TÜRKİYE'DE SİBER GÜVENLİK: YASAL VE KURUMSAL ALTYAPI*

CYBER SECURITY IN TURKEY: LEGAL AND INSTITUTIONAL INFRASTRUCTURE

H. Alpay KARASOY**
Pelin BABAOĞLU***

ÖZET

Başlangıçta askeri faaliyetlerin bir ürünü olan ağ teknolojileri, Soğuk Savaş'ın sona ermesiyle birlikte 1990'lı yıllardan itibaren sivilleşmeye başlamıştır. Sonrasında bu alanı destekleyen ve geliştiren teknolojilerle birlikte ağ teknolojileri; geniş insan kitlelerinin ilgisini çeken, hayatlarını kolaylaştıracak, zamandan tasarruf ettirecek kolaylıklar sağlayan ancak büyük tehlikeleri de barındıran bir alan olarak doğmuştur. Böylelikle bu tehditlere karşı savunma mekanizmaları olarak siber güvenlik mekanizmaları doğmuştur. Bu çalışma kapsamında Türkiye'deki siber güvenlik çalışmaları mevzuat ve kurumsal yapılar bağlamında ele alınmıştır. Öncelikle bu alandaki çalışmalar ve hukuki boyutları değerlendirilmiş, ardından sorumlu kurumlar incelenmiştir. Yasal ve kurumsal altyapı üzerinden yapılacak çıkarımlarla öneriler geliştirilmiştir.

Anahtar Kelimeler: Dijitalleşme, siber güvenlik, teknoloji, siber savunma

* Araştırma Makalesi
Makale gönderim tarihi: 05.10.2021
Makale kabul tarihi: 24.11.2021

** Doç. Dr. Selçuk Üniversitesi, İİBF, SBKY
E-posta: alpaykarasoy@hotmail.com
ORCID: https://orcid.org/0000-0002-3813-2960

*** Öğr. Gör. Isparta Uygulamalı Bilimler Üniversitesi, Uzaktan Eğitim MYO
E-posta: pelinbabaoglu@isparta.edu.tr
ORCID: https://orcid.org/0000-0002-7542-1323

ABSTRACT

Network technologies, which were initially a product of military activities, have become civilian since the 1990s with the end of the Cold War. Together with the technologies that support and develop this field, network technologies have emerged that attract the attention of large masses of people, provide conveniences that will make their lives easier and save time, and excellent harbor dangers. Thus, cyber security mechanisms have emerged as defense mechanisms against these threats. Within the scope of this study, cyber security studies in Turkey are discussed in the context of the legislation and institutional structures. First, the studies in this field and their legal dimensions were evaluated, and then the responsible institutions were examined. Finally, suggestions have been developed with the inferences to be made from the legal and institutional infrastructure.

Keywords: *Digitalization, cyber security, technology, cyber defense*

GİRİŞ

18. yüzyıla damgasını vuran "Aydınlanma Hareketi" felsefi yaklaşımlarıyla eskinin geleneksel ve dogmatik düşünüş biçimini temellerinden sarsmıştır. Avrupa'da gelişen ve etkisini tüm dünyada hissettiren bu hareketin, deney ve gözleme atfettiği değer ile "bilginin otoritesi" teolojik metinler, kilise ve ruhban sınıfı olmaktan çıkmış akıl, deney ve gözlemin ta kendisi olmuştur.[1] Aydınlanma hareketiyle bilimsel gelişmelerin iş birliği ve bunların birbirlerine karşılıklı olarak ivme kazandırmasının en önemli meyvesinin, 19. yüzyılda gerçekleşen endüstri devrimi olduğunu söylemek mümkün olacaktır. Şunu da belirtmekte fayda vardır ki bir süreç olan aydınlanma hareketi, endüstri devriminin aynı zamanda bir sonucudur.[2] Endüstri devrimine kadar yaşanan teknolojik gelişmeler genel olarak dar bir alanda etki oluştururken endüstri devrimi, dünya çapında büyük kitlelerin hem ekonomisini hem de sosyal yaşantısını etkilemiştir.[3] Öyle ki kırsal kesimden kentlere büyük göçler yaşanmış kırsalla kent arasındaki çizgi belirginleşmiş, dünyanın "ekonomi lokomotifi" tarım olmaktan çıkıp devasa endüstri kuruluşları olmuştur. O halde bu döneme "Sanayi Çağı" demek ve yaşanan tüm bu gelişmelerin; akıl, deney ve gözleme dayanan bilgi aktarımının sonucu olarak insan hayatında sosyal, ekonomik ve kültürel devrimler olduğunu söylemek hiç de yanlış olmayacaktır. Ancak insanoğlunu doğrudan etkileyen bu çarpıcı değişim ve dönüşüm süreci durulmayacaktır. 20. yüzyılın ortalarına gelindiğinde dünya, endüstri devriminin de önemli etkisinin var olduğu bilinen iki büyük savaş geçirmiştir. Bu savaşların etkisiyle dünyanın merkezinde yer alan kadim denilebilecek devletler gücünü yitirmiş iki yeni ve büyük süper güç ortaya çıkmıştır: Amerika Birleşik Devletleri (ABD) ve Sovyet Sosyalist Cumhuriyetler Birliği (SSCB). Dünya, döneminin üst düzey teknolojisiyle donatılmış silahlarla gözle görülebilir, etkisi doğrudan hissedilebilen savaşları atlattıktan sonra meydana çıkan bu iki süper gücün birbirleriyle temasa geçmeden gerçekleştirdikleri olağanüstü silahlanma ve askeri modernizasyon yarışına şahit olmuştur. İşte bu yarış haline Soğuk Savaş adı verilmekte olup bu dönemde ortaya konulan teknolojiler özellikle de ağ teknolojileri, siber uzay alanının temellerini atmıştır.[4] Nihayet aydınlanma hareketinin

1 Yaşar Salihpaşaoğlu, *Din ve Devlet Arasında İktidar Mücadelesi: Avrupa Örneği,* Adalet Yayınevi, 4.Baskı, Ankara, 2018, s. 145-149.

2 Ayşe Usta, "Aydınlanma Düşüncesine Kısa Bir Bakış", *Kastamonu İletişim Araştırmaları Dergisi*, S. 1, s. 88, https://dergipark.org.tr/tr/download/article-file/1673364, Erişim Tarihi: 30.04.2021.

3 Raşit Şahin, "Sanayi Devrimi Osmanlı İmparatorluğu'nda Neden Başlamadı?", *Business, Economics and Management Research Journal – BEMAREJ*, C. 2, S. 1, s. 2, https://dergipark.org.tr/en/download/article-file/726651, Erişim Tarihi: 30.04.2021.

4 Ali Burak Darıcılı, "Türkiye'nin Siber Güvenlik Politikalarının Analizi: Türkiye'nin Potansiyel Siber Güvenlik Stratejisi", *TESAM Akademi Dergisi,* C. 6, S. 2, s. 11.

ilk temsilcilerinin dahi hayal edemeyeceği, bilgiyi tam anlamıyla orijininde tutan yeni bir çağın başladığı söylenebilecektir: Bilgi Çağı.[5] Siber tehditlerin hedefinde yukarıda da belirttiğimiz üzere bireylerden devletlere kadar tüm gerçek ve tüzel kişiler olduğundan siber güvenlik, bireylerin olduğu kadar diğer tüm tüzel kişilerin de gereksinimi olmuştur. Ayrıca gelişen yeni teknolojilerle ortaya çıkan veri meselesi de ayrı bir güvenlik başlığı halini almıştır.[6] Gartner Araştırma ve Danışmanlık şirketine göre; dünya siber güvenlik sektörü pazar hacmi, 2019 yılında artan saldırılara rağmen bir önceki yıla nazaran yüzde 2,4 büyüyerek 124 milyar dolara yükselmiştir.[7] Bilhassa devletler bu konuyu ulusal güvenlik açısından program ve politikalarına taşımıştır. Türkiye de 1990'lı yıllardan itibaren bu kapsamda program, eylem planı ve politikalar gerçekleştirmektedir. Bu yolda önemli adımlar atılmıştır.[8] Bu çalışma kapsamında siber güvenlik alanında atılan adımlar ve mevzuat düzenlemeleri odaklı bir şekilde Türkiye'nin güncel durumu incelenmiştir. Bu kapsamda öncelikle siber güvenliğe dair kavramlar ve alanın gelişimi incelenmiş, ardından düzenlemeler ve kurumsal yapılar ele alınmıştır.

1. SİBER GÜVENLİĞİN TARİHÇESİ VE BAZI TEMEL TANIMLAR

ABD Savunma Bakanlığı'nın girişimleri sonucunda kurulan Gelişmiş Savunma Araştırmaları Birimi ARPA'nın, 1969 yılında ortaya çıkardığı yeni iletişim sistemi olan internet teknolojisinin tüm dünyaya yayılmasından sonra meydana gelen veri iletişimine yönelik birtakım saldırılar, söz konusu sanal dünyanın güvenliğinin yani siber güvenliğin sağlanmasının uluslar açısından zorunlu olduğu sonucunu ortaya çıkarmıştır.[9] Siber güvenlik kavramını incelemeden önce bu kavramın üst çatısını oluşturan siber uzay ve alt kavramlarının uluslararası çevrelerce nasıl tanımlandığını ve Türkiye cephesinde de bu kavramın nasıl anlaşıldığını kavramak siber güvenliği anlama noktasında yerinde olacaktır.

5 Mustafa Ünver vd., "Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler", *ANKARA: BTK*, s. 1, https://www.academia.edu/24841538/Ulusal_Siber_G%C3%BCvenli%C4%9Fin_Sa%C4%9Flanmas%C4%B1, Erişim Tarihi: 30.04.2021.

6 Levent Memiş – Melikali Güç, "Akıllı Kentlerde Verinin Gizliliği ve Güvenliği: İlkeler ve Yaklaşımlar", *Güvenlik Bilimleri Dergisi, UGK Özel Sayısı*.

7 *Hürriyet*, Yerli Siber Güvenlik Şirketlerinin Küresel Arenadaki Durumu Nasıl?, https://www.hurriyet.com.tr/teknoloji/yerli-siber-guvenlik-sirketlerinin-kuresel-arenadaki-durumu-nasil-41250148, Erişim Tarihi: 24.04.2021.

8 Mustafa Afyonluoğlu, "Siber Güvenlik ve Kamu Politikaları", *Teknoloji ve Kamu Politikaları Kitabı*, 379-411, (Ed.: Mete Yıldız-Cenay Babaoğlu), Gazi Kitabevi, Ankara, 2020, s. 401., Darıcılı, "Türkiye'nin Siber ...", s.15, Hilal Başak Kılcı, "Türkiye'nin Siber Güvenlik Politikaları", *Cyberpolitik Journal*, C. 5, S. 9, s.2, http://cyberpolitikjournal.org/index.php/main/article/download/7/7/13, Erişim Tarihi: 27.04.2021.

9 Afyonluoğlu, "Siber Güvenlik…", s. 382-383.

1.1. Siber Uzay

Amerika Birleşik Devletleri Savunma Bakanlığı tarafından siber uzay ve kapsamı; bilgi teknolojilerinin altyapıları olan, internet, iletişim ağları, bilgisayar sistemleri, gömülü işlemci ve kontrol birimlerinden meydana gelen birbirine bağlı ağların oluşturduğu bilgi ortamındaki küresel alanı kapsar şeklinde tanımlanmıştır.[10] Siber uzay kavramının içine insanların da dâhil edildiği bir başka tanım ise NATO'ya aittir. Söz konusu tanımda siber uzay; ağ teknolojilerinin ürünü olan bir sayısal dünya olarak insan ve bilişim teknolojilerinin bir arada olduğu sanal dünya şeklinde açıklanmıştır.[11] Bünyesinde internetin de olduğu fakat yalnızca interneti kapsamayan bu olgunun[12] bilişim sistemleri, iletişim ağları ve bunun sonucunda ortaya çıkan insan ürünü bilgi ortamının tamamını kapsayan çatı bir kavram olarak ön plana çıktığı görülmektedir.

