarafından ayrıca denetime tabi tutulması gerektiği düzenlenmiştir. Öz denetim sonrasında kuruluş tam uyum, kısmen uyum, uyumsuz olarak değerlendirilebilecek olup ve beklenen kontrol maddeleri dışında alternatif yöntemler de kapsam dışı olarak nitelendirilebilecektir. Ancak her kuruluşun hedeflenen tamamlama süresi içinde tam uyumlu yani yetkinlik modeli kapsamında yer alan ana kontrol başlıklarında bulunan her bir kontrol maddesine ilişkin gereksinimin modelde yazıldığı şekilde karşılanması beklenmektedir. Öz denetim ve sektörel denetim yükümlülükleri kapsamında hazırlanan raporların, tamamlanmasından itibaren bir ay içerisinde Enerji Piyasası Bildirim Sistemi aracılığıyla iletmeleri beklenmektedir. Kuruluşlar tarafından yaptırılması beklenen sektörel denetimlerin, bulundukları seviyeye bağlı olarak 1. Seviye için 12 ayda bir kez, 2. Seviye için 18 ayda bir kez ve 3. Seviye için 24 ayda bir kez olacak şekilde ve öz denetim analizinde dış kaynak ile çalışılmışsa bu dış kaynak ile aynı olmayacak ve her halükarda aynı firma ile ancak 3 sefer üst üste çalışma koşuluyla tekrarlanması gerekmektedir.

Siber Güvenlik Yetkinlik Modeli kapsamında denetim yapacak firmalar için, Bilgi ve İletişim Güvenliği Rehberi'nde yer alan yükümlülüklerin yerine getirilmesine ilişkin kontrolleri gerçekleştirmeye yetkin kabul edilme ve Bilgi Güvenliği Denetim Rehberi'nin "3.1.1. Denetim Ekibinin Belirlenmesi" başlığı altında yer verilmiş denetim yapma yeterliliğine sahip olma asgari koşullarının¹⁷¹ sağlanmasına ek olarak, denetimleri yapacak firma personelinin, Kritik Altyapılar Ulusal Test Yatağı Merkezi¹⁷² tarafından verilen EKS eğitimleri sonrası başarı sertifikası bulunması da beklenmektedir. Dolayısıyla enerji piyasasında yer alan

¹⁷¹ Tüm denetçilerin TSE tarafından Bilgi ve İletişim Güvenliği Rehberi Uyum Denetimi Hizmeti Veren Personel ve Firma Belgelendirme Programı tamamlamış olması, program kapsamında yetkilendirilen en az bir denetçi ve bir başdenetçi olması, birden fazla varsa en az birinin yoksa başdenetçinin Denetim Koordinatörü olarak gerekli sorumlulukları üstlenmesi beklenmektedir.

¹⁷² Enerji Sektöründe Siber Güvenlik Yetkinlik Modeli Yönetmeliği, Tanımlar Madde 4 f bendi gereği "Sakarya Üniversitesi bünyesinde kurulan kritik enerji altyapılarının modellenmesi ve güvenliği ile ilgili koruyucu ve önleyici çözümlerin araştırılması ve geliştirilmesi amacıyla kurulan merkezi,"ni ifade etmektedir.

sistem ve bileşenlerine hâkim kişilerce, sektörün gereklerine uygun şekilde ve etkili bir denetim yapılması amaçlanmaktadır. Denetim yapacak kuruluşlara ilişkin yetkinlik değerlendirmesinin de Siber Güvenlik Yetkinlik Modeli madde 11 ve devamında gelen hükümlere uygun olarak EPDK tarafından verilebileceği düzenlenmiştir. Dolayısıyla denetim yapması beklenen kuruluşların, EPDK tarafından, denetim yetkisi verilmemiş herhangi bir firmaya yaptıracağı denetimin Siber Güvenlik Yetkinlik Modeli hükümlerine uygun olmayacağı görülmektedir.

3.3.2. Enerji Sektöründe Kullanılan Endüstriyel Kontrol Sistemleri için Güvenlik Analiz ve Test Usul ve Esaslar

Enerji Sektöründe Kullanılan Endüstriyel Kontrol Sistemleri İçin Güvenlik Analiz Ve Test Usul Ve Esaslar, 2019 yılında yayımlanan ilk versiyonu ile Enerji Sektöründe Kullanılan Endüstriyel Kontrol Sistemlerinde Bilişim Güvenliği Yönetmeliği'nin Risk Yönetimi başlıklı 8. Maddesinin 2. Fıkrasında yer alan *“Yükümlü kuruluşların EKS'lere yönelik risklerinin tespiti için yaptırdıkları güvenlik analizi ve testlerinin usul ve esaslarını belirlemeye Kurul yetkilidir.”* Şeklindeki hükmüne istinaden düzenlenmiş teknik yükümlülükleri içermektedir. Enerji Sektöründe Kullanılan Endüstriyel Kontrol Sistemlerinde Bilişim Güvenliği Yönetmeliği'nin güncellenen versiyonu Enerji Sektöründe Siber Güvenlik Yetkinlik Modeli Yönetmeliği'nin 15. Maddesinde yer alan *“Yükümlü kuruluşların EKS'lere yönelik risklerinin tespiti için yaptırdıkları güvenlik analizi ve testlerinin usul ve esaslarını belirlemeye Kurul yetkilidir.”* Şeklinde hükmü uyarınca da ilgili Usul ve Esaslar güncellenerek 16 Temmuz 2023 tarihinde yürürlüğe girmiştir. İlgili Usul ve Esaslar amaç başlıklı 1. maddesinde belirtildiği şekli ile enerji sektöründe kullanılan endüstriyel kontrol sistemlerinde yetkisiz erişim elde edilmesine ve hassas bilgilere ulaşılmasına veya sistem sürekliliğinin aksamasına neden olabilecek güvenlik açıklıklarının sömürülmeden önce tespit edilip giderilmesinin sağlanması için hazırlanmıştır. Bu bağlamda Usul ve Esasları,

- Endüstriyel kontrol sistemleri ağı ve mimari yapının incelenmesi analizini,
- Endüstriyel kontrol sistemleri yapılarında görevli personele yönelik sosyal mühendislik testlerini,
- Endüstriyel kontrol sistemleri ağına zafiyet tarama analizini,
- Endüstriyel kontrol sistemleri ağına zararlı yazılım analizini,
- Kablosuz ağ ve bileşenleri testlerini,
- Endüstriyel kontrol sistemleri ağına sömürü testlerini,

Ve bunlara yönelik teknik detayları içermektedir. Usul ve Esasların yalnızca endüstriyel kontrol sistemiyle sınırlı olmasının bu sistemlere verilen önemin bir gereği olarak kabul edilmesinin yanında, sistemin bağlantılı bulunduğu ortamlarda yaşanacak herhangi bir zaafiyetin de doğrudan etki yaratacağı düşünülerek bir eksiklik olduğu yorumunun yapılması da muhtemeldir.

Enerji Sektöründe Siber Güvenlik Yetkinlik Modeli Yönetmeliğinin ve 15. Maddesi uyarınca yayımlanan Enerji Sektöründe Kullanılan Endüstriyel Kontrol Sistemleri İçin Güvenlik Analiz Ve Test Usul Ve Esaslar uyarınca belirlenen yükümlülüklerin yerine getirilmemesi halinde, Enerji Piyasası Kanunu'nun 16. Maddesinin 1. Fıkrasının c bendi uyarınca aykırılığın niteliğine göre otuz gün içinde giderilmesi veya tekrarlanmamasının ihtar edileceği ve yapılan yazılı ihtar rağmen aykırılığın devam etmesi halinde yahut aykırılık düzeltilmesine imkan bulunmayan hallerde doğrudan idari para cezası verileceği düzenlenmiştir. Siber Güvenlik Yetkinlik Modeli kapsamında bulunduğu belirtilen dağıtım lisansı sahibi şirketler açısından hükmün devamında ayrıca bir düzenleme yer almaktadır. Buna göre mevzuat ihlallerinin EPDK tarafından yönetmelikte belirlenen usul ve esaslara uygun biçimde yerine getirmesinin aksatılması, hizmetin kalitesinin düşmesi ile mevzuata aykırılığın devam etmesi halleri ile şirketin acze düşmesi kararları karşısında aynı maddenin 3. Fıkrasında yer alan idari yaptırımların uygulanacağı

belirlenmiştir. Bu halde, EPDK'nın ilgili dağıtım lisansı sahibi şirketin yönetim kurulu üyelerinde değiştirmek, lisansın yeni kişiye aktarılması gibi önlemleri alabilecektir.

3.3.3. ISO/IEC 27019:2017

ISO/IEC 27019:2017 standardı, elektrik, doğal gaz, petrol gibi enerji sektörlerinde (nükleer enerji tesisleri farklı bir standart düzenlenmiştir) ve bu endüstriye özgü kabul edilen işlem ve kontrol sistemlerine ilişkin bilgi güvenliği yönetimi sağlanabilmesi adına ISO/IEC 27002 kuralları temel alınarak hazırlanmıştır. ISO/IEC 27019:2017,

- Merkezi ve dağıtılmış süreç kontrolü, izleme ve otomasyon teknolojisinin yanı sıra programlama ve parametrelendirme cihazları gibi bunların işletimi için kullanılan bilgi sistemleri;
- Dijital sensör ve aktüatör elemanları da dahil olmak üzere kontrol ve saha cihazları veya Programlanabilir Mantık Kontrolörleri (PLC'ler) gibi dijital kontrolörler ve otomasyon bileşenleri;
- proses kontrol alanında kullanılan, örneğin tamamlayıcı veri görselleştirme görevleri ve kontrol, izleme, veri arşivleme, geçmiş kaydı, raporlama ve dokümantasyon amaçları için tüm diğer destekleyici bilgi sistemleri;
- Proses kontrol alanında kullanılan iletişim teknolojisi, örneğin ağlar, telemetri, telekontrol uygulamaları ve uzaktan kontrol teknolojisi;
- Gelişmiş Ölçüm Altyapısı (AMI) bileşenleri, örneğin akıllı sayaçlar;
- Ölçüm cihazları, örneğin emisyon değerleri için;
- Dijital koruma ve güvenlik sistemleri, örneğin koruma röleleri, güvenlik PLC'leri, acil durum valisi mekanizmaları;

- Enerji yönetim sistemleri, örneğin özel evlerde, konutlarda veya endüstriyel müşteri tesislerinde Dağıtılmış Enerji Kaynakları (DER), elektrikli şarj altyapıları;
- Akıllı şebeke ortamlarının dağıtılmış bileşenleri, örneğin enerji şebekelerinde, özel hanelerde, konutlarda veya endüstriyel müşteri tesislerinde;
- DMS (Dağıtım Yönetim Sistemi) uygulamaları veya OMS (Kesinti Yönetim Sistemi) gibi tüm yazılım, donanım ve uygulamalar ile ekipman ve sistemleri barındıran tüm tesislerin ve belirtilen sistemler için uzaktan bakım sistemlerinin güvenliğine ilişkin esasları düzenlemekte olup, kontrol maddelerini belirler.

ISO/IEC 27019:2017 ayrıca, ISO/IEC 27001:2013'te açıklanan risk değerlendirme ve arıtma süreçlerini, bu belgede sağlanan enerji hizmetleri endüstrisi sektörüne özgü kılavuza uyarlama gerekliliğini de içerir. Oldukça teknik ve enerji sektörüne özgü kontrolleri içeriyor olması nedeniyle ilgil sektör tarafından bilinen standardın getirdiği kontrollerin hayata geçirilmesiyle hem mevzuatta belirlenmiş yükümlülüklerin yerine getirilmesi hem de sistemlerinin güvenliğinin bir kademe daha arttırılmış olması sağlanmaktadır.

3.3.4. Türkiye Elektrik İletim Anonim Şirketi Bilgi Güvenliği Politikaları Yönergesi

İletim lisansı sahibi ve elektrik piyasasına yönelik gözetim ile denetim yetkileri bulunan TEİAŞ tarafından, merkez ve taşra teşkilatı dahil olmak üzere tüm birimlerinde geçerli, personellerin, bilgi sistemleri kullanımına ve İletişim ve Bilgi Sistemleri Dairesi Başkanlığı tarafından yönetimine yönelik kurumsal ve kişisel bilgi güvenliği ilke ve kuralları, Türkiye Elektrik İletim Anonim Şirketi Bilgi Güvenliği Politikaları Yönergesi ile düzenlenmiştir. İlgili Yönerge'de pek çok siber güvenlik kavramına ve teknik unsura ilişkin tanımların yapılmasının yanı sıra, Bilgi Güvenliği Yönetim Sistemi kapsamında politika, prosedür ve el kitabına atıfta

bulunulması, aynı zamanda bir yönetim sistemi çatısı altında bilgi güvenliği süreçlerinin yürütüldüğünü göstermektedir.

Yönerge TEİAŞ bünyesindeki bilgi güvenliğine ilişkin olsa dahi, fiziksel güvenlik, internet erişim ve kullanımı, e-posta, uzaktan erişim, veri tabanı erişim gibi şirket faaliyetleri gereği temas kurulan ve enerji sektöründe bulunan üçüncü tarafları da etkileyecek pek çok süreci düzenlemiş durumdadır. Elektrik piyasasının oldukça kritik bir oyuncusu tarafından yapılmış böyle bir düzenleme oldukça olumlu bir gelişme ve güvenlik adımıdır.