2020 yılında Ulaştırma ve Altyapı Bakanlığı koordinatörlüğünde Türkiye'nin son Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023) hazırlanmış, 29 Aralık 2020 tarihinde kamuoyuna sunulmuştur.[13] Türkiye Devleti ve siyasi iktidarının olaya bakış açısı hakkında önemli bilgiler sunan bu belgede siber uzay, Amerika Birleşik Devletleri Savunma Bakanlığının yaptığı tanımla paralel olarak; "doğrudan ya da dolaylı olarak internete, elektronik haberleşme ve bilgisayar ağlarına bağlı olan tüm sistem ve hizmetler" şeklinde tanımlanmıştır. Türkiye'nin aynı konuda bir önceki eylem planı olan 2013-2014 Eylem Planı'nda siber uzay kavramı yerine eş manada siber ortam kavramı kullanılmış olup siber ortam; "*tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan ortam*" olarak nitelendirilmiştir.[14] Her iki eylem planı da söz konusu kavrama aynı yerden bakmaktadır. NATO'nun siber uzay kavramının kapsamına insanı da dahil etmesi düşünüldüğünde ve bunun yerinde bir eklemleme olduğu ön kabulüyle Türkiye'nin hazırlamış olduğu eylem planlarında bu noktaya da eğilmesi gerekmektedir. Zira insan faktörü, günümüz dünyasında siber uzayın ayrılmaz bir parçası ve önemli bir etkileyicisidir.

---

10 Aşır Sertçelik, "Siber Olaylar Ekseninde Siber Güvenliği Anlamak", *Medeniyet Araştırmaları Dergisi*, C. 2, S. 3, s. 25, https://dergipark.org.tr/tr/pub/mad/issue/35779/443816, Erişim Tarihi: 08.05.2021.

11 *Siber Ortamla İlgili Kullanılan Kavramlar*, http://www.certbylab.com/blog/siber-kavramlar, Erişim Tarihi: 03.05.2021.

12 Sertçelik, "Siber Olaylar…", s.26.

13 *Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023*, https://hgm.uab.gov.tr//uploads/pages/siber-guvenlik/ulusal-siber-guvenlik-stratejisi-ep-2020-2023.pdf, Erişim Tarihi: 30.04.2021.

14 *Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı*, https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-plani-2013-2014-5a3412cf8f45a.pdf, Erişim Tarihi: 02.05.2021.

1.2. Kritik Altyapı

2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'nda kritik altyapı: "*İşlediği bilginin/verinin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılar*" şeklinde tanımlanmıştır. Avrupa Birliği Komisyonunun yaptığı tanımda kritik altyapı; herhangi bir aksama, zarar görme, yetersiz kalma yahut yok edilme durumunda, ülke bireylerinin sağlığını, emniyetini, sosyal fonksiyonlarını, ekonomi ve refahını önemli ölçüde etkileyebilecek sistem ya da bu sistemdeki ilgili parçalar şeklinde tanımlanmıştır.[15]

Kritik altyapı sektörleri Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nın 5. maddesine, aynı zamanda mülga Siber Güvenlik Kurulunun 20 Haziran 2013 tarihli 2 sayılı kararına göre şu şekilde listelenir;

- Kritik Kamu Hizmetleri
- Ulaştırma
- Enerji
- Bankacılık ve Finans
- Su Yönetimi
- Elektronik Haberleşme.[16]

Listede bulunan kritik altyapı sektörleri, yapı ve işleyişlerine göre farklı bilgi ve bilişim sistemlerini kullanmaktadır. Söz konusu kritik altyapı sistemlerinden bazıları Endüstriyel Kontrol Sistemleri (EKS) olan aynı zamanda kendi içerisinde SCADA *(Supervisory Control and Data Acquisition)* ve DCS *(Distributed Control System)* olarak ayrılan özel birtakım sistemlerle denetlenirken diğer bir kısmı ise verilerini genel bilindik izleme ve yönetme sistemleriyle denetlemektedir.[17]

15 Mustafa Ünver vd., "Kritik Altyapıların Korunması", Ankara, BTK, s. 3, https://www.academia.edu/24841891/Kritik_Altyap%C4%B1lar%C4%B1n_Korunmas%C4%B1, Erişim Tarihi: 15.05.2021..

16 *Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı*, https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-plani-2013-2014-5a3412cf8f45a.pdf, Erişim Tarihi: 02.05.2021.

17 *Kritik Altyapılarda Siber Güvenlik*, https://icsdefense.net/blog/kritik-altyapilarda-siber-guvenlik, Erişim Tarihi: 03.05.2021.

1.3. Siber Güvenlik İhlali ya da Siber Saldırı

Siber saldırı ya da bir diğer adıyla siber güvenlik ihlali, siber alan içerisinde bulunan kişi/kişiler ya da bilişim sistemleriyle, EKS yahut bilişim sistemleri tarafından yönetilen ve kontrol edilen verinin gizlilik, bütünlük ve erişilebilirliğini ortadan kaldırmaya yönelik girişimlerdir.[18] Amerika Birleşik Devletleri Ulusal Güvenlik Sistemleri Komitesi'nin 26 Nisan 2010 tarihinde yayımladığı yönergeye göre siber saldırı; *"bilgi sistemi kaynaklarını veya bilginin kendisini toplamaya, bozmaya, reddetmeye veya yok etmeye çalışan her türlü kötü amaçlı etkinlik"* şeklinde tanımlanmıştır. 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'nın siber saldırı hakkındaki yaptığı tanımda geçen gizlilik, erişilebilirlik ve bütünlük kavramları ise sırasıyla şu şekilde tanımlanabilir;

a) Gizlilik: Erişilebilirlik hususunda yetkisi bulunmayan mercii ya da şahıslar tarafından, söz konusu bilgilere/verilere; erişilememesi, kullanılamaması, depolanamaması, farklı bir ortama aktarılamaması veya bunların açığa çıkarılamamasını,

b) Erişilebilirlik: Yetki sahibi kişi ya da sistemlerin, talep edildiği anda bilgi/veriye erişebilmesini ve bu bilgi/verilerin yetkili kişiler tarafından kullanılabilirliğini ifade eder.[19]

c) Bütünlük: Bilgi ve bilişim sistemlerinin yalnızca yetki sahibi kişi ya da sistemler tarafından değiştirilebilmesidir.[20]

Siber alanda planlı ve koordineli bir şekilde gerçekleştirilen siber saldırılar kimi zaman belirli örgütsel yapılar tarafından gerçekleştirilirken kimi zaman da şahıslar tarafından bireysel olarak gerçekleştirilmektedir. DDoS adı verilen Dağınık servis dışı bırakma saldırıları gibi istisnai birtakım saldırılar haricinde genel olarak siber saldırılar, saldırının hedefinde bulunan sistemdeki güvenlik zafiyetinden ve sistem açıklarından faydalanılarak gerçekleştirilir.[21]

1.4. Siber Güvenlik

Uluslararası Telekomünikasyon Birliği'nin yaptığı tanımda siber güvenlik; kurum, kuruluş ya da kullanıcıların siber alandaki oluşumlarını muhafaza etme

18 *Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023*, https://hgm.uab.gov.tr//uploads/pages/siber-guvenlik/ulusal-siber-guvenlik-stratejisi-ep-2020-2023.pdf, Erişim Tarihi: 30.04.2021.

19 a.k.

20 Sertçelik, "Siber Olaylar…", s.26.

21 Salih Bıçakçı vd., Türkiye'de Siber Güvenlik, *EDAM Siber Güvenlik Kağıtları Serisi*, 25 Aralık 2015, S. 1, s.29.

amacıyla araç, politika, güvenlik kavramları ve teminatları, kılavuz, risk yönetimi yaklaşımları, faaliyet ve uygulamalarını içeren teknolojiler bütünü olarak ifade edilmektedir.[22] Siber güvenliğin bir başka tanımı ise Ulusal Siber Güvenlik Eğitim Girişimi (NICE) tarafından: "*bilgi ve iletişim sistemleri ile bu sistemlerin içerisinde yer alan bilgilerin herhangi bir zarara, saldırıya ya da yok edilmeye karşı korunduğu, savunulduğu bir faaliyet ya da süreç*" şeklinde tanımlanmıştır.

Siber alanı oluşturan bilgisayar ve bilişim sistemlerinde bulunan bilgilerin ya da verilerin; gizlilik, bütünlük ve erişilebilirlik hususlarında korumaya alınmasını, siber alanda karşılaşabilecek her türlü muhtemel siber olayların ve tehditlerin tespit edilmesini ifade eder. Bununla birlikte söz konusu tehditlere karşı koruma mekanizmalarının devreye sokulmasını ve bunun akabinde saldırının hedef alındığı sistemin önceki durumuna geri getirilmesini de kapsamında bulunduran etkinlikler bütünüdür.[23]

1.5. Siber Güvenliğin Tarihçesi

Siber güvenlik; 1969 yılında Amerika Birleşik Devletleri Savunma Bakanlığının bünyesinde Gelişmiş Savunma Araştırmaları Projeleri Birimi (ARPA) tarafından insanlar arasındaki iletişimi ve bilgi paylaşımını en kolaya indirme amaçlı olarak geliştirilen internet teknolojisinden sonra ortaya çıkan bir olgudur. Sovyetler Birliği'nin 1957 tarihinde Sputnik adlı uyduyu uzaya göndermesinin ardından, ABD hem Sovyetlerin bu hamlesinin geri planında kalmamak, hem de karşı cepheden gelebilecek saldırı ihtimallerini de göz önünde bulundurarak ARPA'yı kurmuştur.[24] Bu gelişmeden henüz bir yıl sonra ise uzay bilimleri araştırmaları NASA'ya bırakılmış, ARPA ise savunma amaçlı çalışmalardan ziyade araştırma çalışmalarına yoğunlaşmıştır.[25]

1962 yılında günümüz internetinin temeli olarak nitelenen Intergalactic Computer Network tanımı ARPA araştırmacılarından J. C. Robbnet Licklider tarafından yapılmıştır. Licklider'e göre Intergalactic Network ile dünyanın her yerinden dileyen herkesin yer ve zaman fark etmeksizin veri ve programlar aracılığıyla

22 Ünver vd., "Kritik Altyapıların ...", s.1-2.

23 *Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023*, https://hgm.uab.gov.tr//uploads/pages/siber-guvenlik/ulusal-siber-guvenlik-stratejisi-ep-2020-2023.pdf, Erişim Tarihi: 30.04.2021.

24 Mehmet Nesip Öğün - Adem KAYA, "Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler", *Güvenlik Stratejileri Dergisi*, C. 9, S. 18, s. 149, https://www.guvenliweb.org.tr/dosya/czNaM.pdf, Erişim Tarihi: 11.05.2021.

25 Bâkır Emre, "İnternet Güvenliğinin Tarihçesi", *BİLGEM Dergisi*, C. 3, S. 5, s. 8.

ortak bir alanda buluşabilmesi öngörülüyordu. Daha sonra ARPA içerisindeki bilişim sistemlerinin birbirine bağlanarak, projeler üzerinde araştırmacıların bir arada çalışması amacıyla ARPANET projesi gerçekleştirildi.[26] 1962 yılında temelleri atılan ve 1969 yılında ilk veri transferinin yapıldığı bu ilkel bilişim ve internet dünyasındaki kullanıcılar yalnızca; askeri kurumlar, devlet kurumları ve eğitim kurumlarından ibaretti. 1989 ve sonrasında Tim Berners Lee tarafından geliştirilen World-Wide Web (www) tarayıcısı ve http adındaki web sunucusu ile internet sivil kullanımın hizmetine açılmıştır.[27]

Çağımızda bilgi ve iletişim imkânlarının gelişim ve değişim büyük ivmeler kat etmesinin neticesinde insanlığa sunulan bu geniş hizmet gün geçtikçe yaygınlaşmaya başlamıştır. İnsanlık tarihinde yeni bir çağ başlatan bu teknolojik gelişmeler başta ülkeler olmak üzere bireyler için yaşamın kolaylaşması açısından önemli bir etken haline gelmiş, hayatın her alanına hızlı bir şekilde entegre olmuştur.[28] Teknolojik anlamda yaşanan bu gelişmelerle birlikte; bilimsel çalışmalar, iş dünyası, ekonomi, düşünsel etkinlikler, haberleşme ve hatta eğlence gibi günlük yaşama dair faaliyetler sanal dünyaya aktarılmaya başlanmıştır. Bunun yanı sıra dünyada özellikle kurum ve kuruluşlarda dijitalleşme sürecinde belge ve bilgiler dijital ortama aktarılmaya başlanmıştır.[29] Bu sayede devletler, kamu hizmetlerinde kaynak, iş gücü ve zaman konusunda büyük tasarruflar elde etmeye ve bürokrasinin işleyişi hakkında genel kabul gören hantallığı gidermeye çalışmıştır. Nitekim devletler ve bireyler açısından yaşamın ve teknolojiye erişimin kolaylaşmasının neticesinde özellikle insan hayatının fiziki ortamdan sanal ortama doğru evirilmesi suç unsurlarının da bu yönde değişip dönüşmesine sebep olmuştur. Zira tarih boyunca insanoğlunun karşı karşıya kaldığı suçlardan; sabotaj, hırsızlık, dolandırıcılık gibi yüz kızartıcı suçlar sanal âlemde de kendisini göstermeye başlamıştır.

Tarihteki siber saldırılara baktığımızda bu saldırıların, devletler ve toplumları için ne denli bir tahribata yol açtığını gözler önüne serecektir. Bu saldırılardan biri olan 2010 yılının haziran ayında İran'ın Nükleer Geliştirme Tesisi Natanz'a yapılan Stuxnet saldırısı, tesisteki işleyişi bozarak Uranyum zenginleştirme sürecini zayıflatmıştır. Belirlenen maddi kaybın 800 milyon dolar olduğu, aynı zamanda saldırının yapıldığı teknik bölümün ise büyük ölçüde zarara uğratıldığı belirtilmiştir.[30] 23 Aralık 2015 tarihinde ise Ukrayna'ya yönelik siber saldırı girişiminde

26 Emre, "İnternet Güvenliğinin…", s. 8.

27 Kılcı, "Türkiye'nin Siber…", s. 116.

28 Barış Çeliktaş, *Siber Güvenlik Kavramının Gelişimi Ve Türkiye Özelinde Bir Değerlendirme*, (Yayımlanmamış Doktora Tezi), Karadeniz Teknik Üniversitesi Sosyal Bilimler Enstitüsü, Trabzon, 2016, s. 1.

29 Ünver vd., "Kritik Altyapıların ...", s. 1.

30 *Kritik Altyapılarda Siber Güvenlik*, https://icsdefense.net/blog/kritik-altyapilarda-siber-

Stuxnet saldırısındaki gibi tek bir kurum hedef alınmamış, devletin birden fazla kurumuna saldırıda bulunulmuş bunun yanı sıra söz konusu bu saldırıda doğrudan toplum düzenini bozmaya yönelik girişimde bulunulmuştur. Yapılan hasar tespit çalışmalarına göre, saldırıdan yüz binleri aşkın insan etkilenmiş ve saldırı, bölgede yaklaşık altı saatlik bir elektrik kesintisine neden olmuştur.[31]

Siber saldırıların neden olabileceği tüm bu zararlar göz önünde bulundurulduğunda siber uzay; kara, deniz, hava ve uzaydan sonra güvenliğinin sağlanması devletler açısından elzem olan başka bir alan olarak karşımıza çıkmıştır.[32] Bu nedenle başta devletler olmak üzere özel kurum ve kuruluşlar bu suçların önüne geçmek amacıyla birtakım önlemler almaya başlamış ve bu önlemler sonucunda ortaya siber güvenlik adında yeni bir olgu ortaya çıkmıştır.

2. TÜRKİYE'NİN SİBER UZAY ALANIYLA İLGİLİ HUKUKİ DÜZENLEMELERİ VE KAMU POLİTİKASI ÇALIŞMALARI

1990'lı yıllardan itibaren sivilleşen ağ teknolojilerinin önüne geçilemez bir şekilde yaygınlaşması ülkeleri bu yeni durum için hukuksal ve politik altyapı çalışmaları yapmaya itmiştir. Ancak ülkelerin bu yeni duruma tepkisi ilk başta ulusal siber tehditler veya güvenlik anlamında olmamış suç işlenmesine karşı olarak ve toplumsal düzeni korumak amacıyla ceza hukuku kapsamında gerçekleşmiştir.[33] Aşağıda Türkiye'nin geçmişten günümüze siber uzay ve siber güvenlik konularında gerçekleştirmiş olduğu ya da gerçekleştirmeyi hedeflediği mevzuat ile uygulamaları kronolojik olarak kısaca ele alınacaktır.

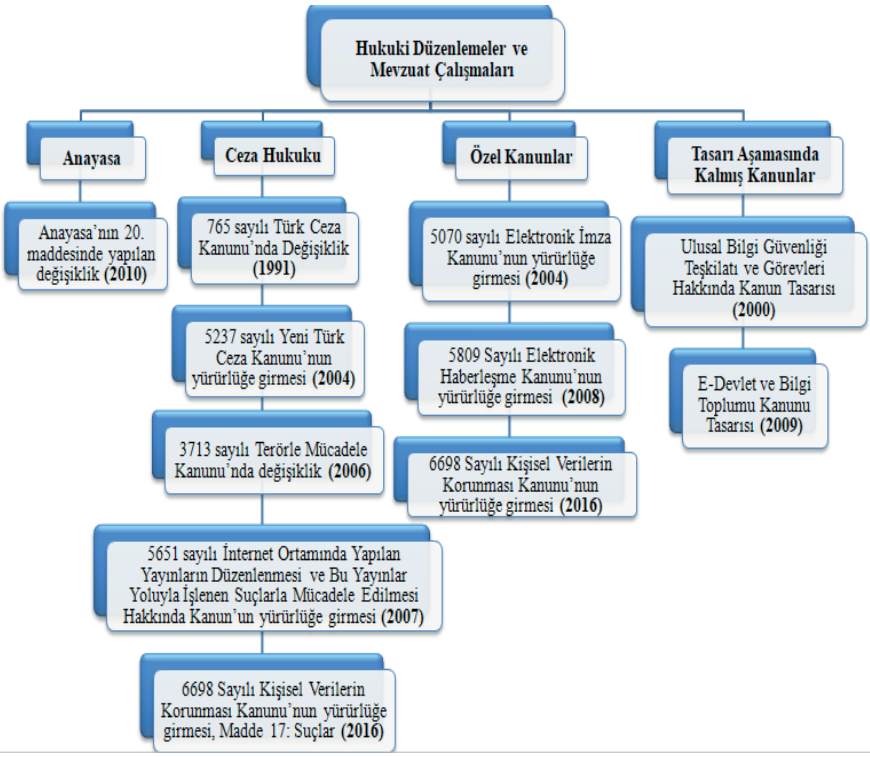
guvenlik, Erişim Tarihi: 03.05.2021.

31 a.k.

32 Afyonluoğlu, "Siber Güvenlik…", s. 383.

33 Bıçakçı vd., "Türkiye'de Siber…", s. 30.

Tablo 1: Hukuki Düzenlemeler ve Mevzuat Çalışmaları



2.1. Hukuki Düzenlemeler ve Mevzuat Çalışmaları

2.1.1. İlk Tepki: Mülga 765 Sayılı Türk Ceza Kanunu'na 1991 Yılında Bilişim Suçlarının Dâhil Edilmesi

Yukarıda da bahsedildiği üzere ağ teknolojilerinin sivilleşip yaygınlaşmasına Türkiye'nin ilk tepkisi ceza hukuku anlamında olmuş, kamu düzeninin ve asayişin bozulmaması için siber alanda gerçekleştirilebilecek hukuka aykırılıklara karşı cezai müeyyideler belirlenmiştir.[34] Türkiye'nin bu ilk tepkisinde kanun koyucunun olaya bakış açısı da dikkatle ele alınmalıdır. Zira söz konusu cezai müeyyidelerle korunmaya çalışılan hukuki değerler incelendiğinde görülecektir ki aslında Türkiye'de siber güvenlik anlamında çok erken bir dönemde farkındalık oluşmuştur.

Mülga 765 sayılı Türk Ceza Kanunu'nda 6 Haziran 1991 tarihinde yapılan değişiklikle Kanun'a *"Bilişim Suçları"* başlığı altında 11. bap eklenmiş 525a-525d

34 a.k., s. 30.

sayılı dört maddeyle suçlar ve cezaları düzenlenmiştir. Bu dört maddede korunan hukuki değerleri şu şekilde sıralamak mümkündür:[35]

- Özel hayatın gizliliği
- Mülkiyet hakkı
- Sırrın masuniyeti (dokunulmazlığı)
- Haberleşme hürriyeti
- Ekonomik menfaatler
- Kamunun bilişim sistemlerine güveni
- Bilişim teknolojileri üzerinden yapılacak ekonomik işlemlerde güvenilirlik

Korunan hukuki değerlerden özellikle, günümüzde Türkiye Cumhuriyeti Anayasası'nda da temel hak ve hürriyetler arasında düzenlenen; özel hayatın gizliliği, haberleşme hürriyeti ve mülkiyet hakkının, sivilleşen ağ teknolojilerinin potansiyel tehditlerine karşı bu erken dönemde korunması yukarıda da belirttiğimiz gibi kanun koyucunun bu konuda farkındalığı hakkında önemli ipuçları vermektedir. Üstelik kanun değişikliğinin gerçekleştiği 1991 yılında henüz normlar hiyerarşisinin en tepesindeki Anayasa'da haberleşme hürriyeti bulunmamaktadır. Ayrıca her ne kadar kanun değişikliğinin yasallaştığı tarihte Anayasa'da özel hayatın gizliliği hak ve hürriyetiyle ilgili madde bulunsa da çok sonraları bu maddeye doğrudan kişisel verilerin korunması hakkında fıkra eklenecektir. Böylelikle ceza hukuku kapsamında gerçekleştirilen bahsi geçen kanun çalışmasıyla kanun koyucunun, gününün ötesinde çıkarımlar yaptığı, tehditler tespit ettiği ve bu tehditlere yönelik tedbirler ortaya koyduğunu söylemek hiç de güç olmayacaktır.

2.1.2. Ulusal Bilgi Güvenliği Teşkilatı ve Görevleri Hakkında Kanun Tasarısı

1990'ların sonlarına gelindiğinde Türkiye'de Milli Savunma Bakanlığının koordinatörlüğünde Ulusal Bilgi Güvenliği Teşkilatı ve Görevleri Hakkında Kanun adında bir kanun çalışması yapılmıştır.[36] Yürürlüğe konulması düşünülen bu Kanun'da ulusal bilgi güvenliğinin sağlanması amacıyla Başbakanlığa bağlı bir üst kurul ve kamu tüzel kişiliğine sahip Ulusal Bilgi Güvenliği Kurumu Başkanlığı oluşturulması öngörülmüş, Üst Kurulun üyeleri ve çalışma şekli tespit edilmiş, ayrıca Başkanlığın görevleri ve teşkilatlanması düzenlenmiştir.[37] Nihayetinde Ka-

35 Umut Eker, "Türk Ceza Hukuku'nda Bilişim Suçları" Eski TCK Bağlamında Hukukumuzda Yer Alan İlk Düzenlemeler ve 5237 Sayılı Yeni Türk Ceza Kanunu'nun İlgili Hükümlerinin Yorumu", *Türkiye Barolar Birliği Dergisi*, S. 62, s. 111-116.

36 Bıçakçı vd., "Türkiye'de Siber…", s. 31-32.

37 *Ulusal Bilgi Güvenliği Teşkilatı ve Görevleri Hakkında Kanun Tasarısı*, https://www.

nun'un yürürlüğe konulması hususunda uzlaşma sağlanamamış ve Kanun tasarı aşamasında kalmıştır.

2.1.3. 5070 Sayılı Elektronik İmza Kanunu'nun Yürürlüğe Girmesi

2004 yılının Ocak ayında Türkiye Büyük Millet Meclisinde kabul edilip yine Ocak ayında Resmi Gazete'de yayımlanarak yürürlüğe giren 5070 sayılı Elektronik İmza Kanunu'nun amacına dair ilk maddesi "bu Kanunun amacı, elektronik imzanın hukukî ve teknik yönleri ile kullanımına ilişkin esasları düzenlemektir." ifadesi yer almaktadır.[38] Ayrıca bu Kanun'da, *imza oluşturma verilerinin izinsiz kullanımı* ve *elektronik sertifikalarda sahtekarlık* başlıkları altında cezai müeyyideler belirlenmiştir.