IV. BÖLÜM

ELEKTRİK PİYASASINDAKİ HUKUKİ SORUMLULUK VE YAPTIRIMLAR

Elektrik piyasasında hizmet veren firmalar, hakkında görüş ayrılıkları bulunuyor olsa da, idarenin kamu hizmetlerini görme usullerinden ruhsat (lisans) usulüne uygun şekilde¹⁷³ ve Elektrik Piyasası Kanunu uyarınca, gerekli lisansı temin edip faaliyet göstermeye başlamaktadır. İdare tarafından özel şirketlere aktarılan ancak mevzuatta bu şekilde anılmayan ilgili kamu hizmeti¹⁷⁴, özel şirketler tarafından belirli düzenlemelere tabi şekilde gerçekleştirilmektedir. 1. Başlıkta izah edildiği üzere üretim, iletim, dağıtım, tedarik ve piyasa işletim de dahil olmak üzere tüm elektrik piyasası şirketleri diğer düzenleyici işlemlerin yanında, elektrik piyasasına özgü mevzuat hükümlerine uygun şekilde faaliyet göstermekle yükümlüdür. Bu nedenle diğer piyasalardan farklı olarak, enerji piyasasının düzenleyici otoritesi olan EPDK'ya ve Enerji ve Tabii Kaynaklar Bakanlığı'na karşı yerine getirilmesi gereken özel sorumlulukları mevcuttur. Kritik altyapılara yönelik sorumluluklar da elektrik piyasası özelinde hali hazırda bir sektör ve alt sektör ayrımı yapılmamış olsa da yerine getirilmesi beklenen sorumluluklar olarak kabul görmüş durumdadır. Tüm bunların yanında elektrik piyasası şirketlerinin, aynı piyasada faaliyet gösteren ve iletim lisansı faaliyetlerine ek olarak sistem güvenliği, frekans eşitsizliklerini önleme, yük dengeleme, yatırım planlama, denetim ve benzeri görevleri gereği TEİAŞ'a ve piyasa işlemleri ile mevzuatta belirlenen bildirimlerin yapılması, tarifelerin belirlenmesi, organize elektrik piyasasında faaliyet gösteren taraflara yönelik mali uzlaştırmanın sağlanması, piyasa katılımcılarından alınacak teminatların kontrol ve yönetimi gibi sayılanlarla sınırlı olmayacak şekilde EPIAŞ'a karşı da sorumlulukları olduğu söylenebilir.

Elektrik piyasasında sunulan hizmet ve temin edilen elektrik ile alakalı olarak pek tabi tüketicilere karşı da sorumluluklar mevcuttur. Elektrik hizmetinin

¹⁷³ Atıf Kır, “Kamu Hizmetinin Görülme Usullerinden Ruhsat Usulü Ve Elektrik Piyasası Örneği”, Kırıkkale Üniversitesi (Yüksek Lisans Tezi), 2010, s.117.

¹⁷⁴ Ayşe Merve Öztekin, “Elektrik Piyasasında Lisanslar Ve İdarenin Yetkileri” , Ankara Üniversitesi (Yüksek Lisans Tezi), 2020, s.9.

temini dışında dağıtım hizmeti, iletim hizmeti gibi hizmetler ile elektrik üretimi, elektrik tedariki için şebeke kullanılması zorunluluğunun getirdiği tüm süreçler bir paket olarak tüketicinin karşısına çıkmaktadır. Her ne kadar tüketiciler genel itibariyle tedarik şirketleri ile elektrik satış sözleşmesi imzalıyor olsalar da dağıtım, ve iletim hizmeti veren şirketlerin de tüketiciye karşı sorumlulukları bulunmaktadır. Kamu hizmetinin özel şirketler aracılığı ile görülüyor olması, özel hukuk ilişkisinden doğan sorumluluğun dışında, regülasyon tarafından belirlenmiş başkaca sorumluluklarda elektrik piyasası şirketleri tarafından yerine getirilmek durumundadır. Bu sorumlulukların tam ve gerektiği gibi yerine getirilmemiş olması halinde ise “kalite tazminatı¹⁷⁵” doğmakta ve tüketicilere ödenmesi gerekmektedir. Bu durum da, sorumluluğun sıradan bir mal ve hizmet temini süreci şeklinde işletilmediğini göstermektedir. Belirtilen ve elektrik piyasasında bulunuyor olmanın getirdiği sorumlulukların dışında, ilgili şirketlerin ticari alım satımlarında, kurmuş oldukları şirketin tüzel kişiliğine gereği, şirketin önemli kaynaklarından biri olan çalışanlarına karşı, vergi düzenlemelerinden sosyal güvenlik düzenlemelerinden ya da eğer çalışanları üye ise sendikalara ilişkin düzenlemelerden kaynaklanan pek çok sorumluluğu olduğunu söylemek mümkündür. Elektrik piyasası şirketlerinin bir kısmının halka açık olması sebebiyle aynı zamanda hissedarlarına karşı sorumlulukları da mevcuttur. Kar payı dağıtılması, özel durumların bildirimi, finansal tabloların hazırlanması ile yayımlanması, bağımsız denetimlerin gerçekleştirilmesi, birleşme, bölünme, tür değiştirme, mal varlığı devirleri, faaliyet konusu değişiklikleri gibi konulara ilişkin genel kurul kararı alınması gibi Sermaya Piyasası Kanunu ve ikincil düzenlemelerinden doğan pek çok sorumluluğu yerine getirmesi beklenmektedir.

Doğal olarak elektrik piyasası şirketleri açısından, hem regüle bir piyasada bulunuyor olmanın hem de birden çok sürecin bir araya gelmesiyle mümkün olan bir hizmetin tesis ediliyor olmamanın getirdiği pek çok sorumluluk alanı mevcuttur.

¹⁷⁵ Elektrik Piyasasında Dağıtım ve Perakende Satış Faaliyetlerine İlişkin Kalite Yönetmeliği uyarınca belirlenen yükümlülüklerin yerine getirilememesi halinde tüketicilere ödenmesi beklenen tazminat.

Prof. Ernst Hirsch'in Pratik Hukukta Metot kitabında işaret ettiği üzere hukuki sorumluluğun belirlenebilmesi için öncelikle olayın saptanması, sorunun özünün anlaşılması, olaya uygulanacak hukukun zaman ve yer bakımından tespit edilmesi, nelerin talep edilebileceğinin ve bunların hukuki dayanağının ne olduğunu anlamak önemli olup, belirtilen hususlar açıklığa kavuşmadan bir iddia yahut savunmada bulunmak mümkün olamayacaktır¹⁷⁶. Hukuki sorumluluğun belirlenmesinden evvel yapılacak bu ilk değerlendirme ile taraflar arasındaki hukuki ilişkinin tespiti, bu ilişkideki hangi koşulların bulunduğu yahut bulunmadığı uyuşmazlığın çözümünde atılması gereken adımlar olarak kabul edilmelidir.

Çalışmanın konusu itibarıyla elektrik piyasası şirketlerinin siber güvenliğe yönelik sorumluluklarının incelenmesi amaçlanmış olsa da bu sorumluluğun yerine getirilmesini bekleyen taraf sayısınca inceleme yapılması mümkün olabilecektir. Olayın yarattığı zarar yahut olayın vukuu bulmasına sebep olan tarafların değişmesi halinde de sorumluluk ve incelemenin konusu değişkenlik gösterebilir. Bu nedenle bu kapsamın sınırlarının çizilerek, inceleme alanının daraltılması amacıyla çalışmanın öncesinde incelenen ve siber güvenliğe ilişkin hükümler barındıran mevzuata göre sorumluluğun neler olduğundan bahsetmekle yetinilecektir.

Bunun dışında elektrik piyasasında yaşanacak bir siber güvenlik olayı nedeniyle zarar gören bir tüketicinin belirtilen mevzuat hükümleri uyarınca talepte bulunma imkanı ve bu talebe ilişkin olarak elektrik piyasasının sorumluluğu incelenerek, bu sorumluluğun neleri kapsadığı ve neleri kapsamadığı da değerlendirmeye alınıp çalışmanın amacına ulaşması sağlanacaktır. Kapsam, hem etkin başvuru yollarının görülebilmesi hem de bu başvuru mekanizmalarının işlerliği ve tüketiciye olan faydasının görülebilmesi amacıyla, tüketicilerin doğrudan talep ve başvurularını yapabilecekleri hukuki ilişkiler özelinde

sınırlandırılmıştır. Belirtilen kurumlar yahut incelenen mevzuat dışında da mekanizmaların sürece dahil edilmesi mümkündür. Halka açık şirketlerin 6362 sayılı Kanun'dan doğan yükümlülüklerinin, yatırımcı ve tasarruf sahiplerini korumayı amaçlaması, halka açık olmayan şirketlerin belirtilen kanuna tabi olmamaları bu nedenle daha özel bir düzenleme alanı bulunuyor olduğundan sorumluluk bakımından incelemenin dışında bırakılmıştır.

Bir siber tahribata yol açabilecek eylemlerin pek çoğu da doğası itibariyle bilişim suçu olarak kabul edilebilecektir. Ancak bu suçların işlenmesinde, suçun failinin siber saldırıyı gerçekleştiren olarak kalacağı bir gerçektir. Bu nedenle böyle bir saldırı halinde elektrik piyasasında bulunan tüzel kişilerin suçtan zarar gören, suçun konusu itibariyle bu piyasadaki sistemlerde bilgileri bulunan kişilerin de mağdur olması ihtimali gündeme gelecek olup somut olayın özelliklerine bakılarak bir yargılama yapılması imkanını doğabilecektir. Fakat düzenlenen böyle bir saldırı ve neticesinde yapılacak yargılama, sistemin uğradığı zararı tazmin etmeyi amaçlayan bir ceza sorumluluğu yargılaması olacağından burada hukuki bir sorumluktan bahsetmek ancak ikinci aşamada ve yine özel hukuk mevzuatına dayanarak gündeme gelir. Bu nedenle siber tahribatın, bilişim suçu olarak niteliği de hukuki sorumluluğa etkisi kabul edilerek incelemnin dışında tutulacaktır.

4.1. SİBER SALDIRILAR NEDENİYLE İDARİ OTORİTELERE BAŞVURU İMKANI VE SORUMLULUK

Siber güvenliğe ilişkin pek çok kavramda olduğu gibi siber olay, siber güvenlik ihlali, siber saldırı kavramlarında da bir uzlaşma olmaması somut olayın izahi bakımından kafa karışıklığı yaratmaktadır. 2020-2023 yılları için hazırlanmış Ulusal Siber Güvenlik Strateji ve Eylem Planı içinde siber olay “ *Bilişim ve endüstriyel kontrol sistemlerinin veya bu sistemler tarafından işlenen bilginin/verinin gizliliği, bütünlüğü veya erişilebilirliğinin ihlal edilmesi*” olarak tanımlanmışsa da bu ihlalin kim tarafından gerçekleştirilebilir olduğuna yönelik bir tespit yapılmamıştır. İhlalin gereken önlemlerin alınmaması sebebiyle ortaya

ıkabilmesi gibi bir bařkası tarafından kasıtlı řekilde gerekleřtirilmesi de muhtemeldir. Bu durumda da siber olayın olmasına sebep veren tarafın kim olacađının ve dolayısıyla sorumluluđun kimde olduđunun tespiti konusunda bir netlik bulunmamaktadır. Siber gvenlik nlemleri bakımından yetersiz bir seviyede olması ve siber olayın gerekleřmesinden evvel tespitini yapamaması nedeniyle biliřim sisteminin sahibi mi yoksa siber olayın eylemlerini dođrudan yerine getiren tarafın mı yoksa ikisi tarafın birlikte mi sorumluluđu olduđu konusunda ilgili tanımın aıklayıcı olmadıđı grlmektedir.

Aynı metinde yer alan ve siber gvenlik iin belirlenen “*Siber uzayı oluřturan biliřim sistemlerinin saldırılardan korunmasını, bu ortamda iřlenen bilginin/verinin gizliliđi, btnlđ ve eriřilebilirliđinin gvence altına alınmasını, saldırıların ve siber olayların tespit edilmesini, bu tespitlere karřı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yařanan siber olay ncesi durumlarına geri dndrlmesini kapsayan faaliyetler btn*”n tanımından hareketle de sorumluluđun siber gvenlik nlemlerini alması beklenen tarafta olduđu dřncesi oluřabilecektir. Tanım “siber olayların tespiti” ve “bu tespitlere karřı tepki mekanizmalarının devreye alınması” gibi ykmllkleri de siber gvenlik kapsamında dahil etmiř olduđundan bu gvenliđi sađlayamayan tarafın sorumlu olduđu dřnmek yersiz olmayacaktır.

İlgili tanımlar nedeniyle yařanan belirsizliđi giderebilmek adına, 2020-2023 Ulusal Siber Gvenlik Strateji ve Eylem Planı iinde yer alan “*Siber uzaydaki biliřim ve endstriyel kontrol sistemlerinin veya bu sistemler tarafından iřlenen bilginin/verinin gizliliđi, btnlđ veya eriřilebilirliđini ortadan kaldırmak amacıyla, siber uzayın herhangi bir yerindeki kiři ve/veya biliřim sistemleri tarafından kasıtlı olarak yapılan iřlemler.*” řeklindeki siber saldırı tanımının kullanılması ok da uygun grnmektedir. Tanım itibariyle, zarar veren ve zarar gren taraflara iliřkin daha net tespit yapıldıđından, zararın neden kaynaklandıđı belli olduđundan kavram kafa karıřıklıklarını gidermek bakımından daha kullanıřlı grnmektedir. zellikle bir saldırının, kendini ispat etme, heyecan yaratma, cezalandırma, zarar verme gibi motivasyonlarının yanında kendine fayda

sağlamaya yönelik kötücül amaç¹⁷⁷ unsurunun da bulunduğu düşünüldüğünde bu kavramın, kasıt unsurunu barınması da önemlidir. Tanım itibariyle güvenlik önlemlerinin ihlal edilmesinin arkasında, yerine getirilmesi beklenen kontrollerin yapılmaması ve siber güvenliğin sağlanması amacıyla harekete geçmesi gereken tarafların eksikliğinden ziyade bu önlemlere rağmen kasten bir sistemin gizlilik, bütünlük ve erişilebilirliğine zarar verme eylemi olduğundan, kişilerin sıfatları da daha belirgindir. Dolayısıyla metnin devamında zarar verme kastıyla gerçekleştirilen siber uzaydaki kötücül eylemlerden siber saldırı olarak bahsedilecektir.