2.1.4. 5237 Sayılı Yeni Türk Ceza Kanunu'nun Yürürlüğe Girmesi

Demokratik hukuk devletin yaraşır bir şekilde Anayasa'da belirtilen temel hak ve hürriyetleri korumayı amaçlayan ayrıca kişinin güvenli bir toplumda yaşama hakkını sağlamayı hedefleyen yeni Türk Ceza Kanunu[39], 2004 yılında Türkiye Büyük Millet Meclisinde kabul edilerek aynı yıl yürürlüğe girmiştir. 5237 sayılı Türk Ceza Kanunu'nda kanun koyucu, kişilerin Anayasa tarafından korunan hak ve hürriyetlerini korumayı amaçlarken çağının bir gereği olarak siber alandaki özgürlükleri de ihmal etmemiştir. Bir önceki Kanun'da yer alan başlık aynen kullanılarak Kanun'un 243 ve 246. maddelerinde bilişim suçu oluşturacak fiiller ve bunlara uygulanacak cezai müeyyideler belirlenmiştir. Ayrıca bir önceki Kanun'dan farklı olarak söz konusu fiillerle tüzel kişilere haksız menfaat sağlanması durumunda tüzel kişilere özgü güvenlik tedbirlerinin uygulanacağı hüküm altına alınmıştır.[40]

2.1.5. 3713 Sayılı Terörle Mücadele Kanunu'nda Yapılan Değişiklik

Türk Ceza Kanunu'nda yukarıda bahsi geçen bilişim suçları 2006 yılında Terörle Mücadele Kanunu'nda yapılan değişiklikle *"terör amacı ile işlenen suçlar"*

---

tbd.org.tr/ulusal-bilgi-guvenligi-teskilati-ve-gorevleri-hakkinda-kanun-tasarisi/, Erişim Tarihi: 03.05.2021.

38 *5070 Sayılı Elektronik İmza Kanunu*, https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5070&MevzuatTur=1&MevzuatTertip=5, Erişim Tarihi: 04.05.2021.

39 *5237 Sayılı Türk Ceza Kanunu*, https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5237&MevzuatTur=1&MevzuatTertip=5, Erişim Tarihi: 04.05.2021.

40 *5237 Sayılı Türk Ceza Kanunu*, md. 246, https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5237&MevzuatTur=1&MevzuatTertip=5, Erişim Tarihi: 04.05.2021.

kapsamına alınmıştır.[41] Değişik maddeye göre, Türk Ceza Kanunu'nun 243 ve 244. maddelerinde yer alan fiiller, bir terör örgütünün faaliyeti çerçevesinde gerçekleştirildiği takdirde terör suçu sayılacaktır.[42] Böylelikle, Türkiye'de siber uzayın ilk kez terörizmin faaliyet sahası olabileceği kanun koyucu tarafından kabul edilmiştir.

2.1.6. 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un Yürürlüğe Girmesi

İçerik, yer, erişim ve toplu kullanım sağlayıcılarının uyması gereken kuralları ve bunların sağladığı internet ortamında işlenebilecek suçlarla mücadeleyi düzenleyen 5651 sayılı Kanun, Mayıs 2007 tarihinde yasama meclisi tarafından kabul edilmiş, aynı ay Resmi Gazete'de yayımlanarak yürürlüğe girmiştir.[43] Kanun incelendiğinde, internet ortamında gerçek ve tüzel kişilerin kişisel ya da ekonomik haklarını ihlal edecek içeriklere erişim engeli getirilebilmesinin, hakim kararına bağlandığı görülecektir. Bu sayede kişilerin özel hayatının gizliliğinin yanı sıra mülkiyet hakkı ve haberleşme hürriyetine yönelik yakın tehditlerin hızlıca önlenmesi ve gerçekleşen saldırıların etkisinin giderilmesi amaçlanmıştır. Aynı zamanda içeriklere getirilecek erişim engelinin yargı mercii kararına bağlanması da yine haberleşme hürriyetine devlet otoritesi tarafından getirilecek keyfi kısıtlamaları engelleyecek bir tedbir olarak karşımıza çıkmaktadır. Ayrıca son zamanlarda Türkiye'de gündemi bir hayli meşgul eden ve yabancı kaynaklı olarak nitelendirilen sosyal ağ sağlayıcılarının Türkiye'de temsilci bulundurmasını düzenleyen Kanun hükmü de bu Kanun'da yer almaktadır.[44]

2.1.7. 5809 Sayılı Elektronik Haberleşme Kanunu'nun Yürürlüğe Girmesi

Türkiye'de siber alanı ilgilendiren bir başka kanun olan 5809 sayılı Elektronik Haberleşme Kanunu, 2008 yılında Türkiye Büyük Millet Meclisi tarafından kabul

41 Bıçakçı vd., "Türkiye'de Siber…", s. 30-31.

42 *3713 Sayılı Terörle Mücadele Kanunu,* https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=3713&MevzuatTur=1&MevzuatTertip=5, Erişim Tarihi: 04.05.2021.

43 *5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun.* https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5651&MevzuatTur=1&MevzuatTertip=5, Erişim Tarihi: 05.05.2021.

44 *5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun,* ek md. 4, https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5651&MevzuatTur=1&MevzuatTertip=5, Erişim Tarihi: 05.05.2021.

edilip Kasım 2008'de Resmi Gazete'de yayımlanmıştır. Elektronik Haberleşme Kanunu'nun amacı, Kanun'un 1. maddesinde şu şekilde ifade edilmiştir:[45]

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.

Kanun, ağırlıklı olarak elektronik haberleşme sektörünü geliştirmeye ve yaygınlaştırmaya odaklansa da 2014 ve 2016 yıllarında Kanun'a eklenen hükümlerle Ulaştırma ve Altyapı Bakanlığı ile Bilgi Teknolojileri ve İletişim Kurumu'na (BTK) ulusal siber güvenlik konusunda görev ve yetkiler verilmiştir.[46] Aşağıda söz konusu kurumların siber güvenlikle ilgili yapılanmaları, görev ve yetkileri irdeleneceği için bu hükümlere burada yer verilmemiştir.

2.1.8. E-Devlet ve Bilgi Toplumu Kanunu Tasarısı

2009 yılında kabulü için yasama meclisine sunulan e-Devlet ve Bilgi Toplumu Kanun tasarısıyla hükümet, Türkiye'de, e-Devlet üzerinden vatandaşlara sunulacak hizmetlerin denetimini geçekleştirmeyi, Bilgi Toplumu Ajansı adında bir üst kuruluş kurmayı ve görevlerini belirlemeyi hedeflemiştir.[47] Kanun tasarısında e-Devlet yapılanmasının sağlıklı ve vatandaş lehine çözümler sunacak bir şekilde oluşturulmasının yanı sıra Bilgi Toplumu Ajansı'nı kurmakla da bu yöndeki politikaların kurumsal bir kimliğe bürünmesinin amaçlandığı görülmektedir.[48] Ancak söz konusu yasa çalışmasında;

- Ağırlıklı olarak ekonomik hükümlere yer verilmesi,
- e-Devlet hizmetlerinin yürütüleceği bilişim altyapılarının nasıl korunacağına dair muğlak ifadelerin yer alması ve altyapıları koruma görevinin bunları kullanan kuruma verilmesi,
- Bilgi Toplumu Ajansı'nın hem denetim hem de icra mercii olarak belirlenmesi

gibi unsurlar bahsi geçen amacın gerçekleşmesi yolunda eksiklik olarak gö-

45 *5809 Sayılı Elektronik Haberleşme Kanunu,* https://www.mevzuat.gov.tr/mevzuat?MevzuaNo=5809&MevzuatTur=1&MevzuatTertip=5, Erişim Tarihi: 05.05.2021.

46 a.k.

47 Bıçakçı vd., "Türkiye'de Siber…", s. 31.

48 *E-Devlet ve Bilgi Toplumu Kanunu Tasarısı*, https://www.memurlar.net/haber/146427/e-devlet-ve-bilgi-toplumu-kanun-tasarisi.html, Erişim Tarihi: 02.05.2021.

rülmektedir. Nihayetinde eksikliklerine rağmen e-Devlet politikalarının kurumsallaşması yolunda ilk çalışma olan e-Devlet ve Bilgi Toplumu Kanunu Tasarısı yürürlüğe girmemiş ve tasarı aşamasında kalmıştır.

2.2. Siber Güvenlik Eylem Planları

Türkiye, 1990'lı yılların başında siber uzay alanındaki tehditlere karşı ilk tepkisini ceza hukuku alanında vermiş ancak 1990'lı yılların sonlarına gelindiğinde bu meselenin artık ulusal güvenlik meselesi haline geldiğinin farkına varılmıştır.[49] Bu nedenle ulusal güvenliği sağlayacak tedbirler alınmaya başlanmış bu yönde çalışmalara başlanmıştır. İşte bu bölümde Türkiye'nin günümüze kadar ortaya koyduğu kamu politikaları çalışmalarına kronolojik olarak değinilecek ve söz konusu çalışmaların getirileri irdelenecektir.

Tablo 2: Çalışmaların Kronolojik Sıralaması

1999	• Türkiye Ulusal Enformasyon Altyapısı Anaplanı (TUENA)
2002	• E-Türkiye Girişimi Eylem Planı
2003	• 2003-2004 Kısa Dönem Eylem Planı
2005	• 2005 Kısa Dönem Eylem Planı
2006	• 2006-2010 Bilgi Toplumu Stratejisi Eylem Planı
2013	• Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı
2015	• 2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı
2016	• 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı
2020	• 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı

2.2.1. Türkiye Ulusal Enformasyon Altyapısı Anaplanı (TUENA)

Esasen temelleri 1995 yılında atılan bu çalışma, mülga Ulaştırma Bakanlığının koordinatörlüğünde gerçekleştirilen ve Türkiye Bilimsel ve Teknolojik Araştırma Kurumunun (TÜBİTAK) sekretarya hizmetlerini yaptığı bir çalışmadır.[50] Kamu kurumlarının yanı sıra özel kuruluşlar, dernekler ve akademik çevrenin katılımıyla gerçekleştirilen bu çalışmada;

49 Afyonluoğlu, "Siber Güvenlik…".

50 *Türkiye Ulusal Enformasyon Altyapısı Anaplanı: Sonuç Raporu*, http://www.bilgitoplumu.gov.tr/Documents/1/Yayinlar/991000_TuenaRapor.pdf, Erişim Tarihi: 10.05.2021.

- Türkiye'nin sadece internet değil, tüm bilişim teknolojilerindeki altyapı yeterliliği irdelenmiş,
- Başka ülkelerin eylem planlarıyla kıyaslamalar yapılarak bilişim teknolojilerindeki ekonomik fırsatlar araştırılıp bunlara yönelik öneriler geliştirilmiş ve
- Kanaatimizce en önemli sonuç olarak, siber güvenlik alanındaki tehditlerin ulusal güvenlik açısından son derece önem arz ettiği tespit edilerek bu tehditlere karşı oluşturulabilecek savunma mekanizmaları geliştirme yönünde eyleme geçme sonucuna varılmıştır.

Çalışmanın sonucunda elde edilen çıktılara bakıldığında bu gibi stratejik çalışmaların, farklı alanlardan paydaşlarla koordineli bir şekilde gerçekleştirilmesi gerektiğinin önemi anlaşılmaktadır. Keza siber alandaki durdurulamayacak gelişmeler ve bunun sonucu olarak oluşan tehditler karşısında topyekun tedbirler alınarak çağa ayak uydurulması önerisi çalışmanın da çıktılarından biridir.

2.2.2. E-Türkiye Girişimi Eylem Planı

Kamu politikası çalışmalarında tetikleyici çalışma TUENA olsa da 2000'li yılların başından günümüze değin ortaya koyulan eylem planlarının öncüsü olan e-Türkiye Girişimi Eylem Planı, Başbakanlık genel koordinatörlüğünde 2002 yılında hazırlanmış, aynı yıl ağustos ayında yayımlanmıştır.[51] Bu çalışmada Türkiye'nin gerek kamu hizmetleri anlamında gerekse sivil alanda *"e-dönüşüm"*ünün gerçekleştirilebilmesi için temel yapı taşları olarak teknik ve hukuki altyapılar belirlenmiştir. Temel yapı taşları üzerine hedefler ortaya koyulduktan sonra eğitimden sağlığa, ulaşımdan arşivlemeye, ticaretten çevreye kadar birçok alanda e-dönüşümün sağlanması yönünde hedefler ortaya konulmuştur. Çalışmanın asıl önemi kendisinden sonra oluşturulacak eylem planı ve stratejik belgelere öncülük etmesidir.

2.2.3. 2003-2004 ve 2005 Kısa Dönem Eylem Planları

İnternet kullanımının yaygınlaşması, Türkiye'nin e-dönüşüm sürecini süratle gerçekleştirmesi ve ağ teknolojilerinin güvenliğinin sağlanması amacıyla hazırlanan 2003-2004 Kısa Dönem Eylem Planı (KDEP), bir Başbakanlık Genelgesiyle Aralık 2003 tarihinde Resmi Gazete'de yayımlanmıştır.[52] Yukarıda değinilen bir önceki eylem planı gibi bu eylem planında da birçok farklı alanda hedefler ko-

51 *E-Türkiye Girişimi Eylem Planı*, http://www.bilgitoplumu.gov.tr/Documents/1/Yayinlar/020800_E-TurkiyeEylemPlani.pdf, Erişim Tarihi: 11.05.2021.

52 Afyonluoğlu, "Siber Güvenlik…", s. 387.

yulmuştur. Ayrıca bu çalışmanın eksenlerinden biri olan Teknik Altyapı ve Bilgi Güvenliği ekseni altında yer alan "ağ güvenliğin test edilmesi ve sağlanmasına ilişkin pilot uygulamaların geliştirilmesi" başlıklı 6 numaralı eylem planıyla TUBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü'ne (UEAKE) görev verilmiştir.[53]

2005 yılında tamamlanan bu eylem planının sonuç raporu Mart 2005'te kamuoyuyla paylaşılmıştır. Rapora göre hedeflenen politikalardan %47'si tamamlanmıştır.[54] Tamamlananlar arasında TÜBİTAK-UEKAE'ye verilen görev de bulunmakta olup, UEKAE, kendisine verilen bu görev kapsamında RTÜK bilişim sistemlerindeki riskleri raporlamış, sonrasında bu sistemlerdeki güvenlikleri sıkılaştırmıştır.[55]

2003-2004 KDEP'nin devamında gelen 2005 KDEP'de de yine TÜBİTAK-UEKAE'ye aynı görev verilmiş bu defa UEKAE, kritik ağlar üzerinde işlem yaptığı varsayılan 7 farklı kuruluşun güvenlik risk raporunu hazırlamıştır.[56] Bu raporda söz konusu kuruluşların her birinin farklı güvenlik seviyesinde olduğu, siber güvenlik anlamında oturmuş bir standartlarının bulunmadığı, bu alanda danışmanlık hizmeti veren özel kuruluşların yönlendirmelerine açık olduğu tespit edilmiştir.[57] Sadece 7 kuruluş baz alınarak hazırlanan rapordan da anlaşılacağı üzere Türkiye'nin o dönem katetmesi gereken uzun bir yolunun olduğu anlaşılmaktadır.

2.2.4. 2006-2010 Bilgi Toplumu Stratejisi Eylem Planı

Mülga Devlet Planlama Teşkilatı öncülüğünde, önceki belgelere göre daha uzun bir dönemi kapsayan 2006-2010 Bilgi Toplumu Stratejisi Eylem Planı hazırlanmış, 28 Temmuz 2006 günü Resmi Gazete'de yayımlanmıştır.[58] Detaylı bir çalışmanın ürünü olan bu belge, önceki eylem planlarına göre çok daha kapsamlı olmasının yanı sıra hedeflenen politikaların maliyetlerini de öngörmesi ve ayrıntılı olarak düzenlemesi yönünden dikkat çekicidir. Siber güvenliği, ulusal bir so-

53 *e-Dönüşüm Türkiye Projesi Kısa Dönem Eylem Planı*, http://www.bilgitoplumu.gov.tr/wp-content/uploads/2015/02/050000_E-DonusunTurkiyeKDEP.doc, Erişim Tarihi: 12.05.2021.

54 e-Dönüşüm Türkiye Projesi Kısa Dönem Eylem Planı: Sonuç Raporu, http://bilgitoplumu.gov.tr/Documents/1/KDEP/050500_KDEPSonucaporu.pdf, Erişim Tarihi: 12.05.2021.

55 Afyonluoğlu, "Siber Güvenlik…", s. 387.

56 a.k., s 387.

57 Mert Üneri, "e-Dönüşüm Türkiye Bilgi Güvenliği Projeleri", http://bilgitoplumu.gov.tr/Documents/1/Icra_Kurulu/070123_IK20.ToplantisiUEKAEBilgiGuvenligiSunusu.pdf, Erişim Tarihi: 12.05.2021.

58 Ünver vd., "Kritik Altyapıların…", s. 48.

run olarak ele alan eylem planında bu alanda hedeflenen politikalara, *"IV. Kamu Yönetiminin Modernizasyonu"* başlığı altında 87 ve 88 numaralı eylemlerle yer verilmiştir.[59]

Ülke güvenliği için önem arz eden bilgilerin siber alanda korunabilmesi ve yine devletin bilgi güvenliği sistemlerinin geliştirilmesi için hukuki altyapının oluşturulması, ayrıca Kişisel Verilerin Korunması Hakkında Kanun Tasarısının yasalaşması 87 numaralı eylemin hedefleridir. 88 numaralı eylemde ise bir nevi hava savunma sistemi gibi siber alandaki tehditlere karşı her an tetikte bulunacak, tehdit algıladığında uyarılarda bulunacak ve bu tehditlerle mücadeleyi koordine edebilecek bir kuruluş oluşturulması öngörülmüştür. "*Bilgisayar Olaylarına Acil Müdahale Merkezi (CERT)"* adı verilen kuruluşun oluşturulmasından TÜBİTAK sorumlu tutulmuştur.[60] Ayrıca yine 88 numaralı eylemde, KDEP-2005 gereği TÜBİTAK-UEKAE tarafından 7 kuruluş incelenerek hazırlanan raporun yukarıda da yer verilen sonucu dikkate alınarak şu hedefe yer verilmiştir:

Kamu kurumları için gerekli minimum güvenlik seviyeleri kurum ve yapılan işlem bazında tanımlanacak, kurumlar tarafından kullanılan sistem, yazılım ve ağların güvenlik seviyeleri tespit edilecek ve eksikliklerin giderilmesi yönünde öneriler oluşturulacaktır.

Sonuç olarak 87 numaralı eylem kapsamında Kişisel Verilerin Korunması Kanunu ile Ulusal Bilgi Güvenliği Kanunu tasarıları Adalet Bakanlığı tarafından hazırlanmış ancak yasalaşmamıştır.[61] Hukuki altyapı oluşturulmasını öngören bu eylemin, o dönemdeki en önemli getirisi, yukarıda da ayrıntılı olarak yer verilen 2010 yılı Anayasa değişikliği olarak karşımıza çıkmaktadır.

88 numaralı eylemin sonuçlarına baktığımızda ise bir önceki eyleme oranla daha yüksek bir başarı elde edildiği görülecektir. Zira siber alandaki tehditlerle mücadeleyi koordine etmek amacıyla kurulması hedeflenen kuruluş, TÜBİTAK-UEKAE bünyesinde Türkiye Bilgisayar Olaylarına Acil Müdahale Ekibi (TR-BOME) koordinatörlüğü olarak hayata geçirilmiştir. Ayrıca, kurumlar nezdinde de BOME'ler kurulmuş, ulusal çapta siber güvenlik tatbikatları gerçekleştirilmiş, yine aralarında Başbakanlık, Adalet Bakanlığı gibi kurumların bulunduğu kurum ve kuruluşlarda risk analizi çalışmaları yapılmıştır. Eylem, kendisinden

59 *Bilgi Toplumu Stratejisi Eylem Planı: 2006-2010*, http://www.bilgitoplumu.gov.tr/wp-content/uploads/2014/04/Bilgi_Toplumu_Strateji_Eylem_Plani_2006-2010.pdf, Erişim Tarihi: 15.05.2021.

60 a.k.

61 *2006-2010 Bilgi Toplumu Stratejisi Eylem Planı: Nihai Değerlendirme Raporu,* http://www.bilgitoplumu.gov.tr/Documents/1/Diger/bts_ve_eylem_planı_nıhaı_degerlendırme_raporu.pdf, Erişim Tarihi: 15.08.2021.

sonraki çalışmaları da tetiklemiş, TÜBİTAK Bilişim ve Bilgi Güvenliği İleri Araştırmalar Merkezi'ne (BİLGEM) bağlı olarak siber güvenlik alanında çalışmalar yapmak üzere Siber Güvenlik Enstitüsü 2012 yılında kurulmuştur.[62]

2.2.5. Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı

Daha önceki stratejik belgeler ve eylem planları, Türkiye'nin siber alandaki dönüşümünü; internet kullanımının yaygınlaşması, e-Devlet yapılanmasının oluşturulması, eğitimden ticarete kadar birçok farklı alanının sanal âleme taşınmasını hedefleyen ve siber güvenliğe de kısmen yer veren kamu politikaları olarak karşımıza çıkmaktadır. Ancak 2012 yılında Bakanlar Kurulu Kararıyla kurulan Siber Güvenlik Kurulunun hazırladığı Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, gündemine yalnızca ulusal güvenlik sorunu olarak tespit edilen siber güvenlik konusunu almıştır. Böylelikle bu anlamda ilk ve öncü olduğunu söylemek yerinde olacaktır. Aralık 2012'de Siber Güvenlik Kurulunda onaylanan bu belge, Haziran 2013 tarihinde Resmi Gazete'de Bakanlar Kurulu Kararıyla yayımlanmıştır.[63]

Öncelikle söz konusu belgenin siber güvenlik alanında öngördüğü risklere değinmek yerinde olacaktır. Belgede ilk olarak siber tehditlerin asimetrik oluşu, siber alandaki tüm bilişim sistemlerinin birbirine zarar verecek potansiyele sahip olması, topluma sunulan hizmetlerin çoğunun bilişim sistemleri aracılığıyla gerçekleştirilmesi ve kritik altyapıların neredeyse tamamının internete bağlı olması gibi genel riskler sıralanmıştır. Sonrasında ise Türkiye nezdinde sıralan risk unsurları çarpıcı ve oldukça gerçekçidir. Gerçekten de siber güvenlik konusunda kurumların üst düzey yöneticilerinin yeterli bilinçte olmadığı tespitinin yanı sıra bu alan için özel olarak oluşturulan birimlerdeki insan kaynağının dahi yeterli nitelikte olmadığının ifade edilmesi özellikle çok çarpıcıdır. Belgede bir başka risk unsuru olarak kurumlar arasında ulusal siber güvenlik alanında koordinasyonun gerçekleştirilememesi ve yine bu alanda mevzuat eksikliğinin ulusal ve uluslararası çalışmaları güçleştirdiğinin ifade edilmiştir.[64] Mevzuat alanında günümüze değin önemli sonuçlar elde edilmesine rağmen bu belge ile önceki ve sonraki belgelerde defaten, ulusal siber güvenlik alanında bir kanun ve bu kanuna nazaran çıkarılacak yönetmeliklere ihtiyacın olduğu vurgulanmıştır.

Riskleri ortaya koyduktan sonra çözüm olarak gerek hukuki altyapı gerek eğitim gerekse de kurumsallaşma anlamında birçok eylem öngören Eylem Planı

62 a.k.

63 *Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı*, https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-plani-2013-2014-5a3412cf8f45a.pdf, Erişim Tarihi: 02.05.2021.

64 a.k.

kapsamında, TR-BOME'den daha kapsamlı bir şekilde faaliyet alanı olan Ulusal Siber Olaylara Müdahale Merkezi (USOM), mülga Telekomünikasyon İletişim Başkanlığı (TİB) bünyesinde kurulmuştur. Yine bahsi geçen Eylem Planı'nın sonucu olarak sektörel bazda faaliyet gösterecek olan Siber Olaylara Müdahale Ekibi (SOME), 2014 yılında mülga TİB bünyesinde oluşturulmuştur.[65] İster kamu ister özel sektörün güdümünde olsun, yukarıda tanımlar kısmında değinilen, kritik altyapı sektörlerini siber tehditlere karşı korumak için kurulan SOME'ler aynı zamanda USOM'un kurum ve kuruluşlar içerisindeki bir nevi alt birimleri olarak karşımıza çıkmaktadır. Ulusal siber güvenlik konusunda koordinasyon ve organizasyon kabiliyetini arttıracak bu kurumsal yapılanma, Şubat 2020 tarihi itibariyle sayısı 1000'i aşan SOME ağıyla oldukça hacimli bir yapıya evirilmiştir.[66]

2.2.6. 2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı

2015 yılına gelindiğinde, bilişim teknolojilerinin her alanında Türkiye'nin kalkınmasını hedefleyen ve kapsamı oldukça geniş tutulan Bilgi Toplumu Stratejisi ve Eylem Planı adındaki kamu politikası çalışması geleneğine devam edilmiştir. Böylelikle 2014 yılının Aralık ayında mülga Kalkınma Bakanlığı tarafından hazırlanan 2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı, Şubat 2015 tarihinde Resmi Gazete'de yayımlanmıştır.[67] Kapsadığı dönemde hem 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'nın hem de 2016-2019 Ulusal e-Devlet Stratejisi ve Eylem Planı'nın yayımlandığı bu Eylem Planı, diğerlerinin konularını da kapsayan *"şemsiye"* belge olarak karşımıza çıkmaktadır.[68] 8 eksende gerçekleştirilmesi hedeflenen 72 eylem içeren Eylem Planı'nda 5 numaralı eksen, *"Bilgi Güvenliği ve Kullanıcı Güveni"* başlığı altında düzenlenmiştir.[69] Bu başlıkta, ana hatlarıyla, siber güvenlikle alakalı olarak şu hususlara odaklanılmıştır:

- Nitelikli insan kaynağını artırmak ve toplumun genelinde güvenli internet teknolojileri hakkında farkındalık oluşturmak amacıyla eğitim çalışmalarının sürdürülmesi
- Kurum ve kuruluşlar arasındaki koordinasyonun sağlanması, kurum ve kuruluşların kullandığı altyapıların denetimi
- Hukuki altyapının sağlanarak siber güvenlik alanında asgari standartların

65 *USOM ve Kurumsal Siber Olaylara Müdahale Ekibi*, https://www.btk.gov.tr/usom-ve-kurumsal-siber-olaylara-mudahale-ekibi, Erişim Tarihi: 15.05.2021.