Siber saldırı nedeniyle zarara uğrayan kişi ya da kurumlar bu nedenle uğradıkları zararın tazmini isteyebilecekler midir, bu alanda düzenlenmiş kanunlar kişilere ne gibi haklar ihtiva etmektedir, çoğu zaman kim tarafından gerçekleştirildiğinin tespitinin dahi mümkün olmadığı bu saldırılar nedeniyle uluslararası sorumluluklar nelerdir ve kişilere karşı işlenmiş bir suçun ve dolayısıyla cezai yaptırımın oluşması ihtimalinde nasıl bir yol izlenecektir gibi soruların cevabı gün geçtikçe önem kazanmaktadır. Siber saldırı sayılarının yıllar içindeki artışı da bu alanda yapılan çalışmaların gelişmesi gerektiğine işaret etmektedir. Stratejik ve Uluslararası Çalışmalar Merkezi (CSIS) tarafından yapılan, 2006'dan bu yana yaşanan ve 2024 Mart ayının da dahil edildiği çalışmasında, 2017 yılından sonra 20 ve öncesinde yalnızca 3 adet, enerji sektörüne yönelik olarak ise toplamda 41 ve 2017 öncesinde yalnızca 5 adet siber güvenlik olayının kayıt altına alındığı görülmektedir.¹⁷⁸ Bu artışın da göstereceği üzere görülen zarar gün geçtikçe artmaktadır.

Bu denli karmaşık hukuki bağlamların bulunduğu konulara ilişkin hali hazırda uygulamada olan mevzuat hükümlerinin de zararın tazmini ya da güvenliğin sağlanması noktasında neler içerdiğini incelemek bu bölümden sonraki başlığın konusunu oluşturmaktadır. Çalışmanın bu kısmında siber uzayda yaşanan

¹⁷⁷ Acarer, 2020,s.63.

¹⁷⁸ Stratejik ve Uluslararası Çalışmalar Merkezi (CSIS), “Significant Cyber Incidents Since 2006”, 2024.

bir saldırı nedeniyle zarar gören tarafların bir önceki başlıkta belirtilen kısıtlar uyarınca, uğradığı zararın tazmini konusunda, başvurabilecekleri idari otoriteler ve etkinlikleri incelenecektir. Siber uzayın da toplum yaşamının dinamikleri arasına girerek, teknolojik dönüşüm yanında bireylerin hayatında da bir dönüşüm yarattığı ve dolayısıyla hukukun da toplumun bu alandaki dönüşümüne ayak uydurması ve siber uzay için bir istisnaya dönüşmemesi gerekmektedir¹⁷⁹. İzah edildiği üzere çokça taraf ve hak iddiasının gündeme gelmesi mümkün olduğundan, bu başlıkta yalnızca önceki başlıklarda incelemesi yapılan ve siber güvenliğe ilişkin düzenlemeler içeren hukuki metinler göz önünde bulundurularak bir değerlendirme yapılarak, sorumluluk olgusu bu sınır içinde incelenecektir. İdari makamlar nezdinde mevcut mevzuat hükümleri uyarınca sorumlu olarak elektrik piyasasındaki lisans sahibi şirketler ve sorumluluk talebinde bulunan elektrik hizmeti kullanıcısının olduğu varsayımı ve siber güvenlik ihlalinin gerçekleşmesi durumunda hem elektrik arzının kesintiye uğramasından hem de sistemlerin gizliliğine, erişebilirliğine ve bütünlüğüne verilen zarara ilişkin hangi sorumlulukların atfedilebileceği üzerinde durulacaktır.

4.1.1. BTK Nezdinde Sorumluluk

5809 sayılı Elektronik Haberleşme Kanunu uyarınca BTK'ya, siber güvenliğe ilişkin görev atfeden hüküm madde 6'da *“kamu kurum ve kuruluşları ile gerçek ve tüzel kişilere yönelik siber güvenliğin sağlanmasına ilişkin usul ve esasları belirlemek”* şeklinde düzenlenmiştir. Ancak hükmün işaret ettiği şekilde salt siber güvenliğin sağlanmasına yönelik usul ve esasları içeren ve tüm kamu kurum ve kuruluşları ile gerçek ve özel tüzel kişileri kapsayacak nitelikte bir doküman hali hazırda yayımlanmış değildir. Kurumsal ve sektörel siber olaylara mühadaleye ilişkin çalışmalar, USOM tarafından yayımlanmış rehber dokümanlar, Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği, Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunmasına İlişkin Yönetmelik, Güvenli İnternet Kullanımına İlişkin Tebliğ gibi

¹⁷⁹ Hatipoğlu Aydın, 2022, s.2

metinler içinde çeşitli güvenlik tedbirleri belirlenmişse de, BTK tarafından yayımlanan dokümanların elektronik haberleşme sektöründe yer alan kuruluşlara yönelik olduğu ve bu hükmün işlerliğini kısıtlı bir şekilde ve yalnızca ilgili düzenlemeler üzerinden kazanabildiği görülmektedir. Her ne kadar 6. Maddede belirtilen nitelikte bir düzenleme bulunmuyorsa da, 5809 sayılı Kanun ve farklı kanunları dayanak alarak hazırlanmış, Bilgi Teknoloji Kurumu İdari Yaptırımlar Yönetmeliği'nin şebeke ve bilgi güvenliği ile siber güvenliğe ilişkin ihlalleri, başlıklı 19. Maddesinde¹⁸⁰ düzenlemiş olduğu görülmektedir. İlgili düzenlemenin içeriğine bakıldığında ilk fıkranın *“yetkilendirme çerçevesinde elektronik haberleşme hizmeti sunan ve/veya elektronik haberleşme şebekesi sağlayan ve alt yapısını işleten şirketi”* olan işletmeciye ilişkin olduğu ancak 2018 tarihinde eklenen 2. fıkranın böyle bir ayırım gözetmeksizin yazıldığı görülmektedir. Bilgi Teknoloji Kurumu İdari Yaptırımlar Yönetmeliği'nin kapsamını düzenleyen 2. Maddesinde, aşağıdaki tabloda yer alan mevzuat ile BTK düzenlemeleri de dahil olmak üzere belirlenen yükümlülüklerin yerine getirilmemesi ve mevzuata aykırılık halinde uygulanacak yaptırımların, bunların uygulanmasına ilişkin usul ve esasların düzenlenmiş olduğu belirtildiğinden, kapsamında yalnızca elektronik haberleşme sektöründe yer alan işletmeciler ile sınırlı olmadığı neticesine varılması mümkündür.

¹⁸⁰ Bilgi Teknoloji Kurumu İdari Yaptırımlar Yönetmeliği, “Şebeke ve bilgi güvenliği ile siber güvenliğe ilişkin ihlaller MADDE 19 (1) İşletmecinin, şebeke güvenliği de dahil olmak üzere elektronik haberleşme güvenliğine ilişkin mevzuata uymaması halinde bir önceki takvim yılındaki net satışlarının yüzde birine (%1) kadar idari para cezası uygulanır. (2) Ulusal siber güvenlik faaliyetleri ile siber saldırılara karşı korunma ve caydırıcılığın sağlanmasına yönelik Kurumun görevleri kapsamında belirleyeceği yükümlülükleri yerine getirmeyen veya aldıracağı tedbirleri uygulamayan gerçek kişiler ile işletmeciler dışındaki özel hukuk tüzel kişilerine bin liradan bir milyon liraya kadar idarî para cezası uygulanır. Kurum ihlal konusuna ilişkin olarak gerçek veya tüzel kişiden yazılı açıklamalarını 15 günden 30 güne kadar belirlenebilecek süre içerisinde göndermesini ister. Süresinde gönderilmeyen yazılı açıklama dikkate alınmaz.”

Tablo 4. 1. Bilgi Teknoloji Kurumu İdari Yaptırımlar Yönetmeliği Kapsamında Bulunan İlgili Mevzuat Listesi

	İlgili Mevzuat	Açıklaması
1	4/2/1924 tarihli ve 406 sayılı Telgraf ve Telefon Kanunu	Posta ve telgraf tesis ve işletilmesine ilişkin hizmetler ve telekomünikasyon hizmetlerine ilişkin yetkilendirilen işletmecilere ilişkin genel hükümleri içermektedir.
2	29/6/2001 tarihli ve 4703 sayılı Ürünlere İlişkin Teknik Mevzuatın Hazırlanması ve Uygulanmasına Dair Kanun	12.03.2020 tarih ve 31066 sayılı Resmi Gazete’de yayımlanarak yürürlüğe girmiş 7223 Ürün Güvenliği ve Teknik Düzenlemeler Kanunu madde 25 gereği yürürlükten kaldırılmış olup 4703 s. Kanun’a yapılan atıfları üstlenmiş durumdadır. AB üyesi ülkelere ihraç edilen veya ihraç edilmesi hedeflenen ürünlerin güvenli ve ilgili teknik düzenlemelere uygun olmasını sağlamak; piyasa gözetimi ve denetiminin esasları ile yetkili kuruluşların görevlerini ve iktisadi işletmeciler ile uygunluk değerlendirme kuruluşlarının yükümlülüklerini belirlemektedir.
3	15/1/2004 tarihli ve 5070 sayılı Elektronik İmza Kanunu	Elektronik imzanın hukukî ve teknik yönleri ile kullanımına ilişkin esasları düzenlemekte olup, elektronik imzanın hukukî yapısını, elektronik sertifika hizmet sağlayıcılarının

		faaliyetlerini ve her alanda elektronik imzanın kullanımına ilişkin işlemleri kapsamaktadır.
4	4/7/1934 tarihli ve 2559 sayılı Polis Vazife ve Salahiyat Kanunun ek 7 nci maddesi	Casusluk hariç CMK m. 250 f.1 a, b, c bendinde yazılı suçlar ile bilişim suçlarının önlenmesine yönelik olarak hükümde belirtilen usullere uygun şekilde telekomünikasyon yoluyla yapılan iletişim veya internet bağlantı adresleriyle internet kaynakları arasındaki iletişimin tespiti, dinlenmesi, kayda alınması, değerlendirilmesi ve ilgili hususlara yönelik düzenlemeye karşılık gelmektedir.
5	10/3/1983 tarihli ve 2803 sayılı Jandarma, Teşkilat Görev ve Yetkileri Kanunun Ek 5 inci maddesi	Casusluk hariç CMK m. 250 f.1 a, b, c bendinde yazılı suçlar ile bilişim suçlarının önlenmesine yönelik olarak hükümde belirtilen usullere uygun şekilde telekomünikasyon yoluyla yapılan iletişim veya internet bağlantı adresleriyle internet kaynakları arasındaki iletişimin tespiti, dinlenmesi, kayda alınması, değerlendirilmesi ve ilgili hususlara yönelik düzenlemeye karşılık gelmektedir.
6	1/11/1983 tarihli ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu 6 ncı maddesi	Milli İstihbarat Teşkilatı'nın yetkilerini içermektedir.
7	4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi	Madde 135-İletişimin dinlenmesi, tespiti ve kayda alınması,

	Kanunun 135, 136, 137 ve 138 inci maddeleri ile	Madde 136-Müdafinin bürosu ve yerleşim yeri, Madde 137-Kararların yerine getirilmesi, içeriklerin yok edilmesi, Madde 138-Tesadüfen elde edilen delil başlıkları maddelere karşılık gelmektedir.
8	4/5/2007 tarihli ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun	İçerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları ile internet ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usûlleri düzenlemektedir.
9	5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu	Elektronik haberleşme sektöründe düzenleme ve denetleme yoluyla etkin rekabetin tesisi, tüketici haklarının gözetilmesi, ülke genelinde hizmetlerin yaygınlaştırılması, kaynakların etkin ve verimli kullanılması, haberleşme alt yapı, şebeke ve hizmet alanında teknolojik gelişimin ve yeni yatırımların teşvik edilmesi ve bunlara ilişkin usul ve esasların belirlenmesi amacıyla istisna hükümleri dışındakilerle sınırlı olmak üzere elektronik haberleşme hizmetlerinin yürütülmesi ve elektronik haberleşme alt yapı ve şebekesinin tesisi ve işletilmesi ile her türlü elektronik haberleşme cihaz ve sistemlerinin imali, ithali, satışı,

		kurulması, işletilmesi, frekans dahil kıt kaynakların planlaması ve tahsisi ile bu konulara ilişkin düzenleme, yetkilendirme, denetleme ve uzlaştırma faaliyetlerinin yürütülmesini düzenlemektedir.
10	13/1/2011 tarihli ve 6102 sayılı Türk Ticaret Kanunu	Bir ticari işletmeyi ilgilendiren işlem ve fiillere ilişkin diğer kanunlarda yazılı özel hükümler, ticari hükümleri düzenlemektedir.