66 Afyonluoğlu, "Siber Güvenlik…", s. 392.

67 *2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı*, http://www.sp.gov.tr/upload/xSPTemelBelge/files/uqSFE+2015-2018_Bilgi_Toplumu_Stratejisi_ve_Eylem_Plani.pdf, Erişim Tarihi: 16.08.2021.

68 Afyonluoğlu, "Siber Güvenlik…", s. 388.

69 *2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı…*, Erişim Tarihi: 16.08.2021.

belirlenerek hızla bu standartlara ulaşılması ve siber suçlarla etkin mücadelenin ihtisaslaşarak gerçekleştirilmesi

- *"2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'nın etkin şekilde uygulanması ve gerektiğinde güncellenmesi"*

Daha çok hukuki, idari ve teknik altyapının güçlendirilmesine yönelen Eylem Planı'nın, odaklandığı bu hususlar ışığında gerçekleşmesini öngördüğü eylemler ve neticeleri ise şu şekildedir:

- Daha önceki eylem planları gibi siber güvenlik alanına özgü özel bir kanunun (Siber Güvenlik Kanunu) çıkarılması hedeflenmiş ancak yine gerçekleşmemiştir.
- Kişisel Verilerin Korunması mevzuatının çıkarılması bu belgede de hedeflenmiş ve nihayet Eylem Planı'nın kapsamı içerisinde yer alan 2016 yılında, Kişisel Verilerin Korunması Kanunu yürürlüğe girmiştir.
- Siber suçlarla mücadele için "*Ulusal Siber Suç Stratejisi"* hazırlanacağı belirtilmiş, bu eylem, 2016-2019 ile 2020-2023 yıllarını kapsayacak şekilde hazırlanan Ulusal Siber Güvenlik Stratejisi ve Eylem Planlarında da amaç olarak yer almıştır.
- Bilişim suçları ihtisas mahkemelerinin kurulması eylemler arasında yer almakla birlikte günümüzde henüz gerçekleşmemiştir. Ancak Mart 2021'de Adalet Bakanlığı tarafından yayımlanan 2020-2023 İnsan Hakları Eylem Planı'nda da altı ay içinde, bilişim suçları ihtisas mahkemelerinin belirleneceği, 3. Amaç 4. Eylem olarak yer almaktadır.[70]

2.2.7. 2016-2019 ile 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planları

Siber güvenlik konusunda ilk tematik strateji belgesinin 2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı olduğu ve bu belgenin öncü olduğu daha önce de belirtilmişti. Gerçekten de 2016 yılında mülga Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tarafından hazırlanan 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, önceki belgenin devamı niteliğinde olup 5 stratejik amaç çerçevesinde 41 eylem öngörmüştür.[71] Kritik altyapıların korunmasını amaç merkezine alan ve siber güvenliğin ulusal güvenlik sorunu olduğunu yineleyen bu belgede öncekinin aksine eylemler, hizmete özel olarak nitelendirilip kamuoyuyla

70 İnsan Hakları Eylem Planı ve Uygulama Takvimi, https://rayp.adalet.gov.tr/resimler/1/dosya/insan-haklari-ep02-03-202115-14.pdf, Erişim Tarihi: 16.05.2021.

71 *2016-2019 Ulusal Siber Güvenlik Stratejisi*, https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf, Erişim Tarihi: 16.08.2021, Afyonluoğlu, "Siber Güvenlik…", s. 394.

paylaşılmamıştır. Aynı şekilde 2020 yılının aralık ayında 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı**,** Ulaştırma ve Altyapı Bakanlığı tarafından hazırlanarak bir Cumhurbaşkanlığı Genelgesi ile Resmi Gazete'de yayımlanmıştır.[72] Sekiz stratejik amaç kapsamında kırk adet eylem içeren bu belgede, "*siber güvenliğin ulusal güvenliğin ayrılmaz bir parçası"* olduğu vurgulanmış aşağıdaki 8 amaç kamuoyuyla paylaşılarak eylem planları ise yine hizmete özel olarak nitelendirilip paylaşılmamıştır. Güncel nitelikte olan bu Eylem Planı'nın, kamuoyuyla paylaşılan stratejik amaçları şu şekildedir:

- *Kritik Altyapıların Korunması ve Mukavemetin Artırılması*
- *Ulusal Kapasitenin Geliştirilmesi*
- *Organik Siber Güvenlik Ağı*
- *Yeni Nesil Teknolojilerin Güvenliği*
- *Siber Suçlarla Mücadele*
- *Yerli ve Milli Teknolojilerin Geliştirilmesi ve Desteklenmesi*
- *Siber Güvenliğin Milli Güvenliğe Entegrasyonu*
- *Uluslararası İş Birliğinin Geliştirilmesi*

Her iki eylem planında da eylemlerin paylaşılmaması eylemlerin gerçekleştirme durumunu güçleştirmektedir. Ancak 2017 yılında, Uluslararası Telekomünikasyon Birliği (ITU) tarafından yayımlanan Küresel Siber Güvenlik Endeksi'nde, 164 ülke arasında Türkiye 43. sırada yer alırken, 2019 yılında yenisi yayımlanan raporda, Türkiye'nin 175 ülke arasında 20. sıraya yükselmesi,[73] Türkiye'nin 2016-2019 Eylem Planı döneminde ne denli geliştiğini gözler önüne sermektedir. Tabii ki bu gelişimde yalnızca 2016-2019 Eylem Planı'nın değil, 2000'li yıllardan beridir eksiğiyle fazlasıyla istikrarlı bir şekilde güncellenen politika belgelerinin, kümülatif olarak ilerleyen bilgi, bilinç ve teknoloji çıktılarının da etkisi olduğu bir gerçektir.

3. TÜRKİYE'NİN SİBER GÜVENLİK TEŞKİLATLANMASI

Buraya kadar irdelenen mevzuat ve kamu politikalarının oluşturulması, geliştirilmesi ve bunlarla ortaya konan hedeflerin gerçekleştirilmesi, Türkiye'nin, ulusal siber güvenliğinin tesisi amacıyla oluşturduğu kurumsallaşmayla sağlanmıştır.

72 *Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023*, https://hgm.uab.gov.tr//uploads/pages/siber-guvenlik/ulusal-siber-guvenlik-stratejisi-ep-2020-2023.pdf, Erişim Tarihi: 30.04.2021.

73 *Global Cybersecurity Index (GCI): 2017,* http://www.bilgitoplumu.gov.tr/wp-content/uploads/2017/07/global_cybersecurity_index_2017.pdf, Erişim Tarihi: 19.05.2021, *Global Cybersecurity Index (GCI): 2018*, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf, Erişim Tarihi: 19.05.2021.

Türkiye'de siber güvenlik konusunda günümüze değin birçok kurum ve kuruluş görevlendirilmiştir. Bunlardan bazıları ülkenin savunma hattının nasıl tahkim edileceği yönünde fikirler üretme, bazıları bu fikirler doğrultusunda teknolojik kapasiteyi geliştirme, bazılarıysa -tabiri caizse- siber alandaki savaş meydanında göğüs göğüse çarpışarak tehditleri bertaraf etme fonksiyonlarını üstlenmiştir. Bu bölümde, Türkiye'nin, siber güvenlik konusunda bahsedilen fonksiyonları üstlenmekte başı çeken kurum ve kuruluşları ile bunların görevlerine kısaca değinilecektir.

3.1. TÜBİTAK ve Alt Kuruluşları

Siber güvenlik konusunda günümüzde de birçok görevi bulunan TÜBİTAK; bünyesinde yer alan kuruluşlarla 2012 yılından önce bu alanda Türkiye'nin siber güvenliği konusunda asıl görevi üstlenen bir kurum olarak karşımıza çıkmaktadır.[74] Türkiye'nin ilk kurum risk analizlerini yapıp buna yönelik raporlar hazırlayan UEKAE ve enformasyon çalışmalarında önemli rol alan Marmara Araştırma Merkezi (MAM), TÜBİTAK bünyesinde yer alan önemli kuruluşlar olmakla birlikte bunlar 2010 yılında tek çatı altında birleştirilerek BİLGEM adını almıştır. Siber güvenlik konusunda pek çok ilke imza atan TÜBİTAK; Türkiye'nin ilk Ağ Güvenliği Grubunu da 1997 yılında kurmuş, daha sonra 2012 yılında Ağ Güvenliği Grubu, Siber Güvenlik Enstitüsüne dönüştürülmüştür.[75] 2012 yılında siber güvenlik konusunda başat görevlerini mülga Ulaştırma, Denizcilik ve Haberleşme Bakanlığına bırakan TÜBİTAK, günümüzde hem Ulaştırma ve Altyapı Bakanlığı hem de diğer kurum ve kuruluşlarla birlikte koordineli olarak çalışmakta, BİLGEM ve SGE vasıtasıyla siber güvenlik alanında görevler üstlenmeye devam etmektedir.

3.2. Bilgi Teknolojileri ve İletişim Kurumu (BTK)

27 Ocak 2000 tarih ve 4502 sayılı Kanunla Telekomünikasyon Kurumu adıyla kurulan Bilgi Teknolojileri ve İletişim Kurumu, günümüzdeki adını 2008 yılında yürürlüğe giren 5809 sayılı Elektronik Haberleşme Kanunu ile almıştır.[76] Genel olarak telekomünikasyon sektörünü düzenlemek, bu sektörde rekabeti temin etmek, denetim yapmak gibi amaçlarla kurulan Kurum'a, yine 5809 sayılı Kanun'la 2014 yılında; *"siber güvenlik ve internet alan adları konularında Cumhurbaşkanı, Bakanlık ve/veya Siber Güvenlik Kurulu tarafından verilen görevleri Telekomünikasyon İletişim Başkanlığı veya diğer birimleri marifetiyle yerine getirmek"*

74 Darıcılı, "Türkiye'nin Siber ...".

75 *Biz Kimiz?*, https://bilgem.tubitak.gov.tr/tr/kurumsal/biz-kimiz, Erişim Tarihi: 20.05.2021.

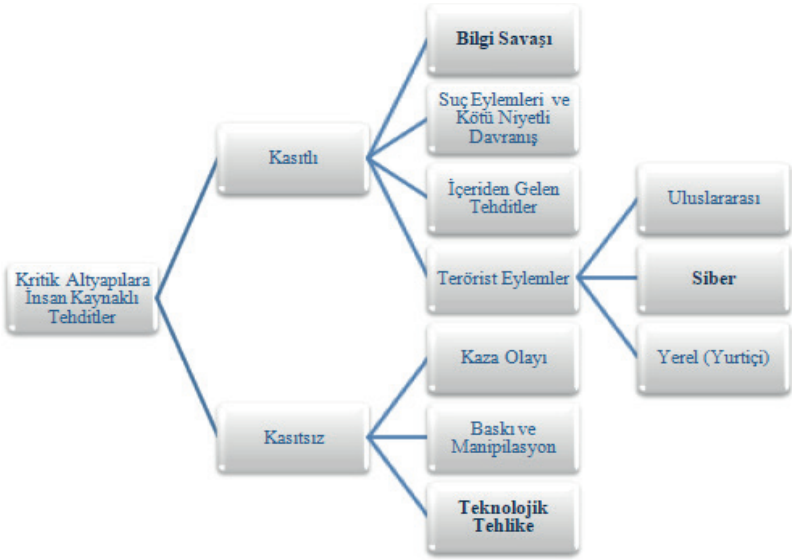
76 *Siber Güvenlik: Mevzuat*, https://www.btk.gov.tr/siber-guvenlik-mevzuat, Erişim Tarihi: 20.05.2021.

görevi verilmiştir.[77]

3.3. Afet ve Acil Durum Yönetimi Başkanlığı (AFAD)

29 Mayıs 2009 tarihinde 5902 sayılı Kanun'un yürürlüğe girmesiyle kurulan AFAD, afet ve kriz yönetiminin merkezi olarak koordine edilmesi ve sağlıklı bir şekilde yürütülmesi amacıyla kurulmuştur.[78] Başkanlığın kuruluşunda siber güvenlikle ilgili olarak görevleri bulunmamakla birlikte, 2014 yılında AFAD tarafından hazırlanan *"2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi"*nin yayımlanmasıyla ulusal kritik altyapıların korunmasında koordine edici kuruluş olarak AFAD'ın görevlendirildiği görülmektedir. Söz konusu belgede kritik altyapılara karşı tehdit oluşturan insan kaynaklı unsurlar arasında siber saldırıların terörizm faaliyeti olarak ve kasıtlı bir biçimde gerçekleştirildiği (Şekil 1) tespitine yer verilmekte, böylelikle bu alandaki koruma faaliyetlerinde de AFAD'ın koordine edici kuruluş olarak görevlendirildiği anlaşılmaktadır.[79]

Şekil 1: 2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi: Kritik Altyapılara İnsan Kaynaklı Tehditler (AFAD, 2014)



77 *5809 Sayılı Elektronik Haberleşme Kanunu*, https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5809&MevzuatTur=1&MevzuatTertip=5, Erişim Tarihi: 05.05.2021.

78 *AFAD Hakkında*, https://www.afad.gov.tr/afad-hakkinda, Erişim Tarihi 20.05.2021.

79 *2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi,* https://afyonluoglu.org/PublicWebFiles/Reports-TR-SG/2014-2023-AFAD-Kritik%20Altyap%C4%B1larin%20Korunmasi%20Yol%20Haritasi.pdf, Erişim Tarihi: 22.05.2021.

3.4. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi

2017 yılında yapılan referandum sonucunda Türkiye'de Cumhurbaşkanlığı Hükümet Sistemi adında yeni bir hükümet sistemine geçilmiş ve bu doğrultuda 10 Temmuz 2018 tarihli ve 30474 sayılı Resmi Gazete'de, yürütmenin başı olan Cumhurbaşkanlığının teşkilatlanması, 1 sayılı Cumhurbaşkanlığı Kararnamesi vasıtasıyla düzenlenmiştir. 1 sayılı Kararnameyle kurulan Dijital Dönüşüm Ofisi'ne yine bu Kararnameyle; kamunun dijital dönüşümüne öncülük etmek, e-Devlet hizmetlerinin sunumunda aracılık etmek, yerli ve milli teknolojilerin kamuda kullanımını temin etmek gibi görevler verilmiştir. Bu görevlerinin yanı sıra "*bilgi güvenliği ve siber güvenliği artırıcı projeler gerçekleştirmek"* görevi de verilen Ofis'in bu bağlamda Siber Güvenlik Daire Başkanlığı adında bir hizmet birimi de bulunmaktadır.[80]

3.5. Ulaştırma ve Altyapı Bakanlığı

Daha önce de ifade edildiği üzere TÜBİTAK, 2012 yılına değin Türkiye'nin ulusal siber güvenlik politikalarında başı çeken kurum iken, Bakanlar Kurulu tarafından verilen Haziran 2012 tarihli *"Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar"* gereğince görevlerini mülga Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'na bırakmıştır.[81] Kararda, Bakanlığa siber güvenlik konusunda;

- Ulusal stratejileri belirleme,
- Eylem planlarını hazırlama,
- Kurumlar arası uyumu sağlama ve koordinasyonu temin etme,
- Aynı Kararla kurulan Siber Güvenlik Kurulunun sekretarya hizmetlerini yürütme,
- Gerektiğinde uluslararası kuruluşlarla iş birliğine gitme,
- Toplumsal farkındalığı artırmaya yönelik eğitim faaliyetlerini yürütme,
- Siber saldırılara karşı milli savunma mekanizmalarını geliştirme

gibi birçok önemli görev verilmiştir.[82] Gerçekten de bu tarihten itibaren siber

80 *1 Sayılı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi,* https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=1&MevzuatTur=19&MevzuatTertip=5, Erişim Tarihi: 23.05.2021.

81 Afyonluoğlu, "Siber Güvenlik…", s. 391.

82 *Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı*, https://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18.htm, Erişim Tarihi: 23.05.2021.

güvenlikle alakalı önemli politika çalışmaları, bakanlık düzeyinde Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tarafından yerine getirilmiştir. Bakanlığa 5098 sayılı Elektronik Haberleşme Kanunu'nda 2016 yılında yapılan değişiklikle de siber güvenlik konusunda ek görevler verilmiştir. 2018 yılında 1 sayılı Cumhurbaşkanlığı Kararnamesiyle Cumhurbaşkanlığı Hükümet Sisteminin gereği olarak Cumhurbaşkanlığına bağlanan ve teşkilat yapılanması değiştirilen Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, Ulaştırma ve Altyapı Bakanlığı ismini almıştır. İlk olarak 2013-2014 Ulusal Güvenlik Stratejisi ve Eylem Planı'nda imzası bulunan Bakanlık, bu tarihten sonraki tüm eylem planı ve stratejilerde başrolü oynamaktadır. Son olarak Bakanlık yukarıda da değinildiği üzere, 29 Aralık 2020 tarihinde 2020-2023 Ulusal Güvenlik Stratejisi ve Eylem Planı'nı yayımlamıştır.

SONUÇ

Siber alan ya da siber uzay, günümüzde korunması gerekli beşinci alan olarak nitelendirilmekte, böylelikle siber güvenlik de bireylerden devlet ve uluslararası örgütlere kadar tüm gerçek ve tüzel kişilerin güvenliklerinde göz ardı edilmeyecek kadar önemli bir yer tutmaktadır. Zira siber saldırılar, günümüzde ekonomik saik ile gerçekleştirilebileceği gibi doğrudan ya da dolaylı olarak kişilerin yaşamlarını ve sosyal yaşantılarını da hedef alabilmektedir. Dolayısıyla saldırının hedefinde hangi yapı olursa olsun, saldırının sonucundan geniş kitleler etkilenebilmekte, devletlerin hizmet mekanizmaları sarsılabilmekte ve belki de en önemlisi gerçek veya tüzel kişilerin varlıkları, saldırının maddi veya manevi etkisiyle son bulabilmektedir. Tüm bu nedenlerden ötürü siber alanın, günümüzde, bir savaş meydanı haline geldiğini ve başta devletler olmak üzere -gerçek yahut tüzel- toplumu oluşturan bütün yapıların siber güvenlik hatlarını tahkim etmelerinin zorunluluk arz ettiğini söylemek yanlış olmayacaktır.

Ağ teknolojilerinin sivil hayata tesir ettiği ilk günlerden bu yana Türkiye siber güvenlikte bir hayli yol kat etmiş, önemli politik ve hukuki çalışmalarla hem devlet mekanizmasının hem de toplumunun siber güvenliğini sağlamayı amaçlamıştır. Uluslararası Telekomünikasyon Birliğinin 2018 yılı siber güvenlik verilerine göre; Türkiye, Avrupa ülkeleri arasında 11. sırada, dünya genelinde ise 175 ülke arasında 20. sırada olup azımsanmayacak derecede önemli bir seviyededir.[83] Ancak son yıllarda ülkenin ulusal güvenliği açısından gerçekleştirdiği yerli ve milli teknolojik hamleler, Türkiye'nin siber güvenlik alanında da daha fazlasını yapabileceğini göstermektedir.

Siber alanda güvenliğin sağlanması için öncelikle zafiyet alanlarının farklı farklı değerlendirilerek ele alınması gerekmektedir. Zafiyetlerin tespitinde kamu

83 Afyonluoğlu, "Siber Güvenlik…", s. 401.

otoritesi; bu alanda faaliyet gösteren özel işletmeler, üniversiteler ve sivil toplum kuruluşları gibi paydaşlarla birlikte çalışmalı, yine bu kuruluşlarla birlikte, istişare kültürünü işleterek, koordineli bir şekilde siber güvenliğin sağlanması için politika çalışmalarını yürütmesinin gerekliliği açıktır. Ayrıca bu çalışmaların da süreklilik arz etmesi gerekmektedir.[84]

Türkiye'nin, son zamanlarda askeri kabiliyetlerini geliştirmek amacıyla yaptığı modernizasyon çalışmalarında devlet destekli özel şirketlerin ortaya koyduğu performans Türkiye'yi bir anlamda çağ atlatmıştır. En son Polonya Savunma Bakanlığından yapılan açıklamaya göre; Polonya Devleti, Türkiye'den Bayraktar adlı şirketin geliştirmiş olduğu 24 adet Silahlı İnsansız Hava Aracı (SİHA) ithalatını gerçekleştirecektir. Böylece Türkiye ilk defa bir NATO üyesi Devlete yerli ve milli insansız hava araçlarından ihraç edecektir.[85] Bu örnekten hareketle Türkiye'de siber güvenlik teknolojileri alanında da özel şirketler, özellikle de Türkiye'nin savunma sanayi kuruluşları arasında başı çeken ASELSAN, HAVELSAN, TUSAŞ, ROKETSAN ve Bayraktar gibi şirketleri desteklemesi yerinde olacaktır. Türkiye'nin gittikçe büyüyen siber güvenlik pazarından ekonomik gücüyle ölçülü olarak payını alması gerekmektedir. Türkiye'deki özel şirketler de devlet tarafından teşvik ödenekleriyle desteklenmeli, bu konuda gerekli yasal düzenlemeler yapılmalı, halihazırdaki siber güvenlik önlemlerinin yerlileştirilmesine yoğunlaşılmalıdır. Böylece tabanda özel girişimler, orta düzlemde devlet destekli savunma şirketleri nihayet tavanda kamu kurumlarının olduğu bir bilgi ve teknoloji aktarım piramidi modelinin geliştirilmesinin Türkiye'nin bu alandaki ihtiyaçlarını karşılayacağı düşünülmektedir.

Siber güvenliğin sağlanmasında bir başka dikkat edilmesi gereken husus; siber saldırıların çok yönlü olması nedeniyle, saldırı tekniklerinin, siber güvenlik konusunda görevli kuruluşlar tarafından uygulamalı olarak öğrenilmesi ve tatbik edilmesidir. Siber güvenlik konusunda Türkiye; Amerika Birleşik Devletleri, Rusya Federasyonu, Çin Halk Cumhuriyeti, İsrail ve hatta komşusu olan İran'ın aksine genel olarak strateji çalışmalarını savunma üzerine temellendirmektedir.[86] Ancak alışılagelen klasik savaşlardan edindiğimiz tecrübelerle savaşlarda yalnızca savunma stratejileriyle başarı kazanmanın bir hayli güç olduğunu rahatlıkla söylemek mümkündür. Sıraladığımız bu devletler, siber güvenlikte bugün dünya ülkeleri arasında ön sıralarda yer almalarını, siber saldırı ve siber istihbarat konularında da uzmanlaşmalarıyla elde etmişlerdir. Türk Silahlı Kuvvetlerinin; *"yurt-*

84 a.k., s. 401.

85 *AB üyesi Polonya, Türkiye'den silahlı insansız hava aracı satın alacak*, https://www.aa.com.tr/tr/dunya/ab-uyesi-polonya-turkiye-den-silahli-insansiz-hava-araci-satin-alacak/2250932, Erişim Tarihi: 24.05.2021.

86 Darıcılı, "Türkiye'nin Siber ...", s. 14.

ta sulh cihanda sulh" gayesi ve *"etkin, caydırıcı, saygın"* mottosunu bir arada düşünüldüğünde Türkiye, siber alanda da barışçıl ama aynı zamanda caydırıcı olmayı hedeflemelidir. Hâlihazırda Cumhurbaşkanlığı Savunma Sanayi Başkanlığı tarafından yürütülen TSK Siber Savunma Merkezi (SİSAMER) projesi bu yönde önemli bir gelişmedir. Ayrıca kamu idarelerinin savunma sanayi şirketleri ürünlerinden de maksimum verimle faydalanmaları sağlanmalıdır.