İlgili kapsam maddesinde sayılan ve oldukça geniş içerikleri haiz 10 adet kanun ve bunun dışında BTK düzenlemeleri uyarınca, Bilgi Teknoloji Kurumu İdari Yaptırımlar Yönetmeliği'nde yer alan “*Ulusal siber güvenlik faaliyetleri ile siber saldırılara karşı korunma ve caydırıcılığın sağlanmasına yönelik Kurumun görevleri kapsamında belirleyeceği yükümlülükleri yerine getirmeyen veya aldiracağı tedbirleri uygulamayan gerçek kişiler ile işletmeciler dışındaki özel hukuk tüzel kişilerine bin liradan bir milyon liraya kadar idarî para cezası uygulanır. Kurum ihlal konusuna ilişkin olarak gerçek veya tüzel kişiden yazılı açıklamalarını 15 günden 30 güne kadar belirlenebilecek süre içerisinde göndermesini ister. Süresinde gönderilmeyen yazılı açıklama dikkate alınmaz.*” şeklindeki 19. Maddenin kapsamının ve dolayısıyla idari yaptırım uygulama yetkisinin de oldukça geniş aynı zamanda hukuki açıdan problemli olduğu görülmektedir. Anayasa Mahkemesi’nin 24.07.2019 tarih ve 2017/16 esas ve 2019/64 karar sayılı dosyasında yapılan incelemeye ilişkin yazılmış karşı oylarda da belirtildiği üzere yalnızca bir kanuni düzenlemenin şeklen varlığının hukuka uygunluk yaratamayacağı, yapılan müdahalenin demokratik toplum düzeninin gerekleri ile ölçülülük ilkesine de uygun olması gerekliliğinin bu düzenleme bağlamında da tartışmaya açılması mümkün görünmektedir. 19. madde uyarınca, siber güvenliğe ilişkin yaptırımı düzenleyen ilgili hükümde de bahsi geçen;

1. “Ulusal siber güvenlik faaliyetleri” kapsamından ne anlaşılması gerektiği,

2. Bir saldırının hangi durumlarda “siber saldırıları” olarak kabul edilmesinin uygun olacağı,
3. “siber saldırılara karşı korunma ve caydırıcılığın sağlanmasına yönelik Kurumun görevleri kapsamında belirleyeceği yükümlülükleri”nin neler olarak kabul edilmesi gerektiği,
4. Kimlerin bu yükümlülükleri “yerine getirmeyen veya aldıracağı tedbirleri uygulamayan gerçek kişiler ile işletmeciler dışındaki özel hukuk tüzel kişileri” olarak kabul edileceği
5. Niçin bu önlemleri almayan “gerçek kişi ve işletmecilerin” yaptırım hükmünün dışında tutulduğu da ayrıca bir belirsizlik yaratmaktadır.

Bu belirsizlik ortamı, suistimallerin artması, siber saldırı kavramının genişletilmesi yahut yanlış tanımlanması, gerçek kişilerin ve işletmelerinin siber güvenlik önlemlerine tabi olmak yükümlülüğünün baştan itibaren yok sayılması ve yaptırımların caydırıcılığından istisna tutulmaları sebebiyle, siber güvenlikte bütünsel bir yaklaşım ve asgari korumanın sağlanmasına zarar verebileceği görülmektedir.

Hükmün kapsamındaki genişlik ve gri alanlar, siber güvenlik alanında kapsayıcı bir düzenleme ile ortadan kaldırılması gerekirken, birden çok kanunda yer alan ve yargı düzeninin farklı alanlarına ilişkin konuların da “siber güvenlik faaliyetleri ve siber saldırılara karşı koruma” çatısı altında idari yaptırım uygulanması neticesinde etkisiz bırakabilecek bir belirsizlik ve güvensizlik yaratmaktadır. Bunun yanı sıra herhangi bir idari yaptırım cezasının, ilgili kurum ve kuruluşa yönelik düzeltici bir işlem olduğu kabul edilebilecekse de, bu olaydan zarar gören taraflara yönelik bir düzenleme içermediği yahut buna işaret eden herhangi bir hükmün ilgili mevzuatta bulunmadığı da görülmektedir.

19. maddenin yanı sıra 24. Madde ve devam hükümlerinde, BTK’nın bilgi belge temini yetkisi ve bu yetki gereği yapılacak taleplerin yerine getirilmemesi

halinde ortaya çıkacak idari yaptırımlar gündeme gelebilecektir. Ulusal siber güvenlik faaliyeti ya da siber saldırı halinde ve kapsam maddesinde yer alan mevzuat hükümleri uyarınca, BTK tarafından talep edilen her türlü bilgi ve/veya belgenin süresinde verilmesi gerekmekte olup, eksik, yanlış yahut yanıltıcı bilgi verilmesi hali yaptırıma tabi kılınmıştır¹⁸¹. Verilecek cezanın belirlenmesinde, zararın varlığı, haksız ekonomik kazancın varlığı, tekerrürün varlığı, aynı madde ihlaline ilişkin olarak işletmeciye son beş yılda uygulanan idari yaptırımlar uygulanıp uygulanmadığı, iyi niyetin varlığı gibi unsurların göz önünde bulundurulacağı da düzenlenmiştir. Bilgi teminine yönelik 24. maddenin, her türlü kurum ve kuruluştan istenebileceği şekilde düzenlenmiş olmasına karşılık, uygulanacak yaptırımın ölçütüne ilişkin 44. Maddenin 1. Fıkrasının ç bendinde “işletmeciye son beş yılda uygulanan idari yaptırımlar uygulanıp uygulanmadığı” düzenlemesi ile işletmecilerin aynı madde ihlaline ilişkin geçmişinin kontrol edileceği belirtilmiş olduğundan, ceza verilmesi hükmünün mü yoksa yaptırımın belirlenmesinde yapılacak değerlendirmenin mi işletmecilere özgü olduğu hususu da kafa karışıklığı yaratmaktadır.

4.1.2. CDDO Nezdinde Sorumluluk

6 Temmuz 2019 tarihinde yayımlanarak yürürlüğe giren Bilgi ve İletişim Güvenliği Tedbirleri konulu Cumhurbaşkanlığı Genelgesi¹⁸² uyarınca hazırlanmış olan Bilgi ve İletişim Güvenliği Rehberi ile Bilgi ve İletişim Güvenliği Denetim Rehberi’nde yer alan yükümlülüklerin, tüm kamu kurum ve kuruluşlarının yanında elektrik piyasasının da içinde bulunduğu kritik altyapıların tarafından yerine getirmesi beklenmektedir. Bu kapsamda BİG Rehber’de belirtilen sorumlukların yerine getirilmiş olup olmadığına ilişkin, BİG Denetim Rehberi’ne uygun şekilde denetimler yapılması öngörülmüştür. Kapsamda bulunan kuruluşlardan olan

¹⁸¹ Bilgi Teknolojileri ve İletişim Kurumu İdari Yaptırımlar Yönetmeliği, Bilgi ve/veya belgenin süresinde verilmemesi madde 23, Yanlış bilgi ve/veya belge verilmesi madde 24, Eksik bilgi ve/veya belge verilmesi madde 25, Yanıltıcı bilgi ve/veya belge verilmesi madde 26.

¹⁸² Bilgi ve İletişim Güvenliği Tedbirleri konulu 2019/12 sayılı Cumhurbaşkanlığı Genelgesi, 30823 sayılı Resmi Gazete (6 Temmuz 2019)

elektrik piyasası şirketlerinin de BİG Rehberin yayım tarihi olan 27 Temmuz 2020 itibarıyla 24 aylık bir uyum süresi sonunda denetim faaliyetlerine başlaması gerekmiştir. 2019/12 sayılı Cumhurbaşkanlığı Genelgesi uyarınca, yılda en az bir defa uygulanması beklenen denetim sonuçlarının, kuruluş genelinde yapılan düzeltici ve önleyici faaliyetleri de içerir şekilde, BİG Denetim Rehberinde belirtilen usul ve esaslara göre bir rapor olarak Dijital Dönüşüm Ofisine göndermesi gerekmektedir. Bu raporlara ilişkin DDO tarafından ilgili mevzuat çerçevesinde gözetim faaliyetlerinin yürütüleceği belirlenmiştir.

Açıklanan süreç neticesinde, raporların neticelerine bakılarak DDO'ya verilen görevlerin yerine getirileceği, ancak denetim sonuçları kapsamında denetimi yapmakla yükümlü kuruluşların akıbetinin ne olacağı belirlenmemiş durumdadır. Denetim neticesinde,

- Kurum varlık gruplarının, Rehberde yer alan varlık grubu ana başlıkları ile uyumlu olacak şekilde tanımlanma durumu,
- Kurum bilgi varlıklarının mutlaka bir varlık grubu altında tanımlanma durumu,
- Varlık grupları tanımlama çalışmalarının varsa bilgi güvenliği yönetim sistemi kapsamında oluşturulan varlık envanteri ile ilişkilendirilme durumu,
- Varlık grupları kritiklik derecelerinin Rehberde uygun olarak belirlenme durumu,
- Varlık gruplarının kritiklik derecesine uygun tedbirlerin belirlenmesi,
- Uygulama ve teknoloji alanına yönelik tedbirler ve sıkılaştırma tedbirlerinin varlık grubu ile uygun bir şekilde eşleştirilmesi,
- Her bir varlık grubu için mevcut durum ve boşluk analizi çalışmalarının yapılması,

- Telafi edici kontrollerin dokümanite edilmesi,
- Rehber uygulama yol haritasının oluřturulma durumuna iliřkin olarak “kısmen gerekleřtirilmiřtir”, “tamamen gerekleřtirilmiřtir”, “hi gerekleřtirilmemiřtir.” řeklinde kategorize edilen bir denetim grřüřü sunulması beklenmektedir.

Bunun dıřında raporun ieriğinde, BİG Denetim Rehberi’nde yer alan,

- a) EK – A’da yer alan Denetim Ekibi Bilgisi
- b) EK – B’de yer alan Varlık Grupları ve Denetim Kapsamı
- c) EK – E’de yer alan Rehber Uygulama Süreci Etkinlik Durumu
- ) EK – F’de yer alan Tedbir Etkinlik Durumu
- d) EK – H’de yer alan Denetim Grřüřü’nin yer alması gerektiğii de belirtilmiřtir.

Belirtilenler dıřında, denetimin ieriğinin gsterildiğii denetim programı ile bulgu tablosunun iletimine ihtiya duyulmamıřtır. Bu durum denetlenen ve denetim sonucu ortaya ıkan aksiyonlardan ziyade, ynetiřim aısından bilgi gvenliğii tedbirlerinin rehberlere uygun řekilde yrtlp yrtlmediğii ynelik bir değeriendirme yapıldığii sonucunu verebilecektir. Zira alınması beklenen aksiyon ve eksikliklerin gsterildiğii bulgu tablosu aslında řirketin kontrol adımlarından hangilerini yerine getirmediğii ve olası bir siber saldırıya karřı ne derece etkin bir gvenlik sağladığının da anlařılmasına yardımcı olabilecektir.

4.1.3. KVKK Nezinde Sorumluluk

Siber saldırının sistemleri bozma, iřlemez yahut eriřilemez hale getirmesi gibi pek ok marifetinin yanında sistemlerde kayıtlı verileri de alma, kopyalama, bozma gibi amalara hizmet ettiğii ve hatta sonrasında elde edilen bu verilerin farklı saldırıların ya da maniplasyon, dolandırıcılık, haksız kazanç, fikri mlkiyet

haklarının ihlali gibi eylemlere konu edildiği sık rastlanan örneklerdendir. Kişisel verilerin işlenmesine ilişkin kuralların yanında, korunmasına ilişkin önlemler de bu nedenle önem arz etmektedir. Bu konuda Stewart Room tarafından Avrupa Veri Koruma Hukuku ve Uygulaması isimli kitabın Verilerin Güvenliği başlıklı bölümünde yazılan “*Veri koruma ilkeleri, veri koruma dünyasının ünlüleri ise güvenlik her zaman öncelikli olanlar listesinde yer alır, gerçek bir VIP'dir.*”¹⁸³ cümlesi de konunun önemini oldukça güzel özetlemektedir.

Kişisel verilerin işlenmesine ilişkin kuralları düzenleyen 6698 sayılı Kanun’na ise herhangi bir siber saldırı durumunda değil, ancak bu siber saldırı nedeniyle kişisel verilerin güvenliğine yönelik sorumlulukların yerine getirilmemesi halinde başvurulabilmektedir. Yani elektrik piyasasında yer alan bir şirkete düzenlenen bir siber saldırının, yalnızca sistemlere zarar vermesi ve elektrik arzının sağlanamaması gibi bir neticesi var ve kişisel verilere hukuka aykırı erişimi ya da işlenmesi gibi bir etkisi yok ise 6698 sayılı Kanun hükümlerinden kaynaklanan bir sorumluluk gündeme gelmemektedir.