Türkiye'de günümüze kadar gerçekleştirilen birçok hukuki çalışma olmakla birlikte siber güvenlik stratejileri ve eylem planlarında da defaten gündeme getirildiği üzere, hukuki altyapı yetersizliği nedeniyle hem kamu kurum ve kuruluşlarının hem de özel işletmelerin siber güvenlik alanında yapacağı çalışmalarda önlerine bir hayli engel çıkmaktadır. Bu nedenle siber güvenlikle alakalı olarak mevzuatın güçlendirilmesi ve sürekli olarak güncellenmesi, Türkiye'de yukarıda sıraladığımız önerilerin gerçekleştirilmesi ve hâlihazırdaki politika çalışmalarında da yüksek verim elde edebilmesi için elzemdir. Türkiye'de siber güvenlikle ilgili hukuki düzenlemelerin başta Elektronik Haberleşme Kanunu olmak üzere türlü kanunların içerisinde parça parça yer aldığı gözlemlenmektedir. Bu kapsamda Türkiye'nin siber güvenlik konusuna münhasır bir kanuna ihtiyacı bulunmaktadır. Siber güvenlikle ilgili genel kanunun yürürlüğe girmesinden hemen sonra ülkenin kritik altyapılarına da bütünleşik bir bakış açısıyla bakılmaktan vazgeçilmeli, her kritik altyapı sektörünün siber tehditlere karşı korunmasının usul ve esaslarını düzenleyen farklı hukuki düzenlemelerle hem devlet bünyesinde yer alan hem de özel kuruluşların içinde bulunduğu dağınıklık giderilmelidir.

KAYNAKÇA

1 Sayılı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi, https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=1&MevzuatTur=19&MevzuatTertip=5, Erişim Tarihi: 23.05.2021.

2006-2010 Bilgi Toplumu Stratejisi Eylem Planı: Nihai Değerlendirme Raporu, http://www.bilgitoplumu.gov.tr/Documents/1/Diger/bts_ve_eylem_planı_nıhaı_degerlendırme_raporu.pdf, Erişim Tarihi: 15.08.2021.

2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi., https://afyonluoglu.org/PublicWebFiles/Reports-TR-SG/2014-2023-AFAD-Kritik%20Altyap%C4%B1larin%20Korunmasi%20Yol%20Haritasi.pdf, Erişim Tarihi: 22.05.2021.

2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı, http://www.sp.gov.tr/upload/xSPTemelBelge/files/uqSFE+2015-2018_Bilgi_Toplumu_Stratejisi_ve_Eylem_Plani.pdf, Erişim Tarihi: 16.08.2021.

2016-2019 Ulusal Siber Güvenlik Stratejisi, https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf, Erişim Tarihi: 16.08.2021.

3713 Sayılı Terörle Mücadele Kanunu, https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=3713&MevzuatTur=1&MevzuatTertip=5, Erişim Tarihi: 04.05.2021.

5070 Sayılı Elektronik İmza Kanunu, https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5070&MevzuatTur=1&MevzuatTertip=5, Erişim Tarihi: 04.05.2021.

5237 Sayılı Türk Ceza Kanunu, https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5237&MevzuatTur=1&MevzuatTertip=5, Erişim Tarihi: 04.05.2021.

5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5651&MevzuatTur=1&MevzuatTertip=5, Erişim Tarihi: 05.05.2021.

5809 Sayılı Elektronik Haberleşme Kanunu, https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5809&MevzuatTur=1&MevzuatTertip=5, Erişim Tarihi: 05.05.2021.

6098 Sayılı Kişisel Verilerin Korunması Kanunu, https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6098&MevzuatTur=1&MevzuatTertip=5, Erişim Tarihi: 07.05.2021.

AB üyesi Polonya, Türkiye'den silahlı insansız hava aracı satın alacak,. https://www.aa.com.tr/tr/dunya/ab-uyesi-polonya-turkiye-den-silahli-insansiz-hava-araci-satin-alacak/2250932, Erişim Tarihi: 24.05.2021.

AFAD Hakkında,. https://www.afad.gov.tr/afad-hakkinda, Erişim Tarihi 20.05.2021.

Afyonluoğlu, Mustafa., "Siber Güvenlik ve Kamu Politikaları", *Teknoloji ve Kamu Politikaları Kitabı*, ss. 379-411, (Ed.: Mete Yıldız-Cenay Babaoğlu), Gazi Kitabevi, Ankara, 2020.

Bıçakçı, Salih vd., "Türkiye'de Siber Güvenlik", *EDAM Siber Güvenlik Kağıtları Serisi*, 25 Aralık 2015, S. 1, ss. 28-73.

Bilgi Toplumu Stratejisi Eylem Planı: 2006-2010, http://www.bilgitoplumu.gov.tr/wp-content/uploads/2014/04/Bilgi_Toplumu_Strateji_Eylem_Plani_2006-2010.pdf, Erişim Tarihi: 15.05.2021.

Biz Kimiz? https://bilgem.tubitak.gov.tr/tr/kurumsal/biz-kimiz, Erişim Tarihi: 20.05.2021.

Çeliktaş, Barış, *Siber Güvenlik Kavramının Gelişimi ve Türkiye Özelinde Bir Değerlendirme*, (Yayımlanmamış Doktora Tezi), Karadeniz Teknik Üniversitesi Sosyal Bilimler Enstitüsü, Trabzon, 2016.

Darıcılı, Ali Burak, "Türkiye'nin Siber Güvenlik Politikalarının Analizi: Türkiye'nin Potansiyel Siber Güvenlik Stratejisi"*, TESAM Akademi Dergisi*, C. 6, S. 2, ss. 11-33.

E-Devlet ve Bilgi Toplumu Kanunu Tasarısı, https://www.memurlar.net/haber/146427/e-devlet-ve-bilgi-toplumu-kanun-tasarisi.html, Erişim Tarihi: 02.05.2021.

e-Dönüşüm Türkiye Projesi Kısa Dönem Eylem Planı, http://www.bilgitoplumu.gov.tr/wp-content/uploads/2015/02/050000_E-DonusunTurkiyeKDEP.doc, Erişim Tarihi: 12.05.2021.

e-Dönüşüm Türkiye Projesi Kısa Dönem Eylem Planı: Sonuç Raporu, http://bilgitoplumu.gov.tr/Documents/1/KDEP/050500_KDEPSonucaporu.pdf, Erişim Tarihi: 12.05.2021.

Eker, Umut, "Türk Ceza Hukuku'nda Bilişim Suçları" Eski TCK Bağlamında Hukukumuzda Yer Alan İlk Düzenlemeler ve 5237 Sayılı Yeni Türk Ceza Kanunu'nun İlgili Hükümlerinin Yorumu", *Türkiye Barolar Birliği Dergisi,* S. 62, ss. 101-131.

Emre, Bâkır, "*İnternet Güvenliğinin Tarihçesi*", *BİLGEM Dergisi*, C. 3, S. 5, ss. 6-17.

E-Türkiye Girişimi Eylem Planı. http://www.bilgitoplumu.gov.tr/Documents/1/Yayinlar/020800_E-TurkiyeEylemPlani.pdf , Erişim Tarihi: 11.05.2021.

Global Cybersecurity Index (GCI): 2017, http://www.bilgitoplumu.gov.tr/wp-content/uploads/2017/07/global_cybersecurity_index_2017.pdf, Erişim Tarihi: 19.05.2021.

Global Cybersecurity Index (GCI): 2018, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf, Erişim Tarihi: 19.05.2021.

Hürriyet, *Yerli Siber Güvenlik Şirketlerinin Küresel Arenadaki Durumu Nasıl?,* https://www.hurriyet.com.tr/teknoloji/yerli-siber-guvenlik-sirketlerinin-kuresel-arenadaki-durumu-nasil-41250148, Erişim Tarihi: 24.04.2021.

İnsan Hakları Eylem Planı ve Uygulama Takvimi. https://rayp.adalet.gov.tr/resimler/1/dosya/insan-haklari-ep02-03-202115-14.pdf, Erişim Tarihi: 16.05.2021.

Kılcı, Hilal Başak, "Türkiye'nin Siber Güvenlik Politikaları", *Cyberpolitik Journal*, C. 5, S. 9, ss. 113-140, http://cyberpolitikjournal.org/index.php/main/article/download/7/7/13, Erişim Tarihi: 27.04.2021.

Kritik Altyapılarda Siber Güvenlik. https://icsdefense.net/blog/kritik-altyapilarda-siber-guvenlik, Erişim Tarihi: 03.05.2021.

Kullanıcı Sayısı. https://www.turkiye.gov.tr/, Erişim Tarihi: 07.05.2021.

Memiş, Levent – Güç, Melikali, "Akıllı Kentlerde Verinin Gizliliği ve Güvenliği: İlkeler ve Yaklaşımlar", *Güvenlik Bilimleri Dergisi, UGK Özel Sayısı*, s. 95-112.

Öğün, Mehmet Nesip-– Kaya, Adem, **"**Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler"*, Güvenlik Stratejileri Dergisi*, C. 9, S. 18, ss. 145-181, https://www.guvenliweb.org.tr/dosya/czNaM.pdf, Erişim Tarihi: 11.05.2021.

Salihpaşaoğlu, Yaşar, *Din ve Devlet Arasındaki İktidar Mücadelesi: Avrupa Örneği,* Adalet Yayınevi, 4.Baskı, Ankara, 2018.

Sertçelik, Aşır, "Siber Olaylar Ekseninde Siber Güvenliği Anlamak", *Medeniyet Araştırmaları Dergisi*, C. 2, S. 3, ss. 25-42.

Siber Güvenlik: Mevzuat, https://www.btk.gov.tr/siber-guvenlik-mevzuat, Erişim Tarihi: 20.05.2021.

Siber Ortamla İlgili Kullanılan Kavramlar, http://www.certbylab.com/blog/siber-kavramlar/, Erişim Tarihi: 03.05.2021.

Şahin, Raşit, "Sanayi Devrimi Osmanlı İmparatorluğu'nda Neden Başlamadı?"*, Business, Economics and Management Research Journal – BEMAREJ*, C. 2, S. 1, ss. 1-16.

Türk Ceza Kanunu Madde Gerekçeleri, http://www.baltaci.av.tr/turk-ceza-kanunu-madde-gerekceleri/, Erişim Tarihi: 04.05.2021.

Türkiye Cumhuriyeti Anayasası, *https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=2709&MevzuatTur=1&MevzuatTertip=5,* Erişim Tarihi: 07.05.2021.

Türkiye Ulusal Enformasyon Altyapısı Anaplanı: Sonuç Raporu, http://www.bilgitoplumu.gov.tr/Documents/1/Yayinlar/991000_TuenaRapor.pdf, Erişim Tarihi: 10.08.2021.

Ulusal Bilgi Güvenliği Teşkilatı ve Görevleri Hakkında Kanun Tasarısı, https://www.tbd.org.tr/ulusal-bilgi-guvenligi-teskilati-ve-gorevleri-hakkinda-kanun-tasarisi/, Erişim Tarihi: 03.05.2021.

Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı., https://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18.htm, Erişim Tarihi: 23.05.2021.

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-plani-2013-2014-5a3412cf8f45a.pdf, Erişim Tarihi: 02.08.2021.

Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023, https://hgm.uab.gov.tr//uploads/pages/siber-guvenlik/ulusal-siber-guvenlik-stratejisi-ep-2020-2023.pdf, Erişim Tarihi: 30.09.2021.

USOM ve Kurumsal Siber Olaylara Müdahale Ekibi, https://www.btk.gov.tr/usom-ve-kurumsal-siber-olaylara-mudahale-ekibi, Erişim Tarihi: 15.05.2021.

Usta, Ayşe, "Aydınlanma Düşüncesine Kısa Bir Bakış", *Kastamonu İletişim Araştırmaları Dergisi,* S.1, ss. 74-90.

Üneri, Mert, "e-Dönüşüm Türkiye Bilgi Güvenliği Projeleri", http://bilgitoplumu.gov.tr/Documents/1/Icra_Kurulu/070123_IK20.ToplantisiUEKAEBilgiGuvenligiSunusu.pdf, Erişim Tarihi: 12.05.2021.

Ünver, Mustafa vd., "Kritik Altyapıların Korunması" *Ankara: BTK.*

Ünver, Mustafa vd., "Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler", *Ankara: BTK.*