İdari yaptırıma sebep olacak ve siber güvenlik önlemi kabul edilebilecek hususların, 6698 sayılı Kanun’nun 12. Maddesine bakıldığında oldukça geniş kapsamlı şekilde ele alındığı da görülecektir. İlgili hüküm ile veri sorumlusu, verilerin hukuka aykırı olarak işlenmesi, erişilmesi ya da muhafazasını sağlamak üzere her türlü teknik ve idari tedbiri almakla mükellef kılınmış durumdadır. Hatta ilgili hüküm verinin işlenmesine ilişkin veri sorumlusu adına başka bir gerçek veya tüzel kişi tarafından gerçekleştirilen bir işleme faaliyetinde de gerekli tedbirlerin alınmasında müştereken sorumlu bulunulduğunu belirtmiştir. Alınacak güvenlik önlemlerine ilişkin yayımlanmış pek çok rehber, ilke karar ve Kurul kararı olduğundan, bu konuda atılacak adımların gün geçtikçe belirginleştiği söylenebilir. Ancak yalnızca ilgili metinlerde yer alan önlemlerin alınmış olmasının da sorumluluktan kurtulunmasına imkan tanımayacak ve somut olayın özelliklerine göre sorumluluk belirlenecektir. Bu kapsamda, kişisel verilere ilişkin korumanın

¹⁸³ Uluslararası Gizlilik Profesyonelleri Birliği (IAPP), “Avrupa Veri Koruması Hukuku ve Uygulaması”, 2. Baskı, 2019, 10. Bölüm, s.1.

gerektiği şekilde yapılıp yapılmadığı, siber saldırı olmasından bağımsız şekilde, KVKK tarafından yapılan inceleme ile ve veri sorumlusunun madde 12 kapsamında gerekli güvenlik önlemlerini alıp almadığı ile sınırlı görünmektedir. KVKK yapacağı inceleme neticesinde, 6698 sayılı Kanun uyarınca bir ihlalin varlığını tespit ettiği takdirde;

1. Veri sorumlusunu ihlali ortadan kaldırması gerektiği yönünde talimatlandırabilir,
2. Veri sorumlusunun idari para cezası ödemesine karar verebilir,
3. Veri işlemenin ve aktarımının durdurulmasına karar verebilir,

4. İhlal kararından bağımsız şekilde görev alanı ve veri güvenliği gibi konularda düzenleyici işlem yapabilir durumdadır. Sayılan yetkilerin dışında her ne kadar ilgili kişinin 6698 sayılı Kanun'nun 11. Ve 14. Maddelerin tazminat talep edebileceğine yönelik hükümler bulunuyorsa da, KVKK tarafından bu yöndeki taleplerin karşılanamayacağı ve mahkeme nezdinde dava yoluna gidilmesi gerektiği 16.01.2020 tarih ve 2020/41 sayılı kararında “ *İlgili kişinin başvurusunda manevi zarara uğradığı yönünde bir iddia ve buna ilişkin bir tazminat talebinin söz konusu olduğu dikkate alınarak, Kanunun 14 üncü maddesinin (3) numaralı fıkrasında yer alan “Kişilik hakları ihlal edilenlerin, genel hükümlere göre tazminat hakkı saklıdır.”* Denilmek suretiyle ortaya konulmuştur. Bu değerlendirme uyarınca, kişilerin gördükleri zararın giderilmesine ilişkin taleplerini KVKK'ya yönlendiremeyecekleri, bu hususta Kurul tarafından tesisi edilecek bir işlem bulunmadığı belirtildiğinden yerleşik bir uygulamaya dönmüştür.

KVKK öncesinde de kişilik hakları temelinde genel hükümlere göre talepte bulunabilme hakkının bulunması sebebiyle 6698 sayılı Kanun'nun amacının da bu nitelikteki taleplere hizmet olmadığını ve farklı ihtiyaçların giderilmesine aracılık ettiğini kabul etmek gerekmektedir. Bu hususta 6698 sayılı Kanun'nun amacının önleyici bir koruma sağlamanın yanında, hem kamu hem de özel hukuk düzeni

içinde veri işlemesine ilişkin temellerin geliştirilmesi olduğu belirtilmektedir¹⁸⁴. Bu amacın ötesine geçecek siber saldırı gibi bir olayın neticelerini tazmin etmekte araç olarak kullanılamayacağı kabul edilmelidir. Kişisel verilerin işlenmesine ilişkin sorumluluk siber güvenliğin önemli bir sorunu olarak kabul edilecekse de yalnızca bir parçası olduğu ve yetkinliği de bu ölçüde sınırlıdır¹⁸⁵.

6698 sayılı Kanun'un referans aldığı 95/46 sayılı Direktifi'nin güncel versiyonu olarak yayımlanan GDPR'da ise kişilerin, kişisel verilerinin korunmasına ilişkin yükümlülüklerin yerine getirilemiş olmasından kaynaklanan tazminat hakları 82. Maddede düzenlenmiştir. GDPR'ın 82. Maddesi ile özellikle, veri sahiplerinin kişisel verilerinin hukuka aykırı işlenmesi durumunda uğradıkları zararın karşılanması için başvurabilecekleri bir hukuki mekanizma sunulmaktadır. Madde 82, bu bağlamda her veri sorumlusuna ve hem de veri işleyene karşı tazminat talep etme hakkı sağlayarak, GDPR ihlallerinden doğan zararlardan ilgilileri müştereken ve müteselsilen sorumlu tutmaya imkan sağlamaktadır. Ancak bu imkanın sınırı olarak bir veri işleyenin yalnızca kendi eylemlerinden sorumlu olduğu ve veri sorumlusunun talimatlarına uygun hareket etmesi durumunda sorumluluğunun sınırlı olabileceği de belirtilmiştir. Tazminat talebi, yalnızca maddi değil aynı zamanda manevi zararları da kapsamaktadır. Örneğin kimlik hırsızlığı veya mali kayıpları içerebilirken; itibar kaybı, psikolojik stres ve kişilik haklarının ihlali gibi durumlara karşılık gelen manevi zararlar konusunda da ihlallerinden etkilenen bireylerin, kendilerine özgü zararları ispat ederek uygun bir tazminat alabilmeleri mümkündür. Doğal olarak GDPR Madde 82'nin uygulanmasında, veri sahiplerinin tazminat talep edebilmesi için zarar ile ihlal arasında bir nedensellik bağı kurmaları gerekmektedir. GDPR'nin tazminat hakkına ilişkin bu düzenlemesi, veri koruma ihlallerinin ciddi sonuçları olabileceğini ortaya koyarak, siber saldırılara ilişkin alınan güvenlik önlemleri bakımından büyük bir işlevsellik yaratmakta, veri koruma yükümlülüklerini yerine getirme konusunda tarafları daha dikkatli ve özenli davranmaya zorunlu kılmaktadır. Ayrıca, düzenleme, bireylerin

¹⁸⁴ Elif Küzeci, "Kişisel Verilerin Korunması", Turhan Kitapevi, Ankara, 3. Baskı, Şubat 2019, s. 389-399.

¹⁸⁵ Kossef, 2018, s.995

veri ihlallerine karşı daha güçlü bir koruma mekanizmasına sahip olunmasını, önemli bir hukuki yükümlülük ile kuvvetli bir caydırıcılık yaratılmasını ve siber güvenliğin önemini de ortaya koymaktadır. Benzer şekilde ülkemizde de siber güvenliğe ilişkin sorumluluğun daha ciddiye alınması ve bireylerin korunmasına ilişkin benzer şekilde kolaylaştırıcı hukuki mekanizmaların kurulmasına ihtiyaç bulunmaktadır.

4.1.4. EPDK Nezdinde Sorumluluk

Elektrik piyasasında herhangi bir kuruluşa düzenlenecek bir saldırının, sistemlerin birbirlerine olan bağlantısı nedeniyle birden çok kurum ve kuruluşun aynı anda etkilemesi ihtimali bulunmaktadır. Ancak elektrik hizmetinin tüketiciye ulaştığı ve sözleşme ilişkisinin doğduğu yerde, tedarik lisansı sahibi şirketler yer almaktadır. Bu noktada tüketicinin göreceği zarar elektrik arzının kesintiye uğraması olduğundan bu hususta kendisine elektrik temin etmek üzere sözleşme düzenlemiş olan tedarik şirketinin, sözleşmeden doğan yükümlülüğünü yerine getirmemiş olması mevzu bahis edilebilecektir. Bunun yanında elektriğin şehir içi şebekesinden kullanım yerlerine kadar taşınması konusunda görevli olan dağıtım şirketleri de aynı şekilde ilgili tüketicie karşı sorumlu kabul edilebilir. Bu kapsamda *“elektriğin yeterli, kaliteli, sürekli, düşük maliyetli ve çevreyle uyumlu bir şekilde kullanıcıların kullanımına sunulması amacıyla elektrik enerjisinin tedarik sürekliliği, ticari ve teknik kalitesine ilişkin dağıtım şirketleri, görevli tedarik şirketleri ve kullanıcılar tarafından uyulması gereken kurallar ile uygulamalara ilişkin usul ve esasları”* EPDK tarafından Elektrik Piyasasında Dağıtım ve Perakende Satış Faaliyetlerine İlişkin Kalite Yönetmeliği’nde (bundan sonra Kalite Yönetmeliği olarak anılacaktır) düzenlenmiş durumdadır.

İlgili Yönetmelik uyarınca bir elektrik kesintinin yarattığı etkinin giderilmesine ilişkin imkanlar sunulmuştur. Elektrik kesintisine bir siber saldırının sebep olması halinin de doğal olarak ilgili yönetmelik kapsamında değerlendirilmesinde bu açıdan bir engel olmadığı görülmektedir. Kalite Yönetmeliği’nin 10. Maddesi uyarınca kesintiler kaynağına, süresine, sebebine ve

bildirimli olup olmadığına bakılarak sınıflandırılmaktadır. Süre ve bildirim durumu ödenecek tazminat tutarını belirlemede ayırıcı faktörlerken, kaynak faktörü ödemenin yapılacağı kanalın belirlenmesinde rol oynamaktadır. Ancak kesintinin sebebinin siber saldırı olması halinde Kalite Yönetmeliği'nde yer alan hangi sebebe dayalı bir başvuru olduğunun tespit edilmesi ilk aşama olacaktır. Sebebine göre kesintiler;

1. Mücbir sebep,
2. Güvenlik,
3. Dışsal,
- 4 Şebeke işletmecisi, olarak ayrılmış durumdadır.

Elektrik kesintisine nasıl bir olayın neden olduğuna göre “kesinti sebebi” tespiti yapılacağı da mevzuatta belirtilmiş olduğundan bu tespitlerin hangisinin siber saldırı halinde uğranacak zarara karşılık geleceğinin belirlenmesi önem arz edecektir. Bu kapsamda güvenlik sebebi dışındaki sebeplerin tamamı siber saldırı nedeniyle gerçekleşen bir kesintinin sebebi olarak belirtilebilecek niteliktedir. Yönetmelik;

- Kesinti sebebi olarak dışsalı, “Dağıtım şirketi tarafından belgelenmek şartıyla; hırsızlık, dağıtım tesisinden kaynaklanmayan yangın ile kullanıcılar veya üçüncü taraflarca dağıtım tesisine verilen hasarlar nedeniyle oluşan kesintilerin sebebi”.
- Kesinti sebebi olarak mücbir sebebi, “Doğal afetler ve salgın hastalıklar, savaş, nükleer ve kimyasal serpinçler, seferberlik halleri, halk ayaklanmaları, saldırı, terör hareketleri ve sabotajlar, grev, lokavt veya diğer memur ve işçi hareketlerinden kaynaklanan kesintiler ile dağıtım şirketinin müdahale kapasitesini aşan ölçekteki durumlar ile önemli sayıda kullanıcıyı etkileyen ve niteliği bakımından giderilmesi zaman alan durumlarda dağıtım şirketi tarafından gerekli özen ve dikkatin gösterilmiş olmasına ve

tüm önlemlerin alınmış olmasına rağmen önlenemeyecek, kaçınılamayacak veya giderilemeyecek mahiyette olduğu ve dağıtım şirketinin yükümlülüklerini yerine getirmesini engellediği gerekçesiyle dağıtım şirketinin başvurusu üzerine EPDK tarafından mücbir sebep olarak kabul edilen kesintilerin sebebi”

- Kesinti sebebi olarak şebeke işletmecisini, “EPDK tarafından mücbir sebep kabul edilmedikçe, iletim şebekesinden kaynaklanan kesintiler,” olarak kabul etmiş durumdadır.

Verilen tanımlardan görüleceği üzere, EPDK tarafından siber saldırıların, mücbir sebep olarak kabul edilmeleri ihtimal dahilindedir. Siber saldırı bakımından mevzuatta hali hazırda uzlaşa sağlanmış bir tanım olmadığı ve önlenmesine ilişkin pek çok yükümlülük farklı metinlerde düzenlendiği halde, siber saldırıya mücbir sebep denilmesi uygun görünmemektedir. Mücbir sebepten kaynaklanan kesintilerin nedenleri arasında her ne kadar “saldırı” bulunuyor da olsa bu kavramın, fiziki ortamda kamu güvenliğini bozup tehlike yaratacak boyutta ve hatta terör eylemi niteliğindeki olaylara atfedilmiş bir kavram olduğu, siber ortamın ise bu eyleme konu yer bakımından dahil edilmemiş olduğu lafzından anlaşılmaktadır. Bunun yanı sıra içtihat kararlarıyla mücbir sebebin tanımı “ *Buna göre, bir hususun mücbir sebep olabilmesi için;*

i-) Hukuki ilişkinin kurulduğu an itibarıyla mücbir sebebin taraflarca öngörülemez, veyahut öngörülse dahi etkilerinin bu denli büyük olacağının öngörülemez olması,

ii) Mücbir sebebin tarafların kontrol alanının dışında gerçekleşmiş olması,

iii) Gereken tüm önlemlerin alınmasına rağmen mücbir sebebin, tarafların sözleşmeden kaynaklanan edimlerini yerine getirmesini imkansızlaştırmasının önlenemeyecek olması gerekir.” Şeklinde¹⁸⁶. Siber

¹⁸⁶ T.C. Yargıtay Hukuk Genel Kurulu E. 2019/19-58 K. 2022/40 T. 25.1.2022.

saldırıları açısından mücbir sebep tanımında yer alan koşulların varlığı incelendiğinde lafzi yorum güçlenmektedir. Zira siber saldırıların yaygınlığı ve hakkında alınan onca güvenlik önlemi nedeniyle öngörülemez olduğunu söylemek mümkün değildir. Kontrol alanı dışında olma koşulu bakımından ise doğrudan kurumların sahip olduğu sistemler hedef alındığında ve sistemler üzerinde tüm yetkilerin kuruma ait olması sebebiyle bu koşulun da gerçekleşmeyeceği görülmektedir. Son olarak tüm önlemlerin alınması halinde siber saldırıya uğranılma ihtimalinin ortadan kalması mümkün olduğu gibi verilen zararın giderilmesi de mümkün olabileceğinden, sözleşmeden kaynaklanan edimin imkansızlaşması da ihtimal dahilinde olmayacaktır. Dolayısıyla siber saldırıların mücbir sebep olarak kabulü en azından her türlü siber saldırı için böyle bir kabulle hareket edilmesi mümkün değildir. Ancak bu yorumun aksine bir şekilde mücbir sebep olarak kabul edilmesi de ihtimal dahilindedir.

Bunun dışında siber saldırının şebeke işletmecisi yahut dışsal olarak kabul etmek imkanı da bulunmaktadır. Zira kesintinin “üçüncü taraflarca dağıtım tesisine verilen hasarlar” nedeniyle oluşması dışsal kesinti olarak kabul etmesine yetmektedir. Bir siber saldırının da bir zarar verme ve fayda elde etme saikiyle düzenlenmiş olduğu kabulünden yola çıkarak bu sebebin de uygun olacağı düşünülebilir. Ancak siber güvenlik ihlali ile siber saldırı kavramlarının en başta izah edilen belirsizliğinin de ayrıca değerlendirmesi gerekecektir.

Tazminat belirlenmesi aşamasında yaşanan bu belirsizliğin yanında hesaplanması aşaması da yaşanan zararın etkilerine ilişkin olumsuz bir örnek teşkil etmektedir. Zira tazminat hesaplanmasında mücbir sebep ödemenin yapılmasına engeldir. İşletim gelir tavanını aşan tutar sebebiyle her bir tazminat kaleminin azaltılması, bir saldırı halinde, iletim şebeke işletmecisine rücu imkanının gündeme gelmesiyle tüketicinin yeni bir muhatap edinmesi gibi hususlar gündeme gelecektir. Hesaplamanın salt bir elektrik kesintisi olarak kabul edilmesi, yaratılması beklenen güven ortamı ve uğranılan diğer zararların tazmini açısından da kısıtlayıcı bir

görünümüne sahiptir. Siber saldırının yaratacağı etkinin elektrik kesintisine indirgenmesi, yaşanan olayın yaratacağı etki karşısında yeterli ve etkin değildir.

Bunun yanında EPDK tarafından düzenlenen Siber Güvenlik Modeli Yönetmeliği kapsamında belirlenmiş yükümlülükler de bulunmaktadır. İlgili başlığın sonunda belirtildiği üzere bu yükümlülüklerin ihtar ve idari para cezası dışında, yönetim kadrosunun değiştirilmesi, lisansın başkasına devri gibi neticeleri bulunmakla birlikte bireylere karşı sorumluluk doğuran bir unsur içermediği görülmektedir. Siber Güvenlik Modeli Yönetmeliği'nin tüm elektrik piyasası şirketleri bakımından da uygulama alanı olmadığı düşünüldüğünde, alınması beklenen tüm güvenlik önlemlerine karşılık Yönetmelik kapsamında olmayan farklı bir elektrik piyasası şirketi nezdinde gerçekleşen bir saldırının elektrik sistemine bağlı diğer kurumlara sirayet etmesi ihtimali de göz ardı edilmiş durumdadır.

Görüleceği üzere pek çok metinde ve idari otoritelerin yetkileri arasında yahut yaptıkları düzenleyici işlemlerde siber güvenlikten bahsedilmektedir. Ancak belirlenen bu güvenliğin hedefindekiler, koruduğu sistemler, sistemin sürdürülebilirliğini sağlama yolundaki eylemlerin, sağladığı faydanın kime hizmet ettiği, bu hizmete karşın ne gibi sorumluluklar ve yükümlükler bulunduğu incelendiğinde siber güvenliğin sağlanamadığı zamanda bireylere karşı ne tür bir korumanın inşa edildiği anlaşılamamaktadır. Yapılan düzenlemelerin pek çoğunda siber güvenliğin teknik olarak varlık nedeni ortaya koyulurken, hukuki olarak karşılığı ya da bu güvenliğin sağlanamadığı durumlar karşısında sorumluluğun kimde olduğunu belirlemekten uzaktır. Sistemlerin gizliliğini, bütünlüğünü ve erişilebilirliğini korumak ve saldırıdan önceki haline getirebilmek hedefiyle korunan ve hukuken himaye altına alınan sistemler midir yoksa güvenliğin sağlanması amacı insanlara mı hizmet etmelidir sorusunun yanıtı genellikle yerine getirilmesi gereken yükümlülükler, alınması beklenen önlemler, kontrol maddeleri arasında göz ardı edilmiş durumdadır.

V. BÖLÜM

SİBER GÜVENLİK YÖNETİMİNE DAİR İYİ UYGULAMALAR VE ÖNERİLER

Dijital teknolojilerin hem kişisel hem de profesyonel alanda giderek daha merkezi bir rol oynadığı günümüzün birbirine bağlı dünyasında, siber güvenlik adına her geçen gün iyi uygulamaların takip edilmesi ve mümkün mertebe mevcut sisteme entegre edilmesi, herkesin ve her şeyin mümkün kılınabildiği siber uzayda en önemli gelişim koşullarından biridir. Bu bağlamda ülkemiz içinde de siber risk sigortalarının yaygınlaşması, siber hijyen, siber esneklik, siber etik gibi kavramlarının geliştirilmesinin üzerinde durulması faydalı olacaktır.

Siber sigorta olarak da bilinen siber risk sigortası, siber saldırılar veya veri ihlallerinden kaynaklanan kayıplara karşı finansal koruma sağlamaktadır. Bu poliçeler genellikle bir siber olay sonucunda ortaya çıkan diğer maliyetlerin yanı sıra veri kurtarma, yasal ücretler ve düzenleyici otoriteler tarafından verilen cezalarla ilgili masrafları da kapsayabilecek klostları içermekte olup, hiç öngörülmemiş yahut öngörülemeyecek siber olaylara karşı da koruma sağlamayı vadetmektedir. Kuruluşlar, siber sigortalar ile siber tehditlerle ilişkili finansal riskin bir kısmını sigorta sağlayıcılarına devrederek olası zararları azaltabilir ve bir siber saldırı sonrasında daha iyi yönetebilmektedir. Siber sigortalar ile hem kurumun dijital dünya üzerinde görmüş olduğu zararların, sigorta ettiren kurumu doğrudan etkileyen fidye, şantaj, itibar kaybı gibi durumlara ilişkin zararın hem de üçüncü tarafların uğrayacağı zararları sigorta ettirmesi mümkündür¹⁸⁷. Risk faktörünün artış gösterdiği siber uzayda, en azından bu şekilde bir sigortanın varlığı hem kurumlar hem de kurumların ilişkide olduğu 3. Taraflar için güvenli bir dijital ortama imkan sağlaması bakımından oldukça değerlidir.

Siber hijyen, bireylerin ve kuruluşların bilgi teknolojisi altyapılarını ve dijital ortamlarını korumak için alabilecekleri basit ancak etkili adımları içeren ve

¹⁸⁷Ufuk Tekin, “Hukukî Açıdan Siber Risk Sigortası”, Genç Hukukçu Araştırmacılar Sempozyumu, 11-12 Ekim 2019, Oniki Levha Yayıncılık, Aralık 2020, 671-683, s.680.

toplum güvenliğini geliřtirmeyi amaçlayan bir kavramdır. Bu kapsamda herkes tarafından kolaylıkla yerine getirilebilecek güçlü řifre oluřturma, kimlik doęrulaması adımlarını atlamama, verileri yedekleme gibi yöntemler sayesinde günlük hayatta karřılıřılan çeřitli siber tehditlere karřı savunma mekanizmalarını güçlendirmiş ve güvenli bir dijital ortamın sürdürülebilirlięi saęlanmasında önemli adımlar atılmış olmaktadır. Siber hijyenin geliştirilmesi adına, farkındalık ve eğitimlerin arttırılması, temel saęlık eğitimleri gibi temel siber güvenlik eğitimlerinin yaygınlařtırılması atılabilecek başlıca adımlar arasındadır. ENISA tarafından yapılan kısa içerikli posterler ve videolar¹⁸⁸ ile toplum nezdinde siber hijyen arttırılmaya çalışılmaktadır. Siber güvenlik konusunda görevlendirilmiş pek çok idari otoritenin bulunduęu ülkemizde de toplum farkındalıęının arttırılması ve güvenli bir siber ortam oluřturulması adına bu nitelikteki kolay ama etkili çalışmaların yaygınlařtırılması gerekmektedir. Güvenlik anlayışının temel ilkelerinden olan en zayıf halka kadar güçlü olunabileceęi saikiyle okullarda bir kültür olarak siber hijyen kavramının geliştirilmesi pek çok basit hata nedeniyle uğranılabilecek zararın da üzerinden gelinmesine imkan saęlayacaktır.

Kurumsal düzeyde siber güvenlik anlayışının geliştirilmesi ve bu konuya özgülennmiş kurumların kurulması ile veri ihlallerine ve dięer dijital tehditlere karřı direnme, bu tehditlerden hızlıca toparlanma ve devam eden operasyonel süreçleri sürdürebilme yeteneęinin arttırılması anlamına gelen siber esneklik de bu alanda geliştirilmesi gereken dięer unsurlardır. Avrupa'da NIS İşbirlięi Grubu, Avrupa Kritik Altyapı Koruma Programı (EPCIP), Kritik Altyapı Koruması İçin Avrupa Referans Aęı (ERNICIP) gibi oluřumlar siber tehditlerin ele alınmasında ve kritik altyapıların korunmasında sınır ötesi işbirlięinin önemini örneklemektedir. Aę ve Bilgi Sistemlerinin Güvenlięine iliřkin AB Direktifi (NIS Direktifi) kapsamında kurulan NIS İşbirlięi Grubu, AB üye ülkelerinin bilgi alışveriřinde bulunmaları, en iyi uygulamaları paylařmaları ve siber olaylara

¹⁸⁸ ENISA, “Do's and Don'ts of cyber-hygiene”, link: <https://www.enisa.europa.eu/topics/cybersecurity-education/awareness-campaigns/boostyourcybervitals/media/dos-and-donts-of-cyber-hygiene>, (Son erişim tarihi: 22.06.2024)

müdahaleleri koordine etmeleri için bir platform görevi görmektedir. NIS İşbirliği Grubu, ulusal makamlar, düzenleyici kurumlar ve özel sektör paydaşları arasında işbirliğini teşvik ederek, siber güvenlik yönetimi ve dayanıklılık oluşturma çabalarına yönelik kolektif bir yaklaşımı desteklemektedir. Benzer şekilde EPCIP, ilgili paydaşlar arasında risk değerlendirmesi, risk yönetimi ve bilgi paylaşımını kolaylaştırarak Avrupa genelinde kritik altyapıların dayanıklılığını artırmaya odaklanmaktadır. EPCIP, sektöre özel eylem planları ve sektörler arası işbirliği mekanizmaları aracılığıyla enerji, ulaşım ve finans gibi kritik altyapı sektörlerindeki kırılganlıkları tespit etmeyi ve ele almayı amaçlamaktadır. Avrupa'daki deneyimler, siber tehditlerin etkin bir şekilde ele alınması ve kritik altyapıların korunması için Türkiye'de de benzer işbirliği çerçevelerinin ve mekanizmalarının oluşturulmasının önemini vurgulamaktadır. Hızla büyüyen dijital ekonomi ve bilgi teknolojilerine artan bağımlılığı olan bir ülke olarak Türkiye'de siber tehditlerle mücadele etmek ve aynı zamanda bu alanı geliştirebilmek için idari hiyerarşinin ve olağan kurumların dışında, dinamik, hızlı aksiyon alan ve konuya özgülenmiş kurumlara ihtiyacı bulunmaktadır¹⁸⁹. Tüm dünyada olduğu gibi Türkiye'de hem kamu hem de özel sektör paydaşları kapsamlı stratejileri geliştirilmesi ve ortak çaba ile etkileşim gerektiren benzersiz siber güvenlik zorluklarıyla karşı karşıyadır. Bu nitelikte zorlukların üstesinden gelinebilmesi, tıpkı siber saldırıların arkasında yer alan isimlerin yaptığı gibi sürekli bir iletişim ve kuvvetli bir destek mekanizması ile mümkün olabilir.

Güvenlik yaklaşımlarının ve buna bağlı geliştirilen güvenlik yönetimlerin saldırının etkileri ve amaçlarına bağlı olarak şekillendiği söylenebilir. İlkel anlamda da güvenlik ihtiyacı, günlük hayatın değişen ve gelişen koşullarına bağlı olarak şekillenmiştir. İlk insanların güvenlik ihtiyaçları doğadaki diğer canlılardan korunmak adına bir sığınak edinmek, saldırılara karşı korunmak ya da saldırıda bulunabilmek adına geliştirilen aletlerden silah üretmekken, yerleşik hayata geçilmesiyle birlikte diğer hayvanların saldırılarından haberdar olup korunabilmek adına hayvanların evcilleştirilmesi ve eğitilmesi, toplu yaşama

¹⁸⁹ Bıçakcı, 2014, s.128.

geçilmesiyle birlikte kuralların oluşturulması, şehirdeki düzeni ve devamlılığı sağlayabilmenin yanı sıra şehir dışından gelebilecek saldırılara karşı korunmak ve gerektiğinde savunup saldırabilmek için kalelerin inşa edilmesi, askeri birliklerin oluşturulması, silahların geliştirilmesi şeklinde uzayacak bir liste haline getirilebilir.

Bugünkü hayatımıza baktığımızda fiziksel güvenlik ihtiyacına hizmet eden pek çok yardımcı aracın yanında, artık fiziksel dünyayı doğrudan etkileyen ancak bambaşka bir yapı haline gelen siber uzayda meydana gelen pek çok olay ve korunması gereken pek çok faktör yer almaktadır. Tüm bankalardan, devlet kurumlarına, hastanelerden, taksilere, elektrik hizmetlerinden, uzay çalışmalarına kadar bir çırpıda akla gelebilecek her türlü hizmet, ürün ya da malın siber uzay ile bağlantısı bulunmaktadır. Dolayısıyla aslında fiziksel dünya, dijitale taşınmış durumdayken kritik öneme sahip şirketlerin ve bağlantılı olarak kamu güvenliğinin sağlanarak, bireylerin haklarının korunmasında mevcut yasalar ile yeterli korumanın sağlanması mümkün görünmemektedir.

Günlük hayatımız ve giderilmesine muhtaç durumda olduğumuz her türlü ihtiyacımızın aynı siber uzayı paylaşıyor olması da aslında getirdiği kolaylıkların yanında pek çok tehlike ile de burun buruna olduğumuz anlamına gelmektedir. Kurumların yahut kişilerin siber uzaydaki varlıkları kadar vakıf olabildikleri bu dijital dünyada erişimin saniyeler içinde gerçekleşebiliyor olması herhangi bir saldırı ihtimalinde ne denli hassas ve hızlı etkilenebilir bir konumda olduğumuzu göstermeye yeter ölçüdedir. Bu durumun ortaya çıkardığı tehlikelerin bertaraf edilmesi de yeni ve oldukça önemli bir hale gelen siber güvenlik ihtiyacını ortaya çıkarmıştır. Siber güvenlik adına da tüm bu alanların şekillenmesi ve gelişimi, geliştirilen devlet politikaları ile hukuk sistemlerinin de aynı güvenlik amacını yerine getirmek adına adımlar atması bir zorunluluk halini almıştır. Farklı kurumlar ve mevzuatlar eliyle, siber güvenliğe ilişkin farklı terminolojiler çalışarak bu hususta asgari bir güvenlik düzeyinin yakalanması mümkün olamayacağı gibi bu amacın gerçekleştirilmesi hilafına hukuki boşluklar yaratılması da ihtimal dahilindedir.

Siber uzayda bulunan tüm tarafları kapsayacak bir mevzuat ihtiyacının giderilmesi amacıyla yapılacak hazırlıklar esnasında, siber uzayda güvenliğin, etkin ve aynı zamanda sürdürülebilir bir şekilde sağlanması olduğu da her daim göz önünde bulundurulmalıdır. Güvenliğin sağlanması adına temel ve kabul edilebilir düzeyde bir yatırım yapılması herkes için gerekli kılınmalıysa da, yatırım yapılan alanın bilişim olduğu ve bu nedenle sürekli bir değişim ve gelişim yaşadığı da unutulmamalıdır. Bunun yanında saldırı yöntemleri konusundaki gelişim, zaman zaman teknolojiye ve her daim güvenlik araçlarından da ne yazık ki ileridedir ve ileriye gitmeye gayret etmektedir. Birkaç sene sonra gerek teknolojiye geline nokta gerekse de güvenlik anlayışı itibarıyla bir anlam ifade etmeyecek mevzuat yükümlülüklerine uyma gayreti büyük bir külfet olarak görülebilecek ve dolayısıyla siber güvenlik alanına ilişkin yatırım yapma konusundaki dirençle karşılaşılması ve sorumluluktan kurtulmak için alternatif ve korunaksız çözümlere yönelmesi ihtimaller arasına girecektir. Dolayısıyla hukuki sorumluluğun taraflarca kabul edilmesinde güçlükler yaşanması ve amacına hizmet etmemesi de muhtemeldir. Bunun yanında salt yükümlülük getiren ancak belirlenen yükümlülüklerin yerine getirilmemesi nedeniyle uğranılacak zararlardan doğacak sorumluluğun kime ve ne şekilde atfedilmesi gerektiğini belirlemeyen bir mevzuatta şüphesiz topluma bir fayda yaratmayacak külfetler silsilesinden ibaret görülebilir. Zira belirlenen siber güvenlik önlemlerinin alınmasını gerekçe göstererek tarafların uğradığı zararlar karşısında bir sorumluluk üstlenmeyen sistem ve kurumlara güven duyulması mümkün olmayacaktır. Bunun yanında tarafların korunması amacına hizmet etmesi beklenen hukukun da görevini tam olarak yerine getirmemiş olması neticesini doğacaktır. Hem esnek ve gelişen teknolojiye uyarlabilir nitelikte hem de etkin ve asgari düzeyde korumayı sağlayabilecek yetkinlikte bir kanuni düzenleme yapılması ihtiyaçlara da en doğru şekilde çözüm olacaktır.

SONUÇ

Elektrik hizmet olarak pek çok etkiye sahip ve modern toplumlar açısından herkesin ihtiyacı kabul edilebilecek nitelikte bir önemi haiz olduğundan, hizmetin devamlılığı da aynı ölçüde önem arz eder hale gelmiştir. Hizmette devamlılığın sağlanabilmesi adına alınması gereken pek çok önlemin arasında ve henüz çerçevesi belirlenmemiş olan bir diğer yükümlülük alanı ise artık siber güvenliğe ilişkindir. Siber uzay, hem uluslararası ilişkilerde korunmayı gerektirir bir yer iştigal etmekte hem de teknolojinin etkin bir şekilde kullanılarak verilen hizmetlerde kalitenin arttırılabilmesi adına içinde bulunulması zorunlu bir ortam olarak kabul edilmektedir. Bu yayılım, her türlü sektörde olduğu gibi elektrik piyasası açısından da geçerli görünmektedir. Ancak elektrik piyasası ve benzeri şekilde kritik altyapı olarak kabul edilen piyasaların ihtiyaç olarak önem dereceleri oldukça yukarıda olduğundan, zarar görme ve saldırıya uğrama oranları da aynı şekilde yukarıda olduğu ve saldırıya açık bir alanda bulunuyor oldukları anlamına gelmektedir. Bu netice, diğer piyasalardan daha hassas bir şekilde siber güvenlik araçlarıyla donanmalarını ve çok sayıda hukuki düzenlemenin farklı amaçlara hizmet ediyor olsalar dahi bir şekilde siber güvenliğe ilişkin önlemler getirmesini gerekli kılmıştır. Bu önlemler neticesinde elektrik piyasasında hizmetin devamı açısından siber güvenliğin sağlanmasının gerekliliği yerine getiriliyor olsa dahi yaşanabilecek herhangi bir saldırı neticesinde zarar gören insanların zararlarını ne şekilde tazmin edebilecekleri sorusunun cevabı mevcut hukuki araçlar ile hala tam olarak verilememektedir. Elektrik piyasası oyuncularının sektörel yükümlülüklerinin yanı sıra sektör bağımsız şekilde tarafları etkileyen idari otoriteler ve ikincil düzenlemeleri karşısında sahip oldukları sorumlulukların hukuki zararları tazmin edebilme açısından yetkinliği tartışma konusudur.

Jeff Kossef'in makalesinde işaret ettiği gibi neyi, nerede, kim tarafından, nasıl, ne zaman ve neden korunduğu yahut güvenliğinin sağlandığı sorularının yanıtları, tüm paydaşların uzlaşısı ve açıkta kimse kalmayacak şekilde yanıtlanmaksızın siber güvenliğin sağlandığından bahsetmek mümkün

olmayacaktır. Yalnızca belirli kurumlarda, sadece sınırlı bir alana yönelik ve ancak belirli koşulların varlığı halinde siber güvenlik sağlanması enstürümanlar belirlemiş mevcut mevzuatımız dijital dünyanın pek çok alanını başıboş bırakmış durumdadır. Dijitalleşmenin sağlıklı bir şekilde gelişimi için farklı ihtiyaçlara hitap eden ancak bununla birlikte dijital dünya gerçeğini reddemediği için bu alanda bulunan, dolayısıyla bir nevi fiziki dünyamızda getirilen kuralların işlevselliğini kaybettiği ve yapısal bir kontrolün de bulunmadığı siber uzayda başıboş şekilde hareket ederek aslında bireylere zarar veren kurumların karşısında güçlü, etkin ve dinamik birimler ile hukuki mekanizmaların inşa edilmesi şarttır. Özellikle siber güvenlik anlayışının bazı taraflarca oldukça ileri seviyelerde ve gelişmiş olduğu, bazı tarafların ise farkındalık seviyesinin henüz yeterli önlemleri almaları konusunda dahi eksik kaldığı bu asimetrinin bireylere zarar veren bir dengesizlik ve tehlike yaratacağı ortadadır. Bu dengesizliklerin de giderilmesi ve hukuki açıdan gerekli güvenliğin sağlanması adına genele hitap eder nitelikte bir siber güvenlik mevzuatı oluşturulması, bunun yanında salt siber güvenliğin korunması ile geliştirilmesi amacına hizmet eden otoritelerin oluşturulmasına ihtiyaç bulunmaktadır.

KAYNAKÇA

Avrupa Konseyi Bakanlar Komitesi. (2014). "Guide to Human Rights for Internet Users, Recommendation CM/Rec(2014)6 and explanatory memorandum". *"Guide to Human Rights for Internet Users"*.

Kişisel Verileri Koruma Kurulu. (2018, Ocak 31). ""Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" ile ilgili Kişisel Verileri Koruma Kurulunun 31/01/2018 Tarihli ve 2018/10 Sayılı Kararı". *"Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler Kararı"*. <https://www.kvkk.gov.tr/Icerik/4110/2018-10> adresinden alındı

Kişisel Verilerin Korunması Kurumu . (2023). "Genetik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber". <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/703442e0-690c-4618-91c3-83e7583170ca.pdf> adresinden alındı

(IAPP), U. G. (2019). "Avrupa Veri Koruması Hukuku ve Uygulaması". 2. baskı. (IAPP), Uluslararası Gizlilik Profesyonelleri Birliği.

(ITU), U. T. (2020). *"Global Cybersecurity Index 2020"*. International Telecommunication Union.

AB Komisyonu. (2004). "2004/702 Sayılı Rapor, "Critical Infrastructure Protection in the fight against terrorism".

AB Komisyonu. (2013, Şubat). "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace".

AB Komisyonu. (2013, Şubat). "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace" 2013/1.

AB Konseyi. (1992, Mart). 92/242/EEC Sayılı Karar, "in the field of security of information systems".

AB Konseyi. (2008). 2008/114/EC Sayılı Direktif, “on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection”.

AB Konseyi. (2016, Temmuz). 2016/1148 Sayılı Direktif, “concerning measures for a high common level of security of network and information systems across the Union”.

AB Konseyi ve Parlamentosu. (2004, Mart). 460/2004 Sayılı Tüzük, “establishing the European Network and Information Security Agency”.

AB Konseyi, S. S. (2019, Temmuz 8). “T-Cy Guidance Notes” . Strazburg, Fransa.

AB Parlamentosu ve AB Konseyi . (2019, Haziran). 2019/881 sayılı Regülasyon “on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)”.

Acarer, T. (2020). "Ülke Güvenliğimizde Alınabilecek Makro Siber Güvenlik Önlemleri". 6(2), 61-71. Uluslararası Bilgi Güvenliği Mühendisliği Dergisi.

Adams, M. J. (2017, Ocak 4). “A Warning About Tallinn 2.0 ... Whatever It Says”. The Lawfare Institute. Nisan 20, 2024 tarihinde <https://www.lawfaremedia.org/article/warning-about-tallinn-20-%E2%80%A6-whatever-it-says> adresinden alındı

Afet ve Acil Durum Yönetim Başkanlığı. (2014, Eylül). “2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi”.

Afet ve Acil Durum Yönetim Başkanlığı. (2014, Eylül). “2014-2023 Teknolojik Afetler Yol Haritası Belgesi”.

Afet ve Acil Durum Yönetimi Başkanlığı. (tarih yok). “Açıklamalı Afet Yönetimi Terimleri Sözlüğü”. Haziran 22, 2024 tarihinde

<https://www.afad.gov.tr/aciklamali-afet-yonetimi-terimleri-sozlugu>
adresinden alındı

Anubhav Ratha. (2013, Mart). "India's Blackouts of July 2012: What Happened and Why?". 5(4), 2-6. Ulusal Singapur Üniversitesi, Enerji Araştırmaları Enstitüsü.

Aslan, E. (2010). "Enerji Sektöründe İmtiyaz Sözleşmesi Çukurova-Kepez Örneği". *"Enerji Sektöründe İmtiyaz Sözleşmesi Çukurova-Kepez Örneği"*. Gazi Üniversitesi (Yüksek Lisans Tezi).

Aydın Aksakal, P. (2020). "İnsan Hakları Açısından Enerjiye Erişim Kavramı, Birleşmiş Milletler ve Bölgesel Düzenlemeler Açısından Enerjiye Erişim Kavramı". *"İnsan Hakları Açısından Enerjiye Erişim Kavramı, Birleşmiş Milletler ve Bölgesel Düzenlemeler Açısından Enerjiye Erişim Kavramı"*, 53. İstanbul: (Yüksek Lisans Tezi) İstanbul Bilgi Üniversitesi.

Bakkaloğlu, E. (2022, Mart). "Gerçek Banka veya Kredi Kartlarının Kötüye Kullanılması (TCK. 245/1)". 1. Baskı. Oniki Levha Yayıncılık.

Bıçakcı, S. (2014, Mart 4). "NATO'nun Gelişen Tehdit Algısı: 21.Yüzyılda Siber Güvenlik". 10(40), 100 - 130. Uluslararası İlişkiler Dergisi.

Cormier, R. (tarih yok). The 12 Biggest Blackouts In History. Nisan 16, 2024 tarihinde <https://www.mentalfloss.com/article/57769/12-biggest-electrical-blackouts-history> adresinden alındı

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi. (2020, Temmuz). "Bilgi ve İletişim Güvenliği Rehberi".

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi. (2021, Ekim). "Bilgi ve İletişim Güvenliği Denetim Rehberi".

Cybersecurity & Infrastructure Security. (2021, Temmuz 21). *"Cyber-Attack Against Ukrainian Critical Infrastructure"*. Ocak 1, 2023 tarihinde

www.cisa.gov: <https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01> adresinden alındı

Çelik, S. (2018). “Siber Uzay Ve Siber Güvenliğe Multidisipliner Bir Yaklaşım”. 110-119. Academic Review of Humanities and Social Sciences.

Çeliksa, B. (2016). “Siber Güvenlik Kavraminin Gelişimi Ve Türkiye Özelinde Bir Değerlendirme” . (Yüksek Lisans Tezi) Karadeniz Teknik Üniversitesi.

Çetintaş, H., & Bicil, İ. M. (2015). Elektrik Piyasalarında Yeniden Yapılanma ve Türkiye Elektrik Piyasasında Yapısal Dönüşüm, 2015. 2(2), 1-15. Optimum Ekonomi ve Yönetim Bilimleri Dergisi.

Doğru, C. (2010, Ocak). "Türkiye’de Elektrik Piyasasının Yeniden Yapılanması Sürecine Bir Bakış". *"Türkiye’de Elektrik Piyasasının Yeniden Yapılanması Sürecine Bir Bakış"*, 14. Sosyal Bilimler Metinleri.

Enerji Piyasaları Anonim Şirketi. (tarih yok). *"Esas Sözleşme"*. www.epias.com.tr:https://www.epias.com.tr/wp-content/uploads/2016/01/ek-1-1-epias-esas-sozlesme.pdf adresinden alındı

Enerji Piyasaları İşletme Anonim Şirketi. (2023, Şubat 14). “Faaliyet Raporu 2022” . Nisan 20, 2024 tarihinde <https://www.epias.com.tr/wp-content/uploads/2023/02/EPIAS-2022-Yili-Faaliyet-Raporu-2023.pdf> adresinden alındı

Enerji Piyasası Düzenleme Kurulu. (2003). "Elektrik Piyasasında Uygulama El Kitabı, 2003". Ankara.

ENISA. (tarih yok). “Do's and Don'ts of cyber-hygiene”. Nisan 20, 2024 tarihinde <https://www.enisa.europa.eu/topics/cybersecurity-education/awareness-campaigns/boostyourcybervitals/media/dos-and-donts-of-cyber-hygiene> adresinden alındı

ENISA. (2017). “ Overview of cybersecurity and related terminology”.

- ENISA. (2017, Temmuz). “ENISA overview of cybersecurity and related terminology”, Temmuz 2017.
- ENTSO-E. (2016, Ocak 15). "*Turkish grid operator, TEIAS, joins ENTSO-E as observer member*". www.entsoe.eu:
<https://www.entsoe.eu/news/2016/01/15/teias-member/> S adresinden alındı
- Erdem, K. M., & Erdem, D. (2017, Nisan). "Türkiye’de Elektrik Dağıtımının Özelleştirilmesinin Nedenleri ve Amaçlar Özelleştirmede Tedaş Örneği". *İstanbul Barosu Dergisi*.
- Ertılav, M., & Mehmet, A. (2015). "TEDAŞ (Türkiye Elektrik Dağıtım Anonim Şirketi) Özelleştirmesi". *Uluslararası Alanya İşletme Fakültesi Dergisi*, s. 96-98.
- Hasan Ayrancı. (2000). "*Enerji Sözleşmeleri*". Ankara: Yetkin.
- Hatipoğlu Aydın, D. (2022, Mart). “Siber Alan ve Hukuk”. İstanbul: On İki Levha Yayıncılık A. Ş.
- Hultquist, J. (2016, Ocak 7). “Sandworm Team And The Ukrainian Power Authority Attacks”. <https://www.mandiant.com/resources/blog/ukraine-and-sandworm-team> adresinden alındı
- Karagöz, M. C. (2020, Ekim). “Bilişim Sistemleri Teorisine Giriş İle Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu” . Oniki Levha Yayıncılık.
- Kır, A. (2010). “Kamu Hizmetinin Görülme Usullerinden Ruhsat Usulü Ve Elektrik Piyasası Örneği”. Kırıkkale Üniversitesi (Yüksek Lisans Tezi).
- Kişisel Verileri Koruma Kurumu. (2018, Nisan 6). "Kişisel Veri Güvenliği Rehberi". Nisan 24, 2024 tarihinde <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7512d0d4-f345-41cb-bc5b-8d5cf125e3a1.pdf> adresinden alındı

Kişisel Verileri Koruma Kurumu. (2021, Eylül 16). "Biyometrik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber". Nisan 20, 2024 tarihinde <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/bd06f5f4-e8cc-487e-abe1-d32dc18e2d7e.pdf> adresinden alındı

Kişisel Verileri Koruma Kurumu. (2023, Aralık 22). "Mobil Uygulamalarda Mahremiyetin Korunmasına Yönelik Tavsiyeler". Nisan 20, 2024 tarihinde <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/8ba209bb-fa93-4479-84f0-dd55aac97a0f.pdf> adresinden alındı

Kossef, J. (2018). "Defining Cybersecurity Law". *103(985)*, 985-1031. Iowa Law Review. Nisan 20, 2024 tarihinde alındı

Küzeci, E. (2019, Şubat). "Kişisel Verilerin Korunması", . 3. *Baskı*. Ankara: Turhan Kitapevi.

Meral, M. (2015). "Siber Güvenlik Kapsamında Kritik Altyapıların Korunmasının Önemi",. (Yüksek Lisans Tezi), Harp Akademileri Stratejik Araştırmalar Enstitüsü.

Mustafa Ünver, C. C. (2011, Nisan). "Kritik Altyapıların Korunması". *1. Basım*. Bilgi Teknolojileri Ve İletişim Kurumu.

Obama, B. (tarih yok). "Remarks by the President at the Cybersecurity and Consumer Protection Summit". The White House President Barack Obama . Nisan 20, 2024 tarihinde <https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit> adresinden alındı

Oğuz, M. (2021). "Stratejiden Yasaya Avrupa Birliği Siber Güvenlik Politikası". (Yüksek Lisans Tezi) Marmara Üniversitesi.

- Ottis, R. (2008, Ocak). “Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective”. Estonya/Talin: NATO Müşterek Siber Savunma Mükemmeliyet Merkezi (CCDCOE).
- Önok, M. (2013, Aralık 2013). “Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği”. *Prof. Dr. Nur Centel’e Armağan, Cilt: 19(Sayı: 2)*, 1229 - 1270. Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi.
- Özçelik, B. (2021, Şubat). “Bilişim Sistemine Girme Suçu”. *1. Baskı*. Oniki Levha Yayıncılık.
- Öztekin, A. M. (2020). “Elektrik Piyasasında Lisanslar Ve İdarenin Yetkileri” . Ankara Üniversitesi (Yüksek Lisans Tezi).
- Peleschuk, D. (2022, Kasım 18). *"Blackouts hit Ukraine's small businesses, and wider economy, hard"*. [www.reuters.com: https://www.reuters.com/world/europe/blackouts-hit-ukraines-small-businesses-wider-economy-hard-2022-11-18/](https://www.reuters.com/world/europe/blackouts-hit-ukraines-small-businesses-wider-economy-hard-2022-11-18/) adresinden alındı
- Penna Electric. (tarih yok). Top 5 Of The World’s Biggest Power Outages. Penna Electric. Nisan 16, 2024 tarihinde ink: <https://www.pennaelectric.com/top-5-of-the-worlds-biggest-power-outages/> adresinden alındı
- Pidd, H. (2012, Temmuz 31). "India blackouts leave 700 million without power". The Guardian. Nisan 16, 2024 tarihinde <https://www.theguardian.com/world/2012/jul/31/india-blackout-electricity-power-cuts> adresinden alındı
- Power Technology. (2015, Ocak 13). *"The 10 worst blackouts of the last 50 years"*. Ocak 3, 2023 tarihinde <https://www.power-technology.com/features/featurethe-10-worst-blackouts-in-the-last-50-years-4486990/?cf-view> adresinden alındı

Putra, D. S., Septia, S. T., & Sunaringtyas, U. (2022, Aralık). "The Use of ISO/IEC 27001 Family of Standards in Regulatory Requirements in Some Countries"

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2002). "Identifying, understanding, and analyzing critical infrastructure interdependencies". 11-25. IEEE Control Systems Magazine.

Sağıroğlu, Ş. (2018). "Siber Güvenlik Ve Savunma: Önem, Tanımlar, Unsurlar Ve Önlemler". *"Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık"*(22). Ankara: Grafiker Yayınları.

Sağıroğlu, Ş. (2018). "Siber Güvenlik Ve Savunma: Önem, Tanımlar, Unsurlar Ve Önlemler". *Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık, 1. Baskı*. (Ş. Sağıroğlu, & M. Alkan, Dü) Ankara: Grafiker Yayınları.

Samet Saygı. (2020). "6698 Sayılı Kanun'un Sistematiğinde Yargısal Başvuru Yolları". 2(2), 30-61.

Shuai, M., Chengzhi, W., Shiwen, Y., Hao, G., Jufang, Y., & Hui, H. (2018, 130. sayı). "Review on Economic Loss Assessment of Power Outages". *Procedia Computer Science*, s. 1158–1163.

Siddiqui, A. S., Ahmad, A., & Athar, A. (2015, Mart). "Economic Impact Of Power Outage on GDP of India". *International Journal of Engineering Technology, Management and Applied Sciences*, s. 150-162.

Stratejik ve Uluslararası Çalışmalar Merkezi(CSIS). (2024). "Significant Cyber Incidents Since 2006".

Stratejik ve Uluslararası Çalışmalar Merkezi, (. (2024). "Significant Cyber Incidents Since 2006". <https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024->

04/240418_Cyber_Events.pdf?VersionId=TlrSq2hBc9eZ0dxXgNfkeJpmn169IIOh adresinden alındı

Stycznski, J., & Beach-Westmoreland, N. (2016). *"When the Lights Went Out – A comprehensive review of the 2015 cyber on the Ukrainian critical infracstructure"*. Virginia: Booz Allen Hamilton.

TEİAŞ, & ENTSO-E. (2015, Eylül). "Report on Blackout in Turkey on 31st March 2015".

Tekin, U. (2020, Aralık). "Hukukî Açıdan Siber Risk Sigortası". *Genç Hukukçu Araştırmacılar Sempozyumu, 11-12 Ekim 2019*, 671-683. (M. E. Uğur Orhan, Dü.) Oniki Levha Yayıncılık.

The Economic Times Industry. (tarih yok). "Power outages have negative impact on Indian economy: Moody's". Nisan 16, 2024 tarihinde <https://economictimes.indiatimes.com/industry/energy/power/power-outages-have-negative-impact-on-indian-economy-moodys/articleshow/15328536.cms> adresinden alındı

TRT Haber. (tarih yok). "Başbakan'dan "elektrik kesintisi" açıklaması". <https://www.trthaber.com/haber/gundem/basbakandan-elektrik-kesintisi-aciklamasi-176150.html> adresinden alındı

TÜBİTAK. (tarih yok). "Endüstride Önemli İmza". Haziran 22, 2024 tarihinde <https://tubitak.gov.tr/tr/haber/endustride-onemli-imza> adresinden alındı

Türk Standartları Enstitüsü. (tarih yok). "Bilgi ve İletişim Güvenliği Rehberi Denetim Hizmeti Veren Firma Belgelendirilmesi". Haziran 22, 2024 tarihinde <https://www.tse.org.tr/bilisim-belgelendirme-hizmetleri/> adresinden alındı

Ulaştırma ve Altyapı Bakanlığı. (tarih yok). "Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023". Nisan 20, 2024 tarihinde

<https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusal-siber-guvenlik-stratejisi-ve-eylem-planlari-2020-2023.pdf> adresinden alındı

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı. (2013). “Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı”.

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı. (2016). “2016-2019 Ulusal Siber Güvenlik Stratejisi”.

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, H. (2014, Temmuz). "Kurumsal SOME Kurulum ve Yönetim Rehberi". Nisan 20, 2024 tarihinde https://dsy.usom.gov.tr/usom/19/02/190211090329_Kurumsal%20_SOME_Rehberi.pdf adresinden alındı

Uluslararası Akreditasyon Kurumu. (2022, Ağustos 9). "Transition Requirements For ISO/IEC 27001:2022 (ISO/IEC 27001:2022'ye Geçiş Şartları)". *"Transition Requirements For ISO/IEC 27001:2022 (ISO/IEC 27001:2022'ye Geçiş Şartları)"*.

Uluslararası Telekomünikasyon Birliği . (2008). “ITU-T X-Series Recommendations: Data Networks, Open System Communications And Security, Telecommunication security, Overview of cybersecurity”.

University of York. (tarih yok). *"Data: a Practical Guide, What is data?"*. Nisan 20, 2024 tarihinde <https://subjectguides.york.ac.uk/data/lore> adresinden alındı

Ünver, M., Canbay, C., & Özkan, H. B. (2011, Nisan). “Kritik Altyapıların Korunması”. Bilgi Teknolojileri ve İletişim Kurumu.

Venkatesh, A. K. (2022, Mart). "A Review Paper on Cyber Security, International Journal of Advanced Research in Science". *Communication and Technology (IJARSCT)*, s. 528-531.

Weifang, L., Yong, T., Huadong, S., Qiang, G., Hongguang, Z., & Bing, Z. (2011).
Blackout in Brazil Power Grid on February 4, 2011 and Inspirations for
Stable Operation of Power Grid. Automation of Electric Power Systems 1-
5.